NATIONAL CYBERSECURITY STRATEGIES IN MEMBER STATES OF THE EUROPEAN UNION

Prof. DSc ***Sevdalina Dimitrova,***
„Vasil Levbski" National Military University of Veliko Turnovo, Bulgaria

Prof. Dr. ***Stoyko Stoykov,***
„Vasil Levbski" National Military University of Veliko Turnovo, Bulgaria

Dr. ***Yosif Kochev,***
«Neophyte Rilski» Southwestern University of Blagoevgard, Bulgaria

I Introduction

Searching for solutions to the problems related to cybersecurity which occurred in the early 1990s, with their steadily increasing negative effects, has long gone beyond the borders of a single science and hence requires a complex interdisciplinary approach.

The new challenges facing the international community and the information and communication technologies cross the national borders and the individual countries fail to deal independently and effectively with the new threats against cybersecurity only by policies at national level aiming at ensuring a high level of protection of its citizens and the networks of state power.

The need for collective efforts to protect cyberspace has increased significantly and at present the European Union is one of the most influential players in the field of international policies pertaining to cybersecurity.

Most often cybersecurity refers to:

➢ measures for protecting information technologies;

➢ the included within those measures information, ongoing processes and the related physical and virtual elements (which, taken together, comprise cyber space);

➢ the level of protection resulting from the implementation of those measures.

Virtually all elements in cyberspace are at risk as their interconnection renders it difficult to determine the scope and framework of cybersecurity.

One of the necessary conditions for the creation and development of an EU policy on cybersecurity is an understanding of what the term "cybersecurity" denotes. Achieving this can be difficult for several reasons. Some the main challenges and difficulties include its wide range and multiple aspects that influence the different spheres of social relations between EU citizens and between the Member States of the European Union. The scientific research and analysis of the authors of this publication are focused in this direction.

II Possibilities and the need for a ciber security strategy

The first act of the EU institutions, which is part of secondary legislation of the European Union, giving significant impetus to the development of the definition of information security, is Directive 95/46/EC[1]. However, it is geared more towards protection of individuals with regard to the processing of personal data and on the free movement of such data within the EU space and towards third countries with which the EU has concluded data exchange agreements.

There are many components of cyberspace and various potential participants in the implementation and realization of the cybersecurity policy. Different stakeholders can be involved as objects or subjects in different areas and at different stages of the policy in question and, therefore, attempts to create a coordinated policy within the European Union could be a challenge; at the same time, though, it could turn out to be an indispensable reality containing concentration and unification of traditional political cooperation with other new and constantly changing components of the modern information technologies.

According to the 2003 US National Strategy to Secure Cyberspace, "cyberspace consists of hundreds of thousands of interconnected computers, servers, routers, switches, fiber optic cables that allow our critical infrastructure to work"[2] and refers to "interconnected network of critical information infrastructures". Cyberspace security focuses on the protection of hardware and software, *including the information contained therein*[3].

Potential ambuguity of the term in question *could be a problem and an obstacle* to the development of an EU policy on issues of cybersecurity and it could negatively affect the ability of different stakeholders (states, the private sector – legal entities providing communication services and Internet, as well as entities from the NGO sector, etc.) to agree on the *elements, principles and objectives* of the policy implemented in the new dimension of information and communication technologies. However, as information technology and cyberspace themselves continue to evolve quickly, the strict definition of the concept and setting certain limits will probably quickly lose their relevance[4]. Therefore, it could be useful to maintain the best possible flexible concept.

In EU legislation, *cybersecurity* refers to the precautions and actions that can be used to protect the cyberspace, both in the civilian and military fields, from those threats that are associated with or may harm the functioning of its independent networks and information infrastructure.

The term *cybercrime* commonly refers to a broad range of different criminal activities where computers and information systems are involved either as a primary tool or as a primary target. Cybercrime comprises traditional offences, content-related offences and offences unique to computers and information systems[5].

The use of cyberspace is insufficiently regulated worldwide in terms of both national and international public law. So far, there is no legally binding international treaty pertaining to cybersecurity which expresses the common will of all States and serves as the basis for the formation of a common international legal framework that will bind participating countries to respect and implement the principle pacta sund servanda.

Within the EU, the regulation of cybersecurity, according to the specifics of the principles and effects of the acts of the European institutions, becomes an integral part of the national legislation of the Member States. As this is a rapidly evolving area of law, all cyber threats have not yet been defined. New threats emerge constantly, which requires prompt development of measures to counteract to them.

The lack of a uniform definition of cybersecurity is further indicated by the fact that even the strategies of the individual Member States do not contain such a unified concept.

