CEPI | CENTRAL EUROPEAN POLICY INSTITUTE
BRATISLAVA - BUDAPEST - PRAGUE - WARSAW

POLICY BRIEF

NOVEMBER 2013

# PROTECTING CYBERSPACE IN THE V4: TOWARDS IMPLEMENTATION OF THE EU'S CYBER-SECURITY STRATEGY

JOZEF VYSKOČ, ZSOLT ILESI,
JOANNA ŚWIĄTKOWSKA, TOMÁŠ REZEK

## INTRODUCTION

The Internet and cyberspace more broadly has become vital to our society – economies, citizens' daily life and social interactions all depend on the flawless working of information and communication technology (ICT) systems. Given its importance, cyberspace also needs to be protected from incidents, malicious activities and misuse. The borderless nature of cyberspace implies that broad international collaboration is necessary in order to ensure safety and security within such an environment. The Proposal for the Cybersecurity Strategy of the European Union ("Strategy") and accompanying Proposal for the Directive of the European Parliament and of the Council ("Directive") reflect the need to secure the EU'scyber-space from malicious activities, incidents and misuse. While the Strategy outlines the overall EU vision, strategic priorities and actions as well as the roles and responsibilities of the member states and relevant institutions, the Directive aims at ensuring that all the member-states have a minimum level of national capabilities in place to deal with security challenges in cyberspace.

This policy brief explains which threats the Strategy is aimed at and what the Visegrad countries need to do to implement it.

## CYBER THREATS

Due to the complexity of the ICT used today, the existence of a rich variety of "technical-in-nature" cyber- attacks is not surprising. One that is often cited as typical is the "distributed denial of service" (DDoS) attack, famous for its use against Estonian websites in 2007. But this represents just one of a whole spectrum of possible attacks.

## ABOUT CEPI

The Central European Policy Institute (CEPI), a member of the Strategy Group, is a regional think-tank based in Bratislava.

Our mission is to help decision-makers and opinion-makers in Central Europe to craft common responses to current challenges, and to improve the quality of their contributions to the EU and NATO debates, since we believe that Central Europe should take on more responsibility for issues ranging from the economic crisis to energy and security and thus to boost the region's standing in the eyes of other member-states.

It does so by engaging the region's top experts and institutions, promoting innovative solutions, and working closely with governments to turn recommendations into policy.

This document was elaborated in the framework of the "Cyber Security in the Visegrad Region (CSV4)" project supported by the International Visegrad Fund.

Visegrad Fund

SAC SLOVAK ATLANTIC COMMISSION | 20 YEARS of VISION, DEDICATION and COMMITMENT SLOVAK ATLANTIC COMMISSION

On the other side of the spectrum are new forms of state-sponsored cyber-threats, actively attacking the information systems of nuclear power plants and other critical infrastructures or even "hacking" NATO and governmental organisations, including those of the Visegrad states.

Technical details and media visibility aside, a DDoS attack is a nuisance more than a threat – its key result is a loss of convenience as some services are not available through the Internet. Potentially more disastrous are attacks aimed at the trust our societies rely on – trust in the correct operation of important systems or in certain institutions – especially if such attacks are not immediately detected.

Consider, for example, the following scenarios:

- As the result of a successful attack, crucial state information systems (for instance those used by the tax administration) cannot be trusted to provide complete, authentic and reliable data – at least until detailed forensic analysis (which may take weeks) reveals what actually happened in the attacked system, how long its users worked with untrusted data, and whether and how the damaging actions can be reversed or corrected.

- Due to advances in cryptology it turns out that cryptographic protection of modern national electronic identification cards (e-ID cards) is no longer strong enough, resulting in diminished trust in them as a simple and reliable proof of an individual's identity. Producing false e-ID cards becomes significantly easier than previously thought.

- The trustworthiness of a national e-health system (eg the integrity or authenticity of its data or its ability to protect the privacy of citizens) is convincingly challenged.

