Regulatory Cybersecurity in the European Union and the Republic of Moldova

Liudmila LAPIȚKAIA[*], Alexandru LEAHOVCENCO[**]

Abstract

The rapid development of information technology leads to various opportunities for both individuals and businesses to conduct including financial transactions through the Internet. In such circumstances, cyber security issues become very relevant. In this regard, the European Parliament regularly reviews and updates the cybersecurity regulatory framework. In turn, the Republic of Moldova should also update its legislative framework in the field of cyber security in order to bring it in line with European standards. On the basis of this analysis, the normative documents on cyber security of the Republic of Moldova are considered and the directorates for further development of cyber security in Moldova are established.

Key words: cyber security, Cybersecurity act, the NIS Directive, the National Cyber Security Program of the Republic of Moldova.

JEL Code: Y80

1. Introduction

The dynamic formation of a global information space is connected, on the one hand, with the provision of unprecedented information capabilities to humanity, as well as with the emergence of new threats. A new cybersecurity phenomenon has emerged. Various cybersecurity definitions can be found in the specialized literature. For example: in accordance with the provisions of the Cybersecurity act adopted by the European Parliament on 12 March 2019 *«cybersecurity means the activities necessary to protect network and information systems, the users of such systems, and other persons affected by cyber threats»*. In according to the definition given by The Economic Times: «Cybersecurity or information technology security are the techniques of protecting computers,

[*] Liudmila LAPIȚKAIA is associate professor at Academy of Economic Studies of Moldova, Chisinau, E-mail: liudmila@ase.md

[**] Alexandru LEAHOVCENCO is PHd student at Academy of Economic Studies of Moldova, Chisinau, E-mail: alexandru.leahovcenco@yandex.com

networks, programs and data from unauthorized access or attacks that are aimed for exploitation. (Economic Times)

Description: Major areas covered in cybersecurity are:

1) Application Security,
2) Information Security,
3) Disaster recovery,
4) Network Security».

One of the best-known cyber security firms in Russia, Kaspersky, gives the following definition: «*cyber-security is the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks. It's also known as information technology security or electronic information security. The term applies in a variety of contexts, from business to mobile computing, and can be divided into a few common categories*.

- *Network security is the practice of securing a computer network from intruders, whether targeted attackers or opportunistic malware.*
- *Application security focuses on keeping software and devices free of threats. A compromised application could provide access to the data its designed to protect. Successful security begins in the design stage, well before a program or device is deployed.*
- *Information security protects the integrity and privacy of data, both in storage and in transit.*
- *Operational security includes the processes and decisions for handling and protecting data assets. The permissions users have when accessing a network and the procedures that determine how and where data may be stored or shared all fall under this umbrella.*
- *Disaster recovery and business continuity define how an organization responds to a cyber-security incident or any other event that causes the loss of operations or data. Disaster recovery policies dictate how the organization restores its operations and information to return to the same operating capacity as before the event. Business continuity is the plan the organization falls back on while trying to operate without certain resources.*
- *End-user education addresses the most unpredictable cyber-security factor: people. Anyone can accidentally introduce a virus to an otherwise secure system by failing to follow good security practices. Teaching users to delete suspicious email attachments, not plug in unidentified USB drives, and various other important lessons is vital for the security of any organization». (Kaspersky)*

American company Cisco on it's web page published the following definition: «cybersecurity is the practice of protecting systems, networks, and programs from digital attacks».(Cisco)

Also, ENISA differentiates the following areas of cybersecurity (ENISA,2015,p.11):

Analysing all this information, the authors synthesized the following definition of cyber-security: cyber security is the organization of protection of various information systems and their carriers from cyber-attacks.

Table 1. Different domains of Cybersecurity

Communications Security	Protection against a threat to the technical infrastructure of a cyber system which may lead to an alteration of its characteristics in order to carry out activities which were not intended by its owners, designers or users.
Operations Security	Protection against the intended corruption of procedures or workflows which will have results that were unintended by its owners, designers or users.
Information Security	Protection against the threat of theft, deletion or alteration of stored or transmitted data within a cyber system.
Physical Security	Protection against physical threats that can influence or affect the well-being of a cyber system. Examples could be physical access to servers, insertion of malicious hardware into a network, or coercion of users or their families.
Public/National Security	Protection against a threat whose origin is from within cyberspace but may threaten either physical or cyber assets in a way which will have a political, military or strategic gain for the attacker. Examples could be 'Stuxnet' or wide-scale DOS attacks on utilities, communications financial system or other critical public or industrial infrastructures.

