ISSN 2335-2337, ISSN 2424-5488 (Online). BALTIC JOURNAL OF POLITICAL SCIENCE. December 2016, No 5
DOI: https://doi.org/10.15388/BJPS.2016.5.10337

CYBERSECURITY IN CENTRAL EASTERN EUROPE: FROM IDENTIFYING RISKS TO COUNTERING THREATS

Agnija Tumkevič

ABSTRACT

Today, ensuring security in cyberspace is a top priority of national security policy for most states. States' approaches to cybersecurity can be divided into two categories: those that regard cybersecurity as a civilian task; and those that involve their militaries in creating or implementing cybersecurity policies. Those states that have incorporated cyberwarfare into their military planning and organization perceive cyberattacks as a threat to their national security, while states that charge their civilian agencies with domestic cybersecurity missions classify cyber intrusions as security risks for only particular sectors. Adopting the framework of securitization theory, this article theorizes both civil and military approaches to cybersecurity and threat perceptions and their sources. The theoretical framework is then applied to a study of the cybersecurity policies of Central European countries and the Baltic States.

Keywords*: cybersecurity policy, civil-military approach, securitization, militarization, criminalization.*

INTRODUCTION

Today, cybersecurity is increasingly regarded as a national issue affecting all levels of society (ENISA, 2012). Consequently, securing cyberspace has become an integral part of states' national security policies. Cyberthreats have revolutionised the way people think about security and the rules and methods for safeguarding national security (Świątkowska, 2012). Although, defining cyberthreats seems to be problematic, almost all states agree that cyberspace threats and risks need to be specifically addressed in their national security policies. Countries around the world are, therefore, formulating cybersecurity strategies, usually by devising some kind of national legal act or programme to respond to cyberthreats and protect critical networks (The Cyber Index, UNIDIR, 2013). However, priorities for national cybersecurity policies vary by country. Some countries have a very clear vision of the cyber environment and its main referent objects such as critical infrastructure (*CI*), have formulated a comprehensive perception of issues that pose threats to cybersecurity and national security, and have identified the most dangerous source of cyberthreats. As a result, in these countries, tasking government agencies with cybersecurity management is a key condition for implementing effective cybersecurity policies. In contrast, states with a prevailing civil approach to cybersecurity are mainly concerned with

AGNIJA TUMKEVIČ, PhD candidate, Institute of International Relations and Political Science, Vilnius University, e-mail: agne.tumkevic@gmail.com

cybercrime. The potential sources of cybercrime risks are more diffused and primarily related to private property and the proper functioning of the economic sector.

The roots of states' different approaches to cybersecurity can be analysed from a theoretical point of view. There are competing doctrines for viewing cybersecurity issues. The so-called national security paradigm reflects the traditional role of the state in securing countries' borders and enforcing the rule of law (Newmeyer, 2015). According to Harknett and Stever (2009), the cybersecurity issue is unique multifaceted, establishing cybersecurity requires states to secure public, private, and economic cyber activities. Cybersecurity is considered fundamental to a state's military and economic security and as such is approached with traditional national security arguments based on protecting the homeland (Harnett and Stever, 2009). In other words, this approach emphasizes the link between the protection of critical infrastructure and those public and private systems that are important to the operation of the government. The national security paradigm refers to the top-down approach of managing and securing cyberspace risks in a manner that may result in increasing the military's influence on cyberspace policies (Dunn Cavelty,2013). Therefore, the concept of cyberspace militarization can be analysed through the national security paradigm.

In contrast to the military approach, the civil approach can be analysed through an economic lens. In this regard, the economic paradigm reflects the growing influence of the internet on the state's economic well-being (Newmeyer, 2015). While the national security paradigm excludes all other sectors but the military from the processes of formulating cyberspace policies, the economic perspective emphasizes the importance of the participation of other sectors and institutions in the formulation of cybersecurity policies. According to Moore (2010), from the economic perspective, there are two necessary conditions to implementing a national cybersecurity strategy: 1) internet service providers should be held accountable for eliminating malware-infected computers on their systems; and 2) companies and other agencies should be required to disclose data breeches and control system intrusions. The economic paradigm refers to a decentralized approach among a group of agencies and actors responsible for cybersecurity management. In this approach, the burden of taking measures to protect systems as a whole is shared by the individual, service providers and the government.

Both paradigms, national security and economic, suggest frameworks for a theoretical analysis of the process of creating and implementing cybersecurity policies. A variety of optional theoretical approaches could still be highlighted. The framework used in this paper is the securitization framework of the Copenhagen school. As Hansen and Nissenbaum note (2009), the understanding of security as a discursive modality with a particular rhetorical structure and political effect renders the Copenhagen school's framework well suited to a study of the formation and evolution of cybersecurity discourse. Therefore, this article—based on the results of a qualitative study of the four Visegrad states (Poland, The Czech Republic, Slovakia, and Hungary) and the three Baltic states (Lithuania, Latvia, and Estonia)—aims to: 1) investigate how the civil and military approaches correlate to securitization processes; and 2) contribute to understandings of differences in states‘s cyberspace behaviours and cooperation patterns in cyberspace.