- Social networks are used to spread misinformation or disinformation related to a state institution, important activity or document under preparation at a speed and with a range that cannot be contained.

Since the loss of trust can take just a few minutes, it is very important to know how to handle the resulting crisis. The technical nature of DDoS attacks should not entice bureaucrats and decision-makers to leave the management of cyber-situations solely to IT specialists, for they are not ready for the crises elicited by less technical cyber-threats. For example, just a few days before the start of the 2011 census in Slovakia, misinformation was posted on the Internet alleging that census data was not anonymous and that there was a conflict with the data protection act. The false allegations quickly spread through social networks, but the authority that managed the census was caught unprepared for such a situation. As a result citizens' fears were not properly and quickly dealt with. The resulting loss of trust in the fair and trustworthy processing of census data led to numerous individual misrepresentations and even serious local disruptions of the process. It shows how vulnerable modern societies are to misinformation or disinformation spread within cyberspace and how important it is to prepare for a crisis properly.

Intentional cyber-attacks are a serious threat for modern societies, but they are not the only challenge to the integrity and proper operation of vital ICT systems. Their own instability – stemming from flaws in development, deployment and operation, as well as from the complexity and often unpredictability of interactions between different parts of cyberspace – can create comparable damage. Responsible authorities need to pay appropriate attention to the system architecture, development of code, testing, deployment and regular updates, even if that takes time and requires additional investments from the public budget. If key ICT systems are to bring cost-savings in the long term, they need to be properly funded at the beginning and well-designed.

## European Strategy

In spite of the general progress in the field of cyber-security in the EU, individual initiatives at the national level are insufficient. The level of member states' preparedness varies significantly, and there is a lack of the kind of co-operation mechanisms that are needed in the case of a major incident.

European cyberspace represents a highly interconnected system, where the least secure element can bring down all parts: a problem in one country can quickly spill over to others. Lack of harmonisation is not only detrimental to security but also to the internal market, since it is tempting to avoid problems by disconnecting from the dangerous parts of cyberspace.

The EU has therefore decided to adopt common regulations with its new cyber-security strategy, entitled "An Open, Safe and Secure Cyberspace". The document defines a vision of how the EU and its members should secure cyberspace and includes a set of short- and long-term initiatives and instruments.

The Strategy lists five strategic priorities: to achieve cyber-resilience, drastically reduce cyber-crime, develop a cyber-defence policy and capabilities related to the Common Security and Defence Policy, develop industrial and technological resources for cyber- security and establish a coherent international cyberspace policy for the EU.

The key element for implementation of the Strategy is the Directive, which aims at ensuring a high common level of network and information security (NIS). The most important provisions of the proposed Directive involve the obligation of member states to establish a minimum level of national capabilities, defined as adopting a basic national strategic framework for cyber security (Article 5), establishing a body responsible for implementation of the strategy (Article 6), and having a specialised national unit, known as a Computer Emergency Response Team (CERT), to deal with security incidents (Article 7).

Last but not least, the Directive requires key private players and public administration entities to adopt appropriate and proportionate measures to ensure NIS. These entities will also be obligated to report to the authorities all incidents which severely endanger their networks and information systems and which could also disrupt continuity of service delivery and the supply of critically important products.

## VISEGRAD COUNTRIES

At the first sight, the Visegrad countries score quite well on their level of national capabilities. They have already adopted cyber-security-related strategic documents, assigned responsibility for managing cyber-security activities to a specified body, and established specialised units to deal with security incidents. On closer inspection, however, it is clear that merely complying with these formal requirements is not enough to secure cyberspace.

Firstly, existing Visegrad 4 national strategies focus solely on national institutions and procedures, while the European one stresses the importance of international collaboration. Not even the basic cyber-security-related terminology is harmonised. For example, the Slovak national strategy uses the term "digital space" instead of cyberspace, and further adds to the confusion by explicitly affiliating the term cyberspace with classified information and systems only. Also, these documents seem to be based on the assumption that only tight control can ensure security in cyberspace. Consequently, they are focused almost exclusively on government and public administration systems.