Source: The European Union Agency for Network and Information Security

2. Literature review

The presence of the Internet and the development of digital technologies are dynamically changing the usual spheres of human life, transforming the economy, making it digital. The scale of changes and its innovative significance are so significant that in the European Union they believe that nation states cannot cope with the problems of ongoing transformations due to their limited capabilities. Coordinated policies and general legal frameworks are needed. These arguments formed the basis for the creation of the European Union Single Digital Market Strategy (Digital Single Market), which was presented in the Communication by the European Commission in 2015.

The main documents in the field of cybersecurity in Europe are:

1) The Directive on security of network and information systems (the NIS Directive) was adopted by the European Parliament on 6 July 2016 and entered into force in August 2016.
2) Regulation of the European parliament and of the council on ENISA, the "EU cybersecurity agency", and repealing regulation (EU) 526/2013, and on information and communication technology cybersecurity certification ("Cybersecurity act") adopted at 12 march 2019, during the European Parliament plenary , entering into force 20 days after its publication in the Official Journal of the European Union.

After analysing cyber threats, Europol in its report "Assessment of threats from organized crime on the Internet" (The 2017 Internet Organized Crime threat Assessment (IOCTA)) noted that there is a noticeable convergence of interests of cybercrime and organized crime, using the opportunities of the shadow digital economy, which leads to the conclusion that attacks on various databases, both personal and corporate will become more sophisticated.

The Directive on network and information security (the Directive on security of network and information systems (NIS Directive)) was adopted in 2016 to improve supranational regulation of countering cyber-attacks on critical infrastructure. Until May 2018, EU member States had to incorporate its provisions into their national legislation. EU member States should adopt national cybersecurity strategies that define strategic objectives, appropriate policies and regulatory measures in this area. The Directive also provides for the establishment of a "cooperation Group" to facilitate cooperation and exchange of information among member States, including through the preparation of guidance documents to facilitate the implementation of the provisions of the Directive relating to life support services operators (operators of essential services).

An important provision of the Directive is the establishment of a Network of computer security incident response teams (CSIRTs). The network should include relevant units in each of the EU member States. The European Agency for network and information security (ENISA) will actively support cooperation between these groups.

The Directive also establishes certain obligations towards non-state actors. Enterprises have an important role in society and the economy, is designated in the Directive as "operators of services of critical infrastructure" (these include, in particular, digital infrastructure) should ensure adequate levels of digital security of their services and to notify serious incidents to the appropriate national authority. These obligations are imposed on providers of digital services.

The Directive on network and information security (the Directive on security of network and information systems (NIS Directive)) was adopted in 2016 to address gaps in European regulation of countering attacks on critical infrastructure. Until May 2018, member States should implement its provisions in their national legislation. In particular, they will need to adopt national cybersecurity strategies that define strategic objectives, relevant policies and regulatory measures. The Directive also provides for the establishment of a "cooperation Group" to facilitate strategic cooperation and exchange of information among member States, including through the preparation of guidance documents to facilitate the implementation of the provisions of the Directive relating to life support services operators (operators of essential services)

The Directive establishes the establishment of a Network of computer security incident response teams (CSIRT). The network should include relevant units in each of the EU member States. The European Agency for network and information security (ENISA) actively supports cooperation between these groups.

In addition to obligations for EU member States, the Directive also establishes certain obligations towards non-state actors. Enterprises have an important role in society and the economy, is designated in the Directive as "operators of services of critical infrastructure" (these include, in particular, digital infrastructure) needs to provide the appropriate level of cyber security of their services and to notify serious incidents to the appropriate national authority. These obligations are imposed on providers of digital services.

Thus, the NIS Directive has become the basis of European cooperation to combat serious incidents in the digital space and contribute to improving the conditions for the development of interactions.

3. Analysis of regulations in the field of cyber security of the European Union and the Republic of Moldova

The main task in the field of cyber security is the protection of personal data. In 2016, in the framework of the changing legal regulation of this sphere was adopted by the General regulation on data protection (General Data Protection Regulation (GDPR)), which replaces EU Directive on data protection 95/46/EC, which entered into force on 25 may 2018. This Regulation is intended to protect the rights of individuals with respect to the processing of personal data by all companies offering their services on the European market. Thus, the GDPR applies, among other things, to companies located outside the EU, whose personal data processing activities are related to the supply of goods and services to data subjects in the EU. The regulation establishes multi-level sanctions for violations of data protection legislation.