1. THE COPENHAGEN SCHOOL AND CYBERSECURITY

In the 1990s, securitization theorists such as Buzan, Weaver, and De Wilde did not perceive cybersecurity as an existential threat to states. However, as a consequence of the growing dependence of human societies on cyber networks, cybernetic issues are now securitized, suggesting that the materialization of this process is highlighted through an analysis of policies, institutional and strategic responses (Lobato, 2015). Thus, it is important to analyse, how states, acting as securitizing actors, become alert to the risks of cyberattacks and then establish a specific agenda to deal with threats. In this context, maintaining a secure cyberspace legitimizes the use of extraordinary measures. The ability of an actor to successfully securitize an issue is highly dependent on their position. According to Buzan, security has, to some degree, been institutionalized and, therefore, "some actors are placed in positions of power by virtue of being generally accepted voices of security, by having the power to define security." (Buzan, Weaver, de Wilde, 1998). A government's cybersecurity policy would therefore seem to be an ideal vehicle for mobilizing, and perhaps also legitimizing, a securitizing move. A policy represents an administration's official stance on an issue understood to be a problem and proposes solutions based on technical knowledge and research. In this regard, cybersecurity policies reflect in strategic documents, such as the national and cybersecurity strategies, the processes of defining cyberspace as a realm requiring security measures.

Given this, I operationalize both military and civil approaches of cybersecurity in order to apply the Copenhagen school's theoretical framework to my cybersecurity analysis. Thus, in countries with a military approach, the referent object is the protection of critical infrastructures and of governmental digital resources. Countries implementing this approach are usually technologically advanced, have larger economies, and rely heavily on cyberspace. With this dependency comes vulnerability and maintaining critical cyber infrastructure is considered the main condition for maintaining national security. Conversely, there is no specific referent object identified by civil-oriented countries. These countries believe that cyberattackers are seeking immediate financial gain or seek to steal sensitive or provocative information. Since cyberthreats are closely linked to criminal acts, the main referent object varies from personal information to the proper functioning of information, economic, and social spheres, and other so-called soft sectors.

The second point made by the Copenhagen school is that the concept of security encompasses not only military, but also political, economic, and social aspects. Consequently, the *perception of threats* has also been expanded. Hence, in this article, it is important to analyse how countries perceive potential cyberattacks. Thus, states with a prevailing military approach—due to their heavy dependence on their *CI*—view cyber issues as matters of national security and include cyberwarfare in their military planning and organization. It is worth mentioning that dimensions of national cybersecurity were established when computer intrusions (a criminal act) were clustered together with more traditional and well-established espionage discourse. In this regard, civil-oriented countries perceive particular cyber issues as security risks for only a particular sector, such as financial, social, or private spheres.

According to the Copenhagen school, security discourse refers to the identification of the main *source of threat*. Although, the architecture of cyberspace makes it difficult to clearly determine who initiated a cyberattack, the military approach usually focuses on foreign governments and rogue non-state actors as the sources of threat, while the civil approach concentrates on hacktivism and cybercrimes as the main sources of threat. Consequently, countries with a prevailing civil approach are less likely to envision external threats to cybersecurity. The actors posing the greatest threats in countries with a civil approach may be in the business of stealing personal identities to commit fraud, a crime that in the inter-connected world of cyberspace, renders everyone a potential victim.

Another stage of the securitization process is the acceptance and legitimization of the *extraordinary measures* offered by the securitizing actor. Therefore, based on this logic, the active engagement of military institutions in cybersecurity policy creation and implementation could be seen as one such extraordinary measure undertaken by countries with a prevailing military approach. The so-called militarization of cyberspace refers to the growing pressures on governments to develop the capacity to fight and win wars in this domain (Deibert, 2011). Therefore, the militarization of cyber space shall be considered a result of the securitization process. When cyber space is perceived as a source of threats to national security, governments strengthen their capabilities to offensively fight these threats. Meanwhile, civil-oriented countries are more likely to respond to perceived cybersecurity threats with civilian capacities, structures, and instruments as cybersecurity issues ultimately fall within the remit of interior ministries and civilian agencies.

While cyberspace is not specifically addressed by Buzan, Weaver, et al., the securitization theory could serve as the theoretical framework for the analysis of civil and military approaches to cybersecurity, their relevant premises are demonstrated in Table 1.

TABLE 1. Presumptions of military and civil approaches

	Civil Approach	Military Approach
Referent security object	Private security, information and communications technology (ICT)	Critical infrastructure, ICT
Cyberattack perception	Criminal acts, security risks	National security threats
Sources of cyberthreats	Non-state actors, cybercriminals, hacktivists	Rogue states and non-state actors, cybercriminals, hacktivists
Institutions responsible for cybersecurity management	Interior ministries and civil agencies, etc.	Ministries of defence, other military agencies

2. OVERVIEW OF CYBERSECURITY STRATEGIES AND THE INSTITUTIONAL STRUCTURING OF CYBERSECURITY POLICIES

In the hierarchy of strategic documents, cybersecurity strategies are part of the national security or defence strategies and are connected to several other institutions' strategies due to the all-encompassing impact of cybersecurity on society as a whole. The main goal of this section is to provide an overview of cybersecurity strategies of seven selected countries and the institutions engaged in the implementation of cyber policy objectives.

2.1 Estonia

Estonia*'s* strategic documents on cybersecurity and its institutional structures for maintaining cybersecurity have contributed to its mature and comprehensive cybersecurity culture and policies. This is a country where strategic planning comes first, ensuring the cohesion of the entire cybersecurity architecture. In response to a series of extensive hacking attacks in 2007, Estonia, in 2008, became one of the first countries in the world to adopt a national cybersecurity strategy. The hacking episode Estonia faced in 2007 has been called the first cyberwar, raged as a politically motivated assault, on a country's digital infrastructure. After this "Cyber War I," Estonia's Ministry of Defence drafted a national cybersecurity strategy. Estonia has also published and launched *Digital Agenda 2020* to create an environment facilitating the use of ICT and the development of smart solutions (Digital Agenda 2020 for Estonia, 2013).

Estonia has the most extensive range of institutional cybersecurity policies in the Baltics. The responsibility for coordinating Estonia's cybersecurity policies overall was transferred from Estonia's Ministry of Defence (MOD) to its Ministry of Economic Affairs and Communications in 2011. As an interagency body, Estonia's Cyber Security Council of the Security Committee of the Government has been supporting strategic level interagency cooperation and overseeing the implementation of the country's cybersecurity strategy objectives. The Ministry of Defence is the coordinating authority for cyber defence in the area of national defence. In addition to the MOD, national cyber defence is supported by the Estonian Defence League's Cyber Defence Unit that includes cybersecurity professionals from both the public and private entities. Since 2008, Estonia's defence forces have also hosted the NATO Cooperative Cyber Defence Centre of Excellence—an international military organisation focusing on enhancing the cyber defence capabilities of NATO and its sponsoring nations.

2.2 Latvia

The *Cyber Security Strategy of Latvia for 2014-2018* was adopted in 2014 (Cyber Security Strategy of Latvia 2014-2018, 2014). The strategy highlights the ICT security incidents in Latvian cyberspace and predicts that the country may be subject to increased cybersecurity risks in the future (Cyber Security Strategy of Latvia 2014-2018: 2014). The strategy also appeals to the *Law on the Security of Information Technology* which determines basic security requirements for state, municipal institutions, and providers of public electronic communications services, as well as supervisors of critical ICT infrastructure. Both documents reflect an integrated approach to the protection of Latvia's cybersecurity and national security that prioritizes critical infrastructure and public services.

Latvia's elaborate and efficient institutionalization of its cybersecurity policies is well on the way to becoming a model system. Latvia's National Information Technology Security Council coordinates the development of national cybersecurity policies and the implementation of the policies' objectives and measures. The Council is the central national authority for the exchange of information and cooperation between the public and private sector and the Ministry of Defence coordinates the development and implementation of information technology security and cyberspace protection policies. Naturally, there are some other entities—such as other ministries and a computer emergency response team (CERT)—that also implement Latvia's cybersecurity policies.

2.3 Lithuania

Lithuania's management of cybersecurity threats has gone through a long evolution, starting from the creation of Lithuania's first institutions for dealing with cybersecurity, to the recent passing of an overarching law on cybersecurity (Butrimas, 2015).· Lithuania is the only country in the Baltic region that has not approved a national cybersecurity strategy. However, Lithuania's Seimas (parliament) approved a national security strategy, which declared cybersecurity a priority of national interest. In order to ensure the security of Lithuania's cyberspace, the Lithuanian government approved *The Programme for the Development of Electronic Information Security for 2011-2019*. The programme has three main objectives: 1) to strengthen the security of state-owned information resources; 20 to ensure that critical information infrastructure functions efficiently; and 3) to ensure the cybersecurity of Lithuania's citizens and residents and persons staying in Lithuania (Resolution Nr. 796, 2011). These objectives have been carried over to and further developed by Lithuania's law on cybersecurity, approved in 2014. The significant outcomes of this law include transferring of coordinating national cybersecurity policies to the Ministry of National Defence (MoND), the establishment of a new operational National Cybersecurity Centre (NCC) and the creation of an Advisory Council on Cybersecurity chaired by the MoND (Law on Cyber Security of the Republic of Lithuania, 2014).

2.4 Poland

Poland enacted a long list of comprehensive changes to its cyberspace defence system Poland and managed to publish and implement a cybersecurity strategy. Furthermore, cybersecurity also became an integral part of Poland's national security efforts and is frequently mentioned in other national strategic documents.

The cybersecurity issue in Poland's strategic documents was first mentioned in the *National Security Strategy of the Republic of Poland* in 2007. The document noted a direct relationship between cybersecurity and the country's ability to function properly (National Security Strategy of the Republic of Poland, 2007). Later, the *Strategy of Development of the National Security System of the Republic of Poland 2011-2022* detailed and developed the issues related to cyberspace protection in Poland (The Strategy of National Security of Poland, 2012). However, the first document dedicated solely to cybersecurity, *Cyberspace Protection Policy*, was not published until 2013 (Cyberspace Protection Policy of the Republic of Poland, 2013). In 2015, Poland's National Security Bureau (BBN) published a cybersecurity doctrine (Świątkowska, 2012). The document further lays out work to be completed in order to improve national security in the realm of cyberspace. The doctrine also maps out tasks for state institutions, notably for security agencies, the armed forces, the private sector, and NGOs (Doctrine of Cybersecurity of Poland, 2015). The National Security Bureau, functions as the main entity—together with the

Ministry of Administration and Digitisation, the Internal Security Agency, and CERT—responsible for achieving cybersecurity objectives.

2.5 The Czech Republic

The Czech National Strategy for Information Security approved in 2005 marks the Czech Republic's first attempt to regulate its national cyberspace (National Strategy for Information Security in the Slovak Republic, 2005). In 2011, the National Security Strategy identified cybersecurity as one of the main priorities of the Czech government and placed cyberthreats on the same security-threat level as regional conflicts, terrorism, and weapons of mass destruction (Security Strategy of the Czech Republic, 2011). In 2011 the Czech Republic approved its cyber security strategy and action plan for 2011 to 2015. The strategy primarily aimed to protect ICT systems in the Czech Republic and mitigate damage caused by cyberattacks (Cyber Security Strategy of the Czech Republic for years 2011-2015, 2011). In 2015, the Czech government approved its updated national cybersecurity strategy for 2015 to 2020. This strategy for the latter half of the decade includes a comprehensive set of measures that for achieving the highest possible level of cybersecurity (National Cyber Security Strategy of the Czech Republic for the Period from 2015 to 2020, 2015).

In the Czech Republic, civilian agencies are charged with implementing cybersecurity policy. The overall responsibility for national cybersecurity rests with the country's National Security Authority. The National Cyber Security Centre, an agency within the National Security Authority, is part of the country's national and international early warning system. Additionally, The Ministry of the Interior promotes cybersecurity issues at the political level while the Ministry of Defence only addresses cybersecurity issues cooperatively with NATO.

2.6 Slovakia

Slovakia developed a legal framework for cybersecurity in 2008 by adopting the *National Strategy for Information Security of the Slovak Republic* (NSIS) for 2009 to 2013. The strategy was drafted by the Ministry of Finance, Slovakia's agency responsible for securing unclassified public administration information. In 2012, Slovakia launched its *National Cybersecurity Strategy*. The strategy was accompanied by the Action Plan, a report on the tasks of the NSIS. Slovakia issued an information security plan for each year from 2009 to 2013.

Slovakia's National Security Authority manages classified information, while the Ministry of Finance manages the rest. Mutual communication is facilitated by the Ministry of Finance's Committee for Information Security, which has an advisory and coordinating role, preparing strategic and technical materials on information security. Some specific topics are supervised by the Security Council, the Ministry of Interior and the Ministry of Defence. Thus, the Ministry of Defence does not have a direct role in national cybersecurity management.

2.7 Hungary

In 2013, Hungary adopted a national cybersecurity strategy which expressly states that protecting Hungary's sovereignty in Hungarian cyberspace is a national interest (Government Decision on the National Cyber Security Strategy of Hungary, 2013). Being aware of the fact that threats and attacks emerging in cyberspace may escalate to a level requiring allied cooperation, Hungary considers it highly important that cybersecurity has become an issue for a collective defence under Article 5 of the founding treaty of NATO. It is also worthwhile to note that cyberthreats are also prioritized in Hungary's national security strategy adopted in 2012 (Government Decree on the Hungary's National Security Strategy, 2012).

The main agency responsible for the coordination and implementation of cyber-related policies in Hungary is the National Cybersecurity Coordination Council. Additional institutions charged with aspects of cybersecurity: the Cybersecurity Authority (an agency within the Ministry of National Development), The National Security Office (an agency within) the Ministry of Public Administration and Justice, and CERT (an agency within).

2.8 Cybersecurity strategies in the region overall

This overview of the national cybersecurity strategies in the seven countries examined reveals that the region's cybersecurity strategies are becoming integrated and comprehensive. The strategies approach cybersecurity in a holistic manner and encompass economic, social, legal, law-enforcement, military, and intelligence-related aspects of cybersecurity. Some strategies, such as those implemented in Slovakia and the Czech Republic, support a more flexible approach and emphasize the economic and personal (individual) dimensions of cybersecurity policy. Moreover, the Czech Republic, Slovakia and Hungary belong to a group of countries where civilian agencies are mainly in charge of ensuring cybersecurity. In this regard, cybersecurity in these countries can be described as civil-oriented. Military agencies are more active in coordinating and implementing cybersecurity policies in Estonia, Lithuania, Latvia, and Poland.

3. CYBERSECURITY AND ITS REFERENT OBJECTS

When using a securitization framework to analyse cyberspace defence, the referent object—that which is existentially threatened—is critical infrastructure. However, as Deibert and Saco have argued, cybersecurity is a terrain on which multiple discourses and (in)securities compete (Deibert, 2002; Saco, 1999). Therefore, discussions of cybersecurity hinge on competing ideas regarding cybersecurity's referent objects (Hansen and Nissenbaum, 2009). According to Hansen and Nissenbaum (2009: 1161), the key to understanding the potential magnitude of cyberthreats lies in acknowledging and understanding just how highly networked and integrated computer systems have become. These networks provide critical digital infrastructure: they regulate electricity, financial activities, energy use and even traffic patterns. These networks are identified as a collective referent object and are usually securitized first, since their damage would present a threat to national security.

The economic sector is also rich in referent objects including the private sector's fear of hackers' abilities to steal large sums of money and intellectual property owners' worries that file sharing compromises their rights and revenues (Hansen and Nissenbaum, 2009). In this regard, an individual approach to cybersecurity—stemming from cyber-libertarianism prioritizing personal (or individual) security—prevails.[1] As Hansen and Nissenbaum (2009: 1163) have argued, in private security discourse the individual is not a referent object, instead the individual is linked to societal and political referent objects. In other words, cyber privacy defence has to be mediated through a collective referent object, either a political-ideological one—prompting questions regarding an appropriate individual-state balance—or a national-societal one, which would mobilize values core to community identity. Similarly, securing critical infrastructure cannot stop at the infrastructure itself: the implications of a network breakdown imply other referent objects: society, the regime, and the economy (Hansen and Nissenbaum, 2009). In order to link a theoretical perspective on the variety of referent objects with a study of cybersecurity in the Baltic states and Visegrad countries, requires an analysis of the referent objects identified by the states themselves.

All seven countries acknowledge a link between the cyber- and national security sectors and are aware that cybersecurity issues—such as the destruction of the ICT system or critical infrastructure—can damage national security, adversely impact citizens' lives, and threaten the assets and the proper functioning of the national economy and public services. Consequently, a collective security discourse prevails in all seven countries' strategic documents. However, the countries—such as Estonia, Poland, Latvia, Lithuania and to some degree, the Czech Republic—that articulate a strong need to intensively defend their cyberspaces also present, as reflected in their strategic documents, more comprehensive and clearer visions of their main referent objects. For instance, Lithuania's national security strategy emphasizes the importance of ensuring the security of informational, economic, and social infrastructure as the key objective of national security policy (National security strategy of the Republic of Lithuania, 2012). Meanwhile, the national cybersecurity strategy of the Czech Republic mainly prioritizes the protection of information infrastructure essential to Czech economic and social interests (Cyber security strategy of the Czech Republic for years 2011-2015, 2011); it also focuses on the protection of rights of internet users. However, the Czech Republic's national security strategy presents a more comprehensive concept of critical infrastructure and its vulnerabilities coming from cyberspace than its national cybersecurity strategy does. The national security document states that critical infrastructure as a whole is exposed to a number of threats with natural, technological, and asymmetric aspects. Examples of such threats include cyberattacks, economic crime, and sabotage among others (Cyber security strategy of the Czech Republic for years 2011-2015, 2011). In other words, countries which are keen on securitizing their cyberspace, are more likely to prioritize the safety of critical infrastructure as a key condition of national security. Because national security is linked to critical infrastructure as the referent object, the actors with power to identify objects that require security and defence may claim the right to use extraordinary means in the name of security. For example, Poland's cybersecurity doctrine emphasizes the importance of critical infrastructure and a direct relationship between

[1] More information on cyber-libertarianism can be found for example here: Hofman, J.,''The Libertarian Origins of Cybercrime: Unintended Side-Effects of a Political Utopia''. Centre for analysis of risk and regulation at the London School of Economics and Political Science, 2010. http://www.lse.ac.uk/accounting/CARR/pdf/dps/disspaper62.pdf

cybersecurity and the country's proper functioning, including its economic development and the ability to operate effectively in the military sphere (Cyber security doctrine of the Republic of Poland, 2015). What is more, Poland is the only country which is willing to develop not only defensive but also offensive cyber capabilities in order to deter potential opponents in cyberspace (National security strategy of the Republic of Poland, 2012). Thus, Poland's approach reveals that the more articulated the process of identifying and defending against cyberthreats is, the more militarized it becomes.

On the other hand, countries such as Hungary and Slovakia, also mention critical digital infrastructure as a referent object. However, these countries do not view potential attacks on critical infrastructure as a threat to national survival, as cybersecurity in these two countries is thought to be just one of several national security sectors. Hungary and Slovakia focus mainly on information security. The objectives of Slovakia's information security strategy focus on protecting human rights and freedom, improving information security management, and defending state ICT in order to support the state's critical infrastructure (National strategy for information security in the Slovak Republic, 2008). The concept of referent objects in Hungary's cybersecurity strategy remains even more ambivalent, it lacks any direct reference to primary referent objects. The strategy only mentions protecting national data assets and the "operational safety of the parts of its critical infrastructures linked to cyberspace." (Government decision on the National cyber security strategy of Hungary, 2013). Neither Slovakia nor Hungary identify a specific referent object that should be protected first within cybersecurity, as a consequence both countries have a decidedly civil approach to cybersecurity.

4. PERCEPTIONS OF CYBERTHREATS

The securitization of cyber issues is based on different discourses, most commonly in national security discourse. Therefore, cyber issues usually arise when agents, such as foreign governments or non-state actors, with rogue intentions attempt to gain access to financial, energy, or public-safety systems and the prospect of cyberattacks is presented as a threat that requires an urgent response. Perceiving and presenting cyberattacks in this manner leads to intense security measures. Consequently, in countries where a national security discourse prevails, the threat of cyberattacks are regarded as a top priority and there is a military approach to cybersecurity.

However, threats to cyber- and national security do not arise from external sources alone. Hence, cyberattacks can also arise from systematic threats. These systemic threats, defined by Hundley as ''cyberspace safety'' stem from the inherent unpredictability of computers and information systems, which ''create unintended (potentially or actually) dangerous situations for themselves or for the physical and human environments in which they are embedded'' (Anderson and Hearn, 1996). A more common issue, however, is intentionally provoked systematic threat invoked by criminal syndicates or individuals. In this regard, technical discourse is accompanied with a criminal one and is linked to cybersecurity discourse. In this discourse, cybersecurity can, in short, be seen as safeguarding computers from criminal activity and cyberattacks are perceived not as national security threats, but as common risks in the cyber sector. Consequently, countries that perceive potential cyberattacks as a risk for a particular sector are less keen to define cyber issues as issues of national security and can be identified as civil-oriented states.

Poland, Latvia, Lithuania, Estonia, and the Czech Republic have a multi-layered approach to cyberattacks. First, they evaluate risks to their national security and task state institutions with preventing cyberattacks. Secondly, they identify cyber-related challenges to the integral components of their national security: the economic, financial, and private sectors. This comprehensive approach to cyberattacks is reflected in Estonia's cybersecurity strategy. Estonia claims that it has a growing number of state actors tasked with countering cyber espionage and protecting both internet-connected and closed networks, with the additional aim of collecting information on security and economic interests (Cyber Security Strategy of Estonia 2014–2017, 2014). National security is also the prevailing discourse in Poland's cybersecurity doctrine. The cyberthreats identified in Poland's doctrine include attacks against telecommunications systems important to national security, and cybercrime—specific cybercrimes mentioned in the doctrine include "cyber violence, destructive cyber protests and cyber demonstrations," data and identity theft, and private computer hijacks (Cyber Security Doctrine of the Republic of Poland, 2015). The same discourse is seen in Lithuania and Latvia's strategic documents. For example, Lithuania's state defence concept groups cyberattacks as a national threat together with terrorism and organised criminal activities (The State Defence Concept of the Republic of Latvia, 2012). It is worth mentioning that Latvia's newest national security concept highlights cyberattacks as one of eight primary national security threats (Press release, 2015).

The four countries mentioned above have a comprehensive approach to cybersecurity based on precise evaluations of the potential impact of cyberattacks on different sectors and on national security overall. Since the cyberattacks are perceived mainly as threats to national security, these countries have responded with a military approach.

