SARA Law **R**esearch **C**enter
International **J**ournal of **L**egal and **S**ocial **O**rder, https://www.ccdsara.ro/ijlso
ISSN 2821 – 4161 (Online), ISSN 2810-4188 (Print), ISSN-L 2810-4188
N°. 1 (2023), pp. 273-279

THE EUROPEAN UNION STRATEGY IN THE FIELD OF CYBER-SECURITY

A.C. MOISE

Received 20.11.2023; accepted 11.12.2023
https://doi.org/10.55516/ijlso.v3i1.168

Adrian-Cristian MOISE
Associate Professor, PhD
Spiru Haret University, Faculty of Juridical, Economic and Administrative Sciences, Craiova
E-mail: adrian.moise@spiruharet.ro
ORCID ID: https://orcid.org/0000-0001-8755-0563

Abstract

Cyber-attacks and cybercrime are increasing in number and sophistication across Europe.

The article presents and analyzes the European Union strategy for the period 2020-2025 in the field of cyber-security, as well as the most important legal instruments and bodies that have concerns in the field of cyber-security. The aim of the European Union's cyber-security strategy is to strengthen Europe's resilience to cyber threats and ensure that all citizens and businesses can fully benefit from reliable and trustworthy digital services and tools. The European Union strategy in the field of cyber-security contains concrete proposals for the implementation of regulatory, investment and policy instruments.

Keywords: *cyber-security, European Union strategy, legal instruments, cyber threats.*

INTRODUCTION

At the level of the European Union, there are several normative acts and bodies that address cyber security.

As early as 2013, the European Commission developed the first document entitled Cyber-security Strategy of the European Union: an open, safe and secure cyberspace that presents the point of view of the European Union and the specific actions that must be taken to have a protected cyberspace at the European level. The specific actions are planned both in the short term and in the long term and include a series of instruments and actors, such as, for example, the institutions of the European Union, the component states of the European Union and the relevant industrial activities.

The strategy at the European level in the field of cyber security from 2013 was defined by means of five priorities: obtaining a resilience of cyber infrastructures; the drastic reduction of computer crime; the development of policies and cyber defensive capabilities regarding the common security and defense policies; increasing cyber-security industry and technology resources; the creation of coherent international policy strategies by the European Union regarding cyber space and the promotion of the fundamental values of the European Union..

Cyber-attacks and cybercrime are increasing in number and sophistication across Europe. This trend is expected to continue to grow in the future, given the predictions that 41 billion devices worldwide will be connected to the Internet of Things by 2025.

In October 2020, EU leaders called for strengthening the EU's capacity to: defend itself against new cyber-attacks; create a more secure communication space that uses encryption; allows access to computer data in compliance with criminal procedural laws and for these computer data to be used only in judicial proceedings.

In December 2020, the European Commission and the European External Action Service (EEAS) revealed a new European Union cyber-security plan for the period 2020-2025.

The aim of this 2020-2025 strategy is to strengthen Europe's resilience to cyber threats and ensure that all citizens and businesses can fully benefit from reliable and trustworthy digital services and tools. The new strategy contains concrete proposals for the implementation of regulatory, investment and policy instruments.

The strategy shows how the EU can highlight and improve all its tools and resources to have access to all technological resources. It also shows how the EU can improve its European collaboration activities with other global allies who support the same value system, such as respect for democracy, fundamental human rights and freedoms and a modern rule of law.

The technological sovereignty of the European Union must be based on the resilience of all connected services and products. All four cyber communities, those dealing with the domestic market, law enforcement, diplomacy and defence need to work more closely for a common threat awareness. They should be ready to respond collectively when an attack materializes so that the EU can be greater than the sum of its parts.

The Cyber-Security Strategy 2020-2025 targets some security measures in the field of important services, such as medical services, energy-related services, the railway transport system and some factories and industries. The strategy wants to develop some collective plans to respond to major cyber attacks. The EU strategy also reveals some collaborative partnerships with member states, as well as with allied states worldwide to more effectively secure cyberspace.

Moreover, the strategy sheds light on how a common cyber system can respond promptly to cyber threats using the common resources and expertise in cyber-security of the Member States and the EU.

The new strategy wants to ensure an Internet that is used worldwide and open, to present some sustainable guarantees, in areas where there are risks of violation of fundamental human rights and freedoms in the online environment for the inhabitants of the European Union. Due to the new progress made in previous strategies, this new strategy contains concrete objectives for the implementation of three main points. These three points represent legislative initiatives and investment policies. These three points will consider three areas of EU action: resilience capacity, technological sovereignty and leadership; operational capability to prevent, deