INTERNATIONAL CONFERENCE RCIC'20
Redefining Community in Intercultural Context
Cluj-Napoca, 7-9 May 2020

A COMPARATIVE STUDY ON EUROPEAN CYBER SECURITY STRATEGIES

Simona ENESCU*

* National University of Political Studies and Public Administration, Bucharest, Romania

Abstract: *Technology is evolving fast and the associated cyber threats, even more. Their diversity and the attackers' skills set up real challenges in identifying best preventive measures against cyber-attacks. If taken into consideration the classification that defines five main categories of cyber-attacks – cybercrime, cyber war, cyber terrorism, cyber espionage and hacktivism, at least three of them represent a direct threat to national security. This is one of the reasons for which every country needs legislation in addressing these threats. European Union Member States have issued at least, one national cybersecurity strategy. Given the cyberspace evolution, some of these documents already reached third edition. The article represents a comparative analysis on the cybersecurity strategies of EU members. Even if they benefit from the same guidelines, the documents are different, from one state to another, based on preliminary analysis of each national cyber context. This generates diverse approaches related to priorities, scopes, objectives, and also sets of measures and fields of action. The aim of the article is identifying different approaches of the cybersecurity field and how Member States countries complied to EU regulations. One of the key elements of the strategies constitutes ways to integrate cybersecurity in education system, as a measure meant to raise awareness among internet users and also to increase the cybersecurity culture level of the society.*

Keywords: *community; intercultural context; communication*

1. INTRODUCTION

Established as an economic-political organization, European Union started to show interest in cybersecurity in early 2000s. Since then, European Union have issued a lot of regulations, mandatory or not, for its Member States on different aspects of prevention, regarding personal data protection, critical infrastructure protection, safe online transactions, or a common approach on cybersecurity of 5G networks.

The first integrated EU strategy on cybersecurity dates back on 2013 – EU Cybersecurity Strategy: An Open, Safe and Secure Cyberspace that establishes the core values and the main priorities of the Union in this field. In this document, EU reveals the need for legislation in the field, stressing that "there are still gaps across the EU, notably in terms of national capabilities, coordination in cases of incidents spanning across borders, and in terms of private sector involvement and preparedness" (EU Cybersecurity Strategy, 2013). On 2016, European Parliament and European Commission issued the NIS Directive that sets up some measures to be taken in order to achieve

a high common level of security of network and information systems within the Union so as to improve the functioning of the internal market (Directive (EU)2016/1148).

The most recent such document, issued on 2019, is the EU Cybersecurity Act that lays down new objectives and responsibilities for ENISA – EU Agency for Cybersecurity, and also "a framework for establishment of European cybersecurity certification schemes for the purpose of ensuring an adequate level of cybersecurity for ICT products, services and processes in the Union" with "the purpose of avoiding the fragmentation of the internal market" (The Cybersecurity Act, 2019) on the matter of cybersecurity certification.

Thus, there are to analyze three strategic documents on cybersecurity, although different both by type and by object: one resolution containing general provisions and guidelines, one directive focused exclusively on a single component of cybersecurity - network and information systems protection, and a regulation on another two directions: strengthening an important institution in European cybersecurity, on one hand, and establishing a new set of prevention measures, on the other.

As for the Member States, the first national cybersecurity strategies were issued by Germany and Sweden, in 2005. Following the 2007 Estonia's cyberattack, on 2008, Finland and Slovakia issued their first cybersecurity strategies, along with Estonia. The next strategies, issued on 2011, belong to Czech Republic, France, Lithuania, Luxembourg, Netherlands and Great Britain (at the time, Great Britain was an EU member state). Also, on 2011, Germany revised its 2005 cybersecurity strategy, focusing on critical infrastructures protection (ENISA Study).

At present, every EU Member State has a cybersecurity strategy in force. Some of them are at their third edition, such as those of Germany, Greece, Estonia or Luxembourg.

2. RELEVANT EU PROVISIONS ON CYBERSECURITY

2.1 Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, 2013. The document presents a set of principles for EU cybersecurity policy both within its borders and internationally. These principles refer to: extending the EU core values to cyberspace; protecting fundamental rights, freedom of expression, personal data and privacy; ensuring access to the internet for all; democratic and efficient governance, so that the internet resources, protocols and standards are well managed; and a shared responsibility to ensure security.