Slovakia's updated cybersecurity concept for 2015 to 2020 also presents a complex perception of cybersecurity. Slovakia claims that cybersecurity should not be seen as an isolated problem of the Slovak Republic or as an issue isolated to one or even several sectors and that, due to its global nature, cybersecurity is a society-wide phenomenon (Cyber Security Concept of Slovak Republic for 2015–2020, 2015). The document also identifies the core problem of Slovakia's cybersecurity policy: that cyberthreats are not generally seen as a sufficiently urgent problem and are not explicitly or validly addressed in Slovak law (Cyber Security Concept of Slovak Republic for 2015–2020, 2015). While this document is instrumental in its nature, as it offers a model for managing cybersecurity policies, it lacks a complete vision of cybersecurity challenges. As a result, potential cyberattacks are seen mainly as risks to unnamed targets.

The strategy of the Czech Republic mentions risks such as cyberespionage (industrial, military, political, or other), organized crime in cyberspace, hacktivism, intentional disinformation campaigns with political or military objectives, and even—in the future—cyberterrorism (Cyber security strategy of the Czech Republic for the 2011-2015 period, 2011). These risks are seen mainly as dangerous tendencies in the global cyberspace that have not yet threatened Czech society. The security discourse that prevails in the strategic documents of the Czech Republic mainly refers to systematic threats and "computer safety." In this regard, the Czech Republic's cybersecurity strategy focuses mainly on building a credible information society by safeguarding access to services, protecting data integrity, and promoting the confidentiality of the Czech Republic's cyberspaces (Cyber security strategy of the Czech Republic for the 2011-2015 period, 2011). Meanwhile, Hungary also emphasizes the criminal element of cyberattacks. Thus, Hungary claims that dynamically developing new technologies, like cloud computing and mobile internet, lead to the continuous emergence of new security risks, such as illegal acquisitions of critical information and personal data (Government decision on National cyber security strategy of Hungary, 2013). Moreover, Hungary avoids identifying cybersecurity challenges with threats. It prefers to name cyberthreats as risks to the cyber sector.

The perceptions of cyberthreats and cybersecurity in general, determine the civil approach to cybersecurity management that prevails in the Czech Republic, Slovakia, and Hungary.

5. SOURCES OF CYBERTHREATS

The cyberspace's architecture facilitates anonymity and hinders attempts to track the sources of cyberattacks, constituting an additional factor of insecurity. Nevertheless, it is possible to analyse the sources of cyberattacks and cyberattackers, who may operate as functional actors. The logic of such analysis would be similar to what representatives of the Copenhagen school sketch out in analysing the pollution of the environment: these actors directly influence the dynamic of the cyber sector, but they are neither referent objects nor securitizing actors, though they may contribute to actions that impact the perception of the threat (Buzan, Wæver, and de Wilde, 1998). In a civil-military dichotomy, external cyberthreats such as foreign states or non-state actors, including cyberterrorists and cyberespionage agents, clash with internal actors: hacktivists,cybercriminals, malware authors, cyber scammers and corporations. As mentioned previously, countries that are actively securing their cyberspaces, emphasize the political motivation of cyberattacks and external cyberthreats. This attitude dictates a military approach to cybersecurity management as the most effective. Conversely, focusing mainly on internal cybersecurity threats means that the main referent object is the economic sector or private data. To fight these threats, a civil approach to cybersecurity policy is thought to be sufficient.

Further analysis of how the sources of cyberthreats are understood by particular countries brings us to the conclusion that all countries acknowledge that there are many actors in cyberspace; however, only a few states make a distinction between nature, objectives, and methods of these actors. For example, Estonia's cybersecurity strategy claims that national cybersecurity is affected by the actors operating in cyberspace with various skills, targets, and motivations and that cybersespionage—with the intent to collect national security and economic information—is increasing. Estonia's strategy also emphasizes that the number of states capable of and actually initiating cyberattacks is increasing (Cyber security strategy of Estonia 2014-2017, 2014). This distinction between internal and external threats is also made in the Polish doctrine. External threats listed by the doctrine include cyber crises, cyber conflicts, cyberwar, and cyberespionage involving states and other entities, "threats (for Poland) coming from cyberspace include extremist, terrorist and international criminal organizations whose attacks in cyberspace can have ideological, political, religious, business or criminal motivations." (Cyber security doctrine of the Republic of Poland, 2015).

Lithuania and Latvia, in contrast, haven't identified specific cyberattackers, but their strategic documents refer primarily to external threats, such as neighbouring countries. Meanwhile, both Slovakia and Hungary have quite a blurred and fragmental vision on the sources of cyberthreats. For example, Hungary focuses on technological (internal) vulnerabilities and their effects to the proper functioning of the state's economy without any deeper analysis of their causes and actors engaged into the process. The cybersecurity strategy of Hungary states that 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." (Government decision on National cyber security strategy of Hungary, 2013). The civil approach to the sources of cyber threats is also common to the Czech Republic. The National Security Strategy of the Czech Republic identifies a wide range of potential cyber challenges, however, almost all of them are criminal or technological in nature. These are hackers stealing personal or sensitive data, technological failures, botnets and DDoS/DoS attacks etc.

The perception of cyber threats is closely linked to the sources of the perceived threats. The more securitized a view of cyber threat prevails, the more precisely the source of a threat is identified. What is more, countries that securitize cyber threats, such as Estonia, Poland, Lithuania, and Latvia, make a distinction between external and internal cyberspace actors. Meanwhile, countries that emphasize the criminal element of cyberthreats think about them as internal challenges and limitations of cyberspace. It is noteworthy that almost all of the analysed countries make a distinction between internal and external sources of cyber threats in their strategic documents. However, the countries that are described as civil-oriented are not keen on elaborating this distinction further and focus mainly on internal threat sources as the most common and probable in their security environment.