In 2016, the European Commission and the European cybersecurity organization (ECSO) signed a partnership agreement on cybersecurity in order to implement the tasks related to cybersecurity outlined in the Strategy of building a Single digital market. The Treaty aims to promote competitiveness and innovation in digital security in the private sector. ECSO includes more than 200 members, including large companies in the field of cybersecurity, small and medium enterprises, and start-ups, research centers, universities, clusters and associations.

In 2017, the European Commission also proposed the establishment of a new body, the EU cybersecurity Agency, on the basis of ENISA, with the simultaneous establishment of a pan-European network for certification of information and communication technology products and services.

One of the key conditions for creating a stable functioning Single digital market is to ensure cybersecurity. The most important area of regulation, to which the EU pays special attention, is to ensure the safety of critical infrastructure.

The Cybersecurity Act:

- Strengthens the ENISA by granting to the agency a permanent mandate, reinforcing its financial and human resources and overall enhancing its role in supporting EU to achieve a common and high level cybersecurity.
- Establishes the first EU-wide cybersecurity certification framework to ensure a common cybersecurity certification approach in the European internal market and ultimately improve cybersecurity in a broad range of digital products (e.g. Internet of Things) and services.

The Ministry of Information Technology and Communications of the RM, jointly with the relevant authorities, developed the National Cyber Security Program of the Republic of Moldova. The document was adopted by Government Decision No. 811 of 29 October 2015.

This document is based on the provisions of the National Strategy for information society development "Digital Moldova 2020" strategy and the national security Strategy of the Republic of Moldova. The National Cyber Security Programme includes 7 areas of intervention:

- secure processing, storage and data access;
- security and integrity of electronic communications networks and services;
- emergency prevention and response capabilities (CERT);
- preventing and combating cybercrime;
- strengthening cyber defence capabilities;
- education and information;
- international cooperation and interaction.

This document has been prepared in accordance with the provisions of the Association Agreement, the Republic of Moldova and the European Union, the Council of Europe's Convention on cyber-crime Strategy, the cyber security of the European Union and the Recommendations of the International Telecommunication Union relating to the cyber security of the electronic communication networks.

Secure processing, storage and data access envisage:

1) the ensuring compliance with the legal and regulatory framework on cybersecurity of the Republic of Moldova, which will include:

- definition of cybersecurity terms (concepts) ;
- delineation of competencies by area;
- the establishment of the authority with functions to monitor the compliance of cybersecurity;
- appointment of authority to scrutinize the implementation of audit results in the field of cybersecurity;
- obligations of holders of public information systems to periodically audit these systems, establishing the frequency, levels and reporting to the competent authority;
- establishment of an inter-sectoral Council on cybersecurity (with the function of coordinating cybersecurity activities)

2) Classification of types of information, except for state secrets,

3) Analysis and development of proposals for the application at the national level of standards related to the processing, storage and safe access to data in accordance with the classification of types of information considered in the technical committees on standardization TC 28 "Information technology" and TC 29 «Electronic communications»,

4) Development of a methodology for assessing the vulnerability of public information systems based on defined, adopted and approved standards,

5) Development of mandatory minimum cybersecurity requirements,

6) Certification of specialists of standards and methodologies, and approved mandatory minimum requirements of cybersecurity,

7) Definition and planning in budgets of institutions of the financial means necessary for carrying out audit of cybersecurity on the basis of the approved methodology.

Security and integrity of electronic communications networks and services establishes the need to:

- bring electronic communications legislation into line with the EU framework directives in this area,
- establish minimum security measures to be taken by suppliers to ensure the security, reliability and integrity of electronic communications networks and/or services and reporting incidents with significant impact on them,
- analysis and implementation at the national level of European and international standards relating to the protection and security of electronic communication networks and their transfer to the National Institute for standardization,
- conduct research on amendments to the legislation on electronic communications in order to eliminate or reduce the number of impersonal subscribers of electronic communications services,
- develop of a special communication network of public administration bodies on the whole territory of the Republic of Moldova.