The EU Cybersecurity Strategy also sets up five strategic priorities, along with a set of specific actions, addressing different types of actors, including Member States that gets some responsibilities, mainly on raising awareness: "organize a yearly cybersecurity month" and

> step up national efforts on NIS education and training, by introducing training NIS in schools (…), training on NIS and secure software development and personal data protection for students and NIS basic training for staff working in public administration.

Another strategic priority that need attention from Member States is "Developing cyberdefence policy and capabilities related to the framework of the Common Security and Defense Policy (CSDP)", with some key actions such as: "assess operational EU cyberdefence requirements and promote the development of EU cyberdefence capabilities and technologies", "develop the EU cyberdefence policy framework", "promote dialogue and coordination between civilian and military actors in the EU" and "ensure dialogue with international partners".

Also, under the priority of "Fostering R&D investments and innovation", Member States should: "develop good practices to use the purchasing power of public administration" and "promote early involvement of industry and academia in developing and coordinating solutions".

The document does not offer a definition for cybersecurity, however it mentions that it "commonly refers to the safeguards and actions that can be used to protect the cyber domain, both in the civilian and military fields, from those threats that are associated with or that may harm its interdependent networks and information infrastructure", with the purpose of preserving "the availability and integrity of the networks and infrastructure and the confidentiality of the information contained therein".

The Strategy was adopted by a resolution of the European Parliament, so the provisions of such document are, in fact, recommendations. For example, at the time, only 13 Member States had adopted national cybersecurity strategies, so that the Parliament "reiterates its call" on the matter. Also, the Member States are called

> to take all the action needed to come forward with training programs aimed at promoting and improving awareness, skills and education among European citizens,

or "to set in place adequate framework" for cooperation between private and public sector, or "to establish a network of well-functioning Computer Emergency and Response Teams (CERTs)", or "to take the necessary measures to establish a single market for cybersecurity" etc.

2.2 Directive (EU)2016/1148 concerning Measures for High Common Level of Security of Network and Information Systems across the Union. With a completely different approach, more focused on Member States responsibilities, the NIS Directive establishes a set of measures to be taken with the purpose of securing information networks and systems within the Union.

In fulfilling this scope, Member States have the obligation to adopt national strategies on the security of network and information systems, they should cooperate and exchange information and establish national competent authorities with responsibilities in the security of network and information systems, as well as at least one CSIRT - Computer Security Incident Response Team.

For supporting states to adopt their national NIS security strategies, the Directive offers a set of items that should be addressed, such as: objectives and priorities; a governance framework to achieve the objectives and priorities, roles and responsibilities of the government bodies and other relevant actors; preparedness, response and recovery oriented measures, including cooperation between the public and private sectors; education, awareness raising and training programs; research and development plans; a risk assessment plan; and a list of the relevant actors involved in the implementation of the strategy.

Every Member State has to identify the national operators of essential services, for each sector and subdivisions, and the Directive offers a set of criteria in this way.

The Directive offers a set of definitions to specific terms, without referring to cybersecurity. Instead, there is "security of network and information systems" term that is defined as "the ability of network and information systems to resist, at a given level of confidence, any action that compromises the availability, authenticity, integrity or confidentiality of stored or transmitted or processed data or the related services offered by, or accessible via, those network and information systems".

Unlike the previous EU Cybersecurity Strategy, the NIS Directive has mandatory provisions for Member States, so that, they should have been implemented by 10th of May 2018.

2.3 Regulation (EU)2019/881 on ENISA and on Information and Communication Technology Cybersecurity Certification. Having essentially the same scope as the other two documents mentioned above, "achieve a high level of cybersecurity, cyber resilience and trust within the Union", and being mandatory to the Member States, The Cybersecurity Act is structured on two main components: strengthening ENISA (European Union Agency for Cybersecurity) on one hand, and providing support for Member States in addressing cyberthreats, by establishing unitary European cybersecurity certification schemes for ICT products, services and processes, on the other.

According to this document, ENISA is a permanent, independent, scientific and technical center of expertise on cybersecurity that assists the EU institutions and the Member States in developing and implementing the Union policies related to cybersecurity and that promotes the use of European cybersecurity certification.