CONCLUSIONS

The qualitative analysis of the cybersecurity policies of the four Visegrad countries and the three Baltic states shows that each of these countries have cybersecurity strategies and corresponding laws to address cybersecurity issues. All of the documents analysed refer to higher-level national security or defence strategies and present the legislative environment, although there are significant differences in their profundity. Different cyberspace entities and the potential threats these entities generate are also addressed in the documents. In most national cyberspace security strategies, threats to critical infrastructure and cybercrime play a prominent role and indicate increasing economic damage wrought by cyberattacks. In the formal sense, the domain of cyberspace is already included in the security agendas of all states and could be called "securitized."

However, there are differences of securitization among countries. Cybersecurity differs by how countries: 1) define a referent object (what should be protected); 2) perceive primary threats and risks; and 3) identify the sources of threats and risks. In accordance with these differences, countries can be classified into two categories. The first category, that of countries that militarize cybersecurity issues, includes Poland, Estonia, Lithuania, and, to some degree, Latvia. These countries that have militarized cybersecurity discourse are more precise in identifying specific referent objects and in articulating the defence of these objects as national priorities. This tendency elevates cybersecurity to the highest national security level and focuses on safeguarding ICT and governmental information resources. Poland, Estonia, and Lithuania tend to identify cybersecurity challenges as threats to the proper functioning of the state, and identify attacks from foreign states as the most dangerous sources of such threats. Consequently, in these states, the responsibility of responding to cyberthreats is handed over to military and defence institutions (Table 2).

The second category of securitization discourse refers to the criminalization of cybersecurity issues. The Czech Republic, Slovakia, and Hungary rely on a civil approach to maintain cybersecurity. Their referent objects are diffused and mainly related to the proper functioning of the state's economic system and private property. The ICT and governmental digital resources have no priority over other legitimate referent objects. As a result, countries with a prevailing

TABLE 2. Civil and military approaches in the states' cybersecurity policies

	Referent Object	Cyber Attack Perception	Threat Source	Institutions	Militarization/ Criminalization
Hungary	Digital informational infrastructure	Risk to national cybersecurity	Internal technological vulnerabilities	Civil	Criminalization approach prevails
Czech Republic	Critical & informational infrastructure; rights of internet users	General risk of a global cyberspace	Internal technological vulnerabilities	Civil	Criminalization approach prevails with military elements
Slovakia	Digital informational infrastructure, human Rights & freedoms	Risk to the national cybersecurity	Internal technological vulnerabilities	Civil	Criminalization approach prevails
Poland	Critical & informational infrastructure	National threat	External & internal actors	Military	Militarization approach prevails
Lithuania	Informational, Economic & Social/ Critical Infrastructure	National threat	Usually external actors	Military	Militarization approach prevails
Latvia	Critical & Informational Infrastructure	National Threat	Usually external actors, neighbouring countries	Military	Militarization approach prevails with criminal elements
Estonia	Critical & Informational Infrastructure	Threat to economic, political & other sectors	E External & internal actors	Extensively militarized	Militarization approach prevails

civil approach are mostly concerned with criminal activity conducted in cyberspace and describe cybersecurity issues as “risks”. Potential sources of such risks are also fragmented and include not only external international actors, but also internal actors such as hackers, hacktivists, criminal organisations, and even the unintentional disruption of networks. Civil institutions in the Czech Republic, Slovakia, and Hungary are charged with monitoring cybersecurity risks and coordinating state response to cyber incidents (Table 2).

The conclusions of this article, the categorisation of cybersecurity approaches as civil or militarized may lead to a better understanding of cybersecurity as a phenomenon. It could contribute to the explanation of obstacles for cooperation between states dealing with cybersecurity issues on the international level. Furthermore, the identification of different approaches to cybersecurity could explain specific state‘s actions in cyberspace. Understanding states’ differences in perceiving cyberthreats, referent objects, and potential adversaries constitutes a background to discussions of the so-called cyber-identities of states and non-governmental actors. This could be a useful theoretical tool for analysing potential cyber conflicts and cooperation patterns in further studies.

REFERENCES

Anderson R.H., Hearn A.C., 1996. *An Exploration of Cyberspace Security R&D Investment Strategies for DARPA: ‘‘The Day After … in Cyberspace II’’*. Santa Monica: RAND.

Buzan B., Wæver O., de Wilde J., 1998. *Security- A New Framework for Analysis*, London: Lynne Rienner.

Deibert, R., 2002. ‘‘Circuits of Power: Security in the Internet Environment‘‘. In *Information Technologies and Global Politics: The Changing Scope of Power and Governance* edited by J., N. Rosenau, and J. P. Singh. Albany: State University of New York.

Deibert, R., 2011. ‘‘Tracking the emerging arms race in cyberspace‘‘. *Bulletin of the Atomic Scientists* vol. 67, 1-8.

Dunn Cavelty M., 2013. ’’From Cyber-Bomb to Political Fallout: Threat Representations with an Impact in the Cybersecurity Discourse’’. *International Studies Review*, 15(1), 105-122.

Hansen L., Nissenbaum H., 2009. ‘‘Digital Disaster, Cyber Security, and the Copenhagen School‘‘. *International Studies Quarterly* no. 5 3: 1155–1175. Available at <https://www.nyu.edu/projects/nissenbaum/papers/digital%20disaster.pdf> [Accessed 23 January, 2016].

Harnett R. J., Stever J., 2009. ‘‘The Cybersecurity Triad: Government, Private Sector Partners and the Engaged Cybersecurity Citizens‘‘. *Journal of Homeland Security and Emergency Management*, 6 (1), Art. 79.

Hofman J., 2010. ‘‘The Libertarian Origins of Cybercrime: Unintended Side-Effects of a Political Utopia‘‘. Centre for analysis of risk and regulation at the London School of Economics and Political Science. Available at <http://www.lse.ac.uk/accounting/CARR/pdf/dps/disspaper62.pdf>

Lobato. C. L., Kenkel K.M., 2015. “Discourses of cyberspace securitization in Brazil and in the United States.” Rev. Bras. *Polít. Int.* 58 (2): 23-43. Available at <http://www.scielo.br/pdf/rbpi/v58n2/0034-7329-rbpi-58-02-00023.pdf> [Accessed 1 December, 2015]

Moore J., 2010. The Economics of Cybersecurity: Principles and Policy Options. In *International Journal of Critical Infrastructure Protection*, 3 (3-4), 103-117, 2010.

Newmeyer K. P., 2015. ‘‘Elements of National Cybersecurity Strategy for Developing Nations‘‘. In *National Cybersecurity Institue Journal*, Vol.1 No.3. Available at <http://www.excelsior.edu/static/journals/nci-journal/1-3/offline/download.pdf> [Accessed 2 February, 2016].

Saco D., 1999. ‘‘Colonizing Cyberspace: ‘‘National Security’’ and the Internet‘‘. In *Cultures of Insecurity: States, Communities, and the Production of Danger* edited by J. Weldes, Mark Laffey, Hugh Gusterson and Raymond Duvall. Minneapolis: University of Minnesota Press.

Świątkowska J., 2012. “Cyberthreats as a Challenge to the Security of the Contemporary World”. *V4 Cooperation in Ensuring Cyber Security – Analysis and Recommendations* Ed. J. Świątkowska. The Kosciuszko Institute, 2012. Available at <http://pasos.org/wp-content/uploads/2012/08/kosciuszko_institute_v4_cybersec_062012.pdf> [Accessed 12 March, 2016].

National security documents:

Cyber Security Strategy of the Czech Republic for years 2011-2015, 2011, Government of the Czech Republic, Available at <www.govcert.cz/ViewFile. aspx?docid=21667315>. [Accessed 13 December, 2015].

Cyber Security Strategy of Latvia 2014-2018. Available at <https://www.unodc.org/res/cld/lessonslearned/lva/cyber_security_strategy_of_latvia_20142018_html/Cyber_Security_Strategy_of_Latvia.pdf.> [Accessed 13 December, 2015].

Cyberspace Protection Policy of the Republic of Poland, 2013. Available at<https://www.unodc.org/cld/lessonslearned/pol/cyberspace_protection_policy_of_the_republic_of_poland.html?&tmpl=cyb>. [Accessed 20 December, 2015].

Estonian Ministry of Economic Affairs and Communications, Digital Agenda 2020 for Estonia, 2013. Available at <https://e-estonia.com/wp-content/uploads/2014/04/Digital-Agenda-2020_Estonia_ENG.pdf.> [Accessed 22 December, 2015]

Government 29 June 2011 Resolution Nr. 796. II-(6.1-6.3) Elektroninės informacijos saugos (kibernetinio saugumo) plėtros 2011–2019 metais programą. (The Programme for the Development of Electronic Information Security (CyberSecurity) for 2011–2019). Available at <ttp://www3.lrs.lt/pls/inter3/dokpaieska.showdoc_l?p_id=403385> [Accessed 20 January, 2016].

Government Decision No. 1139/2013 (21 March) on the National Cyber Security Strategy of Hungary. Available at <https://www.unodc.org/res/cld/lessonslearned/national_cyber_security_strategy_of_hungary_html/National_Cyber_Security_Strategy_of_Hungary.pdf> [Accessed 20 March, 2016].1035/2012

(21 March) Government Decree on the Hungary's National Security Strategy. Available at <http://www.mfa.gov.hu/NR/rdonlyres/61FB6933-AE6747F8BDD3ECB1D9ADA7A1/0/national_security_strategy.pdf> [Accessed 20 March, 2016].

Lietuvos Respublikos Kibernetinio saugumo įstatymas, XII-1428, 2014 (Law on Cyber Security of the Republic of Lithuania). Available at <http://www3.lrs.lt/pls/inter3/dokpaieska.showdoc_l?p_id=492070&p_tr2=2.> [Accessed 2 April, 2016].

National Cyber Security Strategy of the Czech Republic for the Period from 2015 to 2020. Available at <https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/CzechRepublic_Cyber_Security_Strategy.pdf.> [Accessed 2 April, 2016].National Security Strategy of the Republic of Poland, Warszawa 2007. Available at <http://www.defesa.gov.br/projetosweb/livrobranco/arquivos/pdf/Polônia%202007.pdf> [Accessed 15 November, 2015].

National Strategy for Information Security in the Slovak Republic (2005). Available at <https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/Slovakia_National_Strategy_for_ISEC.pdf> [Accessed 15 November, 2015].

Security Strategy of the Czech Republic (2011). Available at http://www.army.cz/images/id_8001_9000/8503/Czech_Security_Strategy_2011.pdf> [Accessed 25 October, 2015].

Strategia Rozwoju Systemu Bezpieczeństwa Narodowego RP 2012-2022. (The Strategy of National Security of Poland) Available at <http://mon.gov.pl/z/pliki/dokumenty/rozne/2013/09/SRSBN_RP_przyjeta090413.pdf> [Accessed 20 October, 2016]

Other sources:

The Cyber Index. International Security Trends and Realities. UNIDIR, United Nations Institute for Disarmament Research. 2013. http:// Available at <https://www.nyu.edu/projects/nissenbaum/papers/digital%20disaster.pdf> [Accessed 15 March, 2016].

ENISA, National Cyber Security Strategies, Practical Guide on Development and Execution, 2012. Available at <file:///C:/Users/User/Downloads/ENISA%20Guidebook%20on%20National%20Cyber%20Security%20Strategies_Final.pdf> [Accessed 25 May, 2016]