Emergency prevention and response capabilities (CERT) provides for the following actions:

- creation of a National Cyber Incident Response Center (CERT),
- creating a national cyber incident alert and information system in real time,
- creation of departmental response centres for cyber incidents in the central and local public administration authorities, other institutions that are holders of state information systems,
- establishment for central and local public administration authorities and the business environment in the field of information and communication technologies for mandatory operational reporting on cyber incidents based on a data exchange mechanism and clearly defined roles,
- database organization, with access by responsible authorities, identified or registered cybernetic threats, vulnerabilities and incidents, technologies and methods used for attacks, best practices for protecting the information and communications technology industry,
- Conduct joint exercises and training sessions to strengthen the response capacity to cyber-attacks, including blocking simulated cyber-attacks.

Such a position as Preventing and combating cybercrime sets the following:

- development of a draft law on introducing amendments and additions to criminal legislation and legislation on offenses to prevent and combat cybersecurity information in order to continuously harmonize it with the provisions of the European Convention on Information Crime and the decisions of the Committee of this Convention,
- training of law enforcement officers, specialists certified in the field of cybersecurity,

- implementing the recommendations of the Council of Europe, in particular, the EAP project on training law enforcement personnel,
- development and approval of the draft law on ratification of the Additional Protocol to Council of Europe's Information Crime Convention.

Strengthening cyber defence capabilities directed to:

- develop a section on cyber defence of the Republic of Moldova, as part of the Information Security Strategy of the Republic of Moldova,
- establish of responsible bodies and mutual cooperation in peacetime, in situations of crisis, siege and war in cyberspace,
- use the power of cyberspace to advance national interests, values and goals in cyberspace,
- develop of military capabilities to protect critical infrastructure and services for national defence.

Such a direction as *Education and information* provides development of the concept of information and risk awareness campaigns in cyberspace and supplement of the curriculum in the field of cybersecurity.

International cooperation and interaction aimed at conclusion of cooperation agreements with other national cyber security incident response teams (CERT), as well as US–CERT, European and North Atlantic (NATO NCERT) and creation of a platform for coordination and consulting in the field of cyber threat assessment and search for solutions.

4. Conclusions

In conclusion, it should be noted that the authors analysed the literature on the specialty in terms of the definition of cybersecurity offered their definition, namely: cyber security is the organization of protection of various information systems and their carriers from cyber-attacks.

Having analysed the regulatory framework in the field of cybersecurity of the European Union and the Republic of Moldova, we can state the following:

1) In the light of the changes in the European legislation in the field of cybersecurity, the Republic of Moldova should also update its normative and legislative acts in this field,
2) Moldova should update its critical infrastructure to maintain high level of cyber security against the threats of modern cyberattacks,
3) It is necessary to create a state body for cybersecurity such as the Moldovan cybersecurity Agency that would accumulate a database of cyber threats and take appropriate emergency measures to localize them.

References:

Cisco https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html

ENISA Definition of Cybersecurity Gaps and overlaps in standardization, December 2015

European Parliament legislative resolution of 12 March 2019 on the proposal for a regulation of the European Parliament and of the Council on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification ("Cybersecurity Act") - http://www.europarl.europa.eu/doceo/document/TA-8-2019-0151_EN.html?redirect#BKMD-20,

Hotărîre Guvernului al RM Nr. 811 din 29.10.2015 cu privire la Programul național de Securitate cibernetică a Republicii Moldova pentru anii 2016-2020 http://lex.justice.md/viewdoc.php?action=view&view=doc&id=361818&lang=2

The Economic Times https://economictimes.indiatimes.com/definition/cyber-security

Kaspersky https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security

The effects of cloud technology on management accounting and decision making, Volume 10 – Issue 6, https://www.cimaglobal.com/Research--Insight/The-effects-of-cloud-technology-on-management-accounting/.

Decentralized Applications - Harnessing Bitcoin's Blockchain Technology, by Siraj Raval : O'Reilly Media Release, July 2016 p 118,

“Big data: science in the petabyte era” Nature 455 (7209): 1, 2008.

Douglas and Laney, “The importance of ‘big data’: A definition,” 2008.

Barlow J. P. Selling Wine Without Bottles: The Economy of Mind on the Global Net: http://lib.ru/COPYRIGHT/barlou.txt.

Parinov S.I, Yakovleva T.I, Economy of the 21st century based on Internet technologies.

Big Data: Principles and Best Practices of Scalable Realtime Data Systems, by Nathan Marz, James Warren, p 328, 2015.

Computer Networking: A Top-Down Approach (6th Edition), by James F. Kurose, Keith W. Ross, p 880, 2012