European cybersecurity certification is a new policy of European Union that consists in "a comprehensive set of rules, technical requirements, standards and procedures that are established at Union level and that apply to the certification or conformity assessment of specific ICT products, ICT services and ICT processes falling the scope of the specific scheme".

The Regulation also provides, among other terms, a definition for cybersecurity: "the activities necessary to protect network and information systems, the users of such systems and other persons affected by cyber threats".

3. THE NATIONAL CYBERSECURITY STRATEGIES OF EU MEMBER STATES

Generally, the EU law on cybersecurity recommends and sets up a series of tasks and activities for Member States that can be collected in few major objectives: (1) National cooperation; (2) International cooperation; (3)Awareness, education, research and development; (4) Critical infrastructures protection and the resilience of the network and information systems

3.1 National Cooperation in European Cybersecurity Strategies. Most of the documents approach national cooperation as cooperation between public and private sector in cybersecurity.

Malta describes cooperation both at internal and international level "on a European and on a global basis, enabled by EU and international institutions and activities, based on the understanding that cybersecurity has no bounds".

Another example in this way is Romania's Strategy that explains cooperation equally internal and international by "all public or private entities collaborate at internal and international level, in order to ensure an adequate response to cyber threats".

Some strategies, like the Italian one, defines internal cooperation as public-private partnership, having a central role in cybersecurity, and the partners have to: "communicate to the Cybersecurity Unit every significant security and integrity violation of their computer systems", "adopt the best practices and measures necessary to pursue cybersecurity", "share information with agencies for intelligence and security and allow access to databases that are relevant to cybersecurity" and "collaborate to the management of a cyber crisis by restoring the functionality of the networks and systems they operate".

There is a specific concept for internal cooperation, used only in some of the oldest (strategies of Belgium, 2012 and Finland, 2013) and the most recent strategies (strategies of Netherlands, 2018 and Portugal, 2019) - *situational awareness*, defined in Netherlands' Strategy as "a cooperation platform with the goal to offer more information and a swifter perspective for action with relevant organizations within the legal frameworks". Portugal set this platform at CERT-PT level.

3.2 International Cooperation. It is an important concept, especially related to the borderless, global nature of the cyber threats. Most European Cybersecurity Strategies approach international cooperation in terms of projects and exercises, within international organizations, like EU and NATO, or UN and the OSCE.

Ireland refers to cyber international cooperation as a mean to economic development:

> continue to engage with international partners and international organizations to ensure that cyber space remains open, secure, unitary and free and able to facilitate economic and social development (National Cyber Security Strategy, 2019).

Another approach on the matter belongs to Finland, that underlines "international operational cooperation and the exchange of information will be continued and intensified with EU and with other countries' corresponding law enforcement officials, such as Europol".

One of the specific objectives in Poland's Strategy is "Building strong international position of Poland in the area of cybersecurity", on two coordinates: at strategic and political level, within the EU and other international organizations, and at the operational and technical level, by CSIRT network.

3.3 Awareness, Education, Research and Development. Different concepts by meaning, they are combined in various ways: awareness and education for all internet users, education in schools from primary grades to specialized university level, education and training for employees in both in cybersecurity and IT fields, both in public and private sector. That's why there are a few strategies that relate education with research and development.

Hungary describes the importance of awareness at political and professional decision making and links education, as a continuous process, to research and development.

Czech Republic defines education by public administration, police and the judiciary staff training on one hand, and by adapting the curricula in schools with the purpose of providing experts in cybersecurity and IT.

Another strategy that underlines the importance of training in public administration is the one of Poland, but as a responsibility of NGOs. Poland also describes the role of cyber education in early stages, and as a continuous process for professional development.

There are countries, like Czech Republic, Luxembourg, Denmark or Spain, that specify cyber education as a mean to rising awareness.

Results of national context analysis can be identified in specific elements in this section. Denmark describes the role of education "for children to navigate in a safe, responsible and ethical manner in using ICT technology and social media" and Sweden relates awareness to "counteracting the effects of disinformation and influence campaigns".