Secondly, except in the Czech Republic, the authorities responsible for implementation of the national strategy are existing governmental bodies, rather than specialised organisations, with proper cyber-security-related skills and the ability to focus fully on the issue.

Thirdly, all Visegrad countries have specialised CERT units to deal with security incidents and these have established a certain level of international collaboration, thus being in line with what the Directive expects. There are, however, serious discrepancies between the Directive's requirements and the actual capabilities of the Visegrad countries' CERTs, the most visible being the inability to fulfil the non-stop stand-by regime requirement. As of now, availability is ensured only during standard office hours on working days.

## What needs to be done

To attain at least a minimum level of national capabilities necessary to deal with security challenges in cyber-space, the Visegrad governments need to consider the following shifts in approach:

### Providing security beyond public ICT systems

The kind of direct control applied in the tightly closed cyber-environments of public institutions allows for the straightforward enforcement of protection measures adopted by the state, but is not executable beyond its high walls. Indirect measures therefore need to be considered, such as mandatory reporting of security incidents which motivates private-sector organisations to enhance the security of their ICT systems properly if they are not to risk embarrassment.

### Pooling and sharing existing expertise

Cyber threats cannot be confined to state borders, so the current national approach needs to be internationalised, allowing countries to leverage a broader range of skills and capacities. There is enough technical expertise available in the Visegrad countries to deal with routine issues. More scarce are the advanced qualities and skills needed to handle major cyber incidents, which require a thorough analysis of the attacked systems in order to understand the genetic code of an attack and foresee possible related threats. In addition, countries need to permanently analyse all available information and identify trends in various cyber-security fields. That requires possession of a variety of highly specialised expert skills, which need to be always at their disposal. Close international co-operation – especially the pooling and sharing of existing capacities, as well as certain specialisations – may help to overcome a shared lack of expertise in specific fields.

### Going beyond the technical approach

Since the tools of attack are developing every day, it is important to analyse the threats from a broader perspective, reflecting on who the perpetrators of malicious actions are and what is motivating them. As succinctly expressed by the adage "Amateurs hack systems, professionals hack people", technical measures need to be combined with more political actions.

### Addressing strategy shortfalls

The Strategy and the Directive avoid going into too much detail. It is the responsibility of the national authorities to prepare detailed legislative adjustments and appropriate standards to improve the level of cyber-security. Nevertheless, they need to be cautious because over-harsh measures and imperfectly designed processes can jeopardise the final result. Inappropriate security measures can result in higher costs for many companies, while badly set-up processes can diminish trust among stakeholders, reducing their willingness to share information on cyber-security incidents. Discrepancies between member-states' requirements and approaches to implementation can result in unequal costs, favouring foreign operators at the expense of local companies, and cause disharmony in the EU market. Therefore adequate due diligence and dialogue with all stakeholders on both a national and European level should take place to minimise possible risks related to the implementation of the Directive.

## Conclusion

By proposing its newest initiatives the EU urges the member states to be more engaged in the protection of cyber-space. It is important to ensure the quality of national measures rather than implementing the EU requirements only formally. Co-operation among the Visegrad countries during the period of the Directive implementation will improve the compatibility of their legal and operational environments and help them build a homogenous market. Such an approach will prepare good foundations for further negotiations at the EU level.

***Jozef Vyskoč*** *is Associate Fellow at the Central European Policy Institute;* ***Zsolt Illési*** *is associate professor at the College of Dunaújváros;* ***Joanna Świątkowska*** *is security and defence expert at the Kosciuszko Institute;* ***Tomáš Rezek*** *is research fellow at Prague-based Association of International Affairs (AMO) Research Center.*

Disclaimer: The views and opinions expressed herein are those of the author and do not necessarily reflect those of his employer or of the publisher. This document was elaborated in the framework of the "Cyber Security in the Visegrad Region (CSV4)" project supported by the **International Visegrad Fund**.