Taking advantage of the daily benefits of new technologies, EU citizens and various objects of critical infrastructure are exposed to a number of risks. Maintaining a high level of cyber security requires coordinated action at the international and European level, as well as the national one.

By May 2015, twenty of the EU Member States (*Belgium, the Czech Republic, Denmark, Lithuania, Latvia, Estonia, Finland, France, Germany, Hungary, Italy, Luxemburg, Poland, Romania, Slovakia, Spain, The United Kingdom, the Netherlands (Holland), Austria, Cyprus),* have existing cybersecurity strategies. *(The Republic of Bulgaria still has not enacted such a document, despite the fact that five governments have announced they had worked actively for its drafting.* The period 2011 – 2013 saw the height of the progress in the development and eforcement of various state documents related to the issues of security in the ICT area, including national cybersecurity strategies.

The European Network and Information Security published *National Cyber Security Strategies. Practical Guide on Development and Execution*[6], which presents good practices and recommendations on how to develop, implement and maintain a cyber security strategy.

In the Guide, the national cybersecurity strategy is defined as a tool to improve the security and sustainability of the national information infrastructures and services. It creates a number of national goals and priorities to be achieved within a specified period of time. As such, it provides a strategic framework for a nation's approach to cybersecurity.

In order to trace the individual national approaches of the EU Member States in the preparation and implementation of their strategies, the paper offers a *content analysis* of their national documents related to cybersecurity. In this regard, some elements stand out as common for the reviewed *fifteen strategies*[7], and namely the strategies of: *Austria, Belgium, the Czech Republic, Lithuania, Latvia, Estonia, Finland, Germany, Hungary, Italy, Poland, Spain, the United Kingdom, the Netherlands, and Slovakia.*

III Results and challenges

The other five strategies have not been analyzed as they have been published only in the official language of the country and this could lead to the possibility of certain errors in their translation.

The comparative analysis of the national cybersecurity strategies shows that the abovementioned countries have similar views on a number of issues. Common features include listing of the opportunities and benefits of using cyberspace and new technologies, as well as the risks to cybersecurity resulting from such use. Also, strategic goals to be pursued and areas of action have been identified, and all of the strategies emphasize the importance of *international cooperation in the field of cybersecurity*.

It has to be noted that Austria[8], Estonia[9], the Czech Republic[10], Finland[11], Germany[12], Hungary[13], Latvia[14], Spain[15], Holand[16], Poland[17] and the United Kingdom[18] determine the relevant principles for the implementation of their strategies. Generally, they can be sytematized as follows:

- Cyber security is an integral part of the national security, supports the functioning of the state and society, and promotes the competitiveness of the economy and innovation.
- Cybersecurity should be ensured while respecting the fundamental rights and freedoms, protecting personal freedoms in the network (*the relevant principle is enshrined in the EU cybersecurity strategy as one of the most fundamental to it*), cooperation between the public and private sectors, as well as cooperation with allies, partners and international organizations.
- Cybersecurity entails individual responsibility for safe use of ICT tools.

Although there is a number of differences with regard to the basic concepts and terms, the detailed analysis of the strategies shows that only 9 out of the 15 (*Austria, Finland, Germany, Italy, Latvia, Spain, Poland, Holland and Great Britain*) contain definitions of key terminology pertaining to cybersecurity.

It is noteworthy that the cybersecurity strategies of only three countries (*Estonia, Latvia and Poland*) explicitely mention the compatibility of the strategies with other national plans and regulations. This compatibility shows the relationship and consistency in the development of common rules of conduct within the individual Member States.

Of particular interest is the fact that the strategies of few countries (*Estonia, Latvia, Poland, Italy, Lithuania, the Netherlands, Spain and the UK*), mention *stakeholders* at the high level of cybersecurity and *national authorities responsible for achieving it*. In this connection, it is appropriate to follow the example of the Netherlands, Latvia and Poland, which have developed extremely detailed action plans that include even the specific roles and responsibilities of the participants in cybersecurity.

In the EU Cybersecurity Strategy adopted in February 2013 and the accompanying proposal of the European Commission "regarding the measures for ensuring a high common level of network and information security in the Union", the main emphasis is on the role of the operators of critical infrastructures. With regard to that, each country should determine which sectors and areas fall in the ICT, and devise appropriate measures for managing the security risks, as well as for reporting serious incidents to the competent national authorities.

IV Conclusions

Having considered the best practice in the researched area, we believe it imperative that Member States follow the example of Austria, Latvia, the Netherlands and Estonia (in the strategy for the period 2008 – 2013) and to indicate in their strategies the operators of critical infrastructure.