An awareness related concept is the responsibility of all users. It is underlined in Malta's strategy "to ensure a secure and safe cyberspace for all", by applying "at least some form of basic cyber hygiene in using ICT". Lithuania also defines awareness by "society's culture of self-protection and responsible behavior in cyberspace".

A similar approach belongs to Netherlands: "it is important that citizens and businesses also continue to develop their knowledge to protect themselves against digital threats".

Less used in strategies, cybersecurity culture is another concept strongly related to education and awareness. Lithuania defines cybersecurity culture by education, but most of the documents describe it as being achieved by awareness, as the ones of Austria, Romania, Czech Republic and Slovenia. There are others, like Italy and Sweden, that describes this report the other way around – achieving awareness by cybersecurity culture.

Maybe the most comprehensive sense for cybersecurity culture is given by Spain, which defines the term as evolving "from awareness to commitment, in the understanding that citizens have joint responsibility for national cybersecurity".

The third edition of Estonia' strategy contains some evaluation elements such as: "cybersecurity culture helped preventing incidents with extensive consequences", but society's level of awareness is "still insufficient".

Even though state uses these concepts in various ways – objectives, goals, lines of action, measures or even vulnerabilities, Germany does not use any of these terms.

3.4 Critical Infrastructure Protection and the Resilience of the Network and Information Systems. They are another key element in cybersecurity strategies. Although different concepts and systems, the two types of infrastructures are to be analyzed together, because they are strongly related.

On one hand, there is critical infrastructure, regulated by international law, having two major components: international critical infrastructure and national critical infrastructure, that are strongly connected – the international one consists in the national infrastructures network.

A critical infrastructure is defined, as Finland Strategy shows, as "the structures and functions which are indispensable for the vital functions of society". They are the essential services described by European regulations. Such infrastructures are: transport, energy, financial services, health, water or commerce.

On the other hand, there is the communications and information technology, known as critical information infrastructure. A definition for this concept is to be found also in Finland Cybersecurity Strategy (2013):

> the structures and functions behind the information systems of the vital functions of society which electronically transmit, transfer, receive, store or otherwise process information.

Its importance come from the role it has in all the other infrastructures functioning and that's why one of the key objectives of every cybersecurity strategy is to ensure the resilience of such networks.

In simple words, the resilience term defines a network recovering capacity, after a damaging incident. That's why Austria underlines that it is "a top priority to improve the resilience of the information systems against threats" and, for most of the countries, it's a shared responsibility of governments, designated public institutions and structures and also the essential services stakeholders.

4.CONCLUSIONS & ACKNOWLEDGMENT

Every EU Member State has adopted a cybersecurity strategy. Today, there are in force 27 such documents issued between 2012 and 2019. It is clear that some of them need to be revised, firstly because the cybersecurity environment has changed and secondly, from the perspective of EU membership, every state has to comply to the obligations stated in European regulations.

The EU vision of unitary regulations is accomplished by the fact that every country respected the Union guidelines. Nonetheless, the states' own national cyber context analysis makes great difference. It is only natural that national strategy focuses on national priorities, report to national principles and deal with national risks, as they resulted from analysis. There is a problem concerning different interpretations given to specific concepts and terms and the way they report to each other.

Also, the states' analysis of the cyber environment caused different general approaches. Therefore, some states *dream big* by assuming the role of important international cybersecurity players; some *play low*, by establishing basic objectives; most of them *play safe*, by including all necessary theories, and there are some that remain *cautious*. In the last group we can include Estonia which is a 90% digitalized country. On 2007, Estonia experienced an important cyber-attack targeting the information systems, affecting every citizen, for 22 days. It was the most important cyber-attack on an EU and NATO member state.

The first measure taken by Estonia, was adopting both a cybersecurity strategy and a cybersecurity law.

Today's Estonian Cybersecurity Strategy in force is at its third edition. Some of the third edition strategies are more comprehensive, containing even an analysis on previous edition – achieved objectives and implemented measures and plans of action.

BIBLIOGRAPHY

1. European Union Agency for Cybersecurity (ENISA). (2012). National Cyber Security Strategies. *Enisa* [online]. URL: https://www.enisa.europa.eu/publications/cyber-security-strategies-paper [Accessed on April, 2020].
2. The European Parliament. (2013). EU cybersecurity strategy: an open, safe and secure cyberspace. European Parliament resolution of 12 September 2013 on a Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace (2013/2606(RSP)). P7_TA(2013)0376. *Official Journal of the European Union.* C 93.

3. The European Parliament and the Council of the European Union. (2016). Directive (EU)2016/1148 of the European Parliament and of the Council concerning Measures for High Common Level of Security of Network and Information Systems across the Union, 2016. *Official Journal of the European Union.* L 194.
4. The European Parliament and the Council of the European Union. (2019). Regulation (EU) 2019/881 n ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act). *Official Journal of the European Union.* L 151.
5. ***. (2012). *Cybersecurity Strategy of the Republic of Cyprus. Network and Information Security and Protection of Critical Information Security*. Version 1.0. Nicosia: Office of the Comissioner of Electronic Communication & Postal Regulation (OCECPR).
6. ***. (2012). *Cyber Security Strategy*. Brussels: Belgian Federal Government.
7. ***. (2013). *Austrian Cyber Security Strategy*. Vienna: Federal Chancellery of the Republic of Austria.
8. ***. (2013). *Finland's Cyber security Strategy.* Government Resolution 24.1.2013. Helsinki: Secretariat of the Security Committee.
9. ***. (2013). *National Strategic Framework for Cyberspace Security.* Rome: Presidency of the Council of Ministers.
10. ***. (2013). *National Cyber Security Strategy of Hungary*. Government Decision no. 1139. Budapest: Hungarian Government.
11. ***. (2013). *Romanian National Cyber Security Strategy*. Government Decisiona no.271. Bucharest: Romanian Government.
12. ***. (2014). *Cyber Security Strategy of Latvia 2014-2018.* Riga: Ministru kabineta, Nr.40/ 21 jan.
13. ***. (2015). *Cybers Security Concept of the Slovak Republic for 2015-2019.* Bratislava: Urad Vlady Slovenskej Republiky.
14. ***. (2015). *French National Digital Security Strategy.* Paris: French Government.
15. ***. (2015). *National Cyber Security Strategy of the Czech Republic for the period from 2015 to 2020.* Prague: National Security Authority/ National Cyber Security Centre.
16. ***. (2015). The National Cyber Security Strategy of the Republic of Croatia. *Official Gazette* no.108/ 7 October.
17. ***. (2016). *Cyber Security Strategy. Establishing a system to ensure a high level of Cyber Security*. Ljubljana: Digital Slevenia.
18. ***. (2016). *Cyber Security Strategy for Germany*. Berlin: federal Ministry of the Interior.
19. ***. (2016). *Malta Cyber Security Strategy*. La Valetta: Ministry for Competitiveness and Digital/ Maritime and Services Economy.
20. ***. (2017). *A national cyber security strategy* (Skr.2016/17:213). Stockholm: Governmeent Offices of Sweden/ Ministry of Justice.
21. ***. (2017). *National Framework of Cybersecurity Policy of the Republic of Poland for 2017-2022.* Warsaw: Ministry of Digital Affairs.
22. ***. (2018). *National Cyber Security Strategy.* Version 3.0. Athens: Informatics Development Agency.
23. ***. (2018). *Cybersecurity Strategy. Republic of Estonia. 2019-2022.* Tallin: Ministry of Economic Affairs and Communications.
24. ***. (2018). *Danish Cyber and Information Security Strategy 2018-2021.* Copenhagen: The Danish Government/ Ministry of Finance.
25. ***. (2018). *National Cybersecurity Agenda. A cyber secure Netherlands.* The Hague: National Cyber Security Centre/ Ministry of Justice and Security.
26. ***. (2018). *National Cyber Security Strategy.* Resolution no.818. Vilnius: Governement of the Republic of Lithuania.
27. ***. (2018). *National Cybersecurity Strategy III.* Luxembourg: Government council.
28. ***. (2019). *National Cybersecurity Strategy.* Madrid: Presidencia del Gobierno.
29. ***. (2019). *National Cyber Security Strategy. 2019-2024.* Dublin: Governement of Ireland.
30. ***. (2019). *National Cyberspace Security Strategy 2019-2023.* Resolution 92. Lisbon: Council of Ministers.