Despite the existing differences in the national cybersecurity strategies of Member States of the European Union, there are many converging points. It is these converging points that show the common will and unified approach for achieving a high level of cybersecurity in the EU.

Last but not least, it is necessary, now more than ever, that the countries which have not adopted similar strategic documents yet to take action for their development and administration.

References

[1] DIRECTIVE 95/46/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data https://ccdcoe.org/sites/default/files/documents/EU-951024-DataProtectionDirective.pdf

[2] The National Strategy to Secure Cyberspace, NSSC, VII). https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf

[3] Markova, Ts., Information Security Legal regime, Sofia, 2015, ISBN: 978-619-7143-03-4

[4] Petrova M., Varbanov St. Implementation of information system of enforcement in Bulgaria, according to the Law on Private Enforcement, ISMA, Riga, Latvia, ISSN 1691-2489, Information Technologies, Management and Society (2013) Volume 6, No. 1, 39 – 45.

[5] Cybersecurity Strategy of the European Union. An Open, Safe and Secure Cyberspace, JOIN (2013) 1 final, Brussels, 7.2.2013, p. 3.

[6] National Cyber Security Strategies. Practical Guide on Development and Execution, European Network and Information Security Agency (ENISA), December 2012.

[7] https://ccdcoe.org/strategies-policies.html

[8] Finland's Cyber Security Strategy (2013), http://www.yhteiskunnanturvallisuus.fi/en/materials/doc_download/40-finlandas-cyber-security-strategy

[9] Cyber Security Strategy (2014) https://www.mkm.ee/sites/default/files/cyber_security_strategy_2014-2017_public_version.pdf, as well as the previous strategy for the period 2008 – 2013.

[10] Cyber Security Strategy of the Czech Republic 2015 – 2020 (2015) https://ccdcoe.org/sites/default/files/strategy/CZE_NCSS_en.pdf

[11] Finland's Cyber Security Strategy (2013) http://www.yhteiskunnanturvallisuus.fi/en/materials/doc_download/40-finlandas-cyber-security-strategy

[12] Cyber Security Strategy for Germany (2011) http://www.bmi.bund.de/SharedDocs/Downloads/DE/Themen/OED_Verwaltung/Informationsgesellschaft/cyber.pdf?__blob=publicationFile

[13] National Cyber Security Strategy of Hungary (2013) http://www.nbf.hu/anyagok/Government%20Decision%20No%201139_2013%20on%20the%20National%20Cyber%20Security%20Strategy%20of%20Hungary.docx

[14] Latvian cyber security strategy for the period 2014 to 2018 (2014) https://ccdcoe.org/sites/default/files/strategy/LVA_CSS_2014-2018.pdf

[15] National Cyber Security, a Commitment for Everybody (2013) http://www.ismsforum.es/ficheros/descargas/a-national-cyber-security-strategy-.pdf

[16] National Cyber Security Strategy 2: From Awareness to Capability (2013) http://english.nctv.nl/images/national-cyber-security-strategy-2_tcm92-520278.pdf

[17] Cyberspace Protection Policy of the Republic of Poland (2013) http://www.cert.gov.pl/download/3/162/PolitykaOchronyCyberprzestrzeniRP148x210wersjaang.pdf

[18] The UK Cyber Security Strategy. Protecting and Promoting the UK in a Digital World (2011) https://www.gov.uk/government/publications/cyber-security-strategy

Anotācija

Viens no priekšnoteikumiem Eiropas Savienības politikas stratēģijas izstrādāšanai un attīstīšanai kiberdrošības jomā ir vienota "kiberdrošības" jēdziena izpratne. Izpratnes vienotību apgrūtina šim jēdzienam atbilstošo drošības aspektu daudzšķautnība un plašā ietekme gan uz Eiropas Savienības iedzīvotājiem, gan dalībvalstu attiecībām. Raksta galvenā tēze ir saistīta ar to, ka kiberdrošības problēmas ir ne vien ļoti specifiskas, bet arī ārkārtēji nozīmīgas, tāpēc problēmu kiberdrošības jomā risināšanai ir nepieciešama aktīva valstu un starptautisko organizāciju sadarbība.

Аннотация

Одним из необходимых условий для создания и развития политики ЕС в области кибербезопасности является осознание того, какой смысл вкладывается в понятие «кибербезопасность». Достижение этой цели может быть затруднено по нескольким причинам. Одну из основных проблем и трудностей представляет его широта и многоаспектность влияния на различные сферы общественных отношений между гражданами ЕС и между государствами-членами Европейского союза. Основной тезис данной статьи состоит в том, что проблема кибербезопасности является не только специфической, но и чрезвычайно актуальной проблемой, решение которой требует активного участия стран и международных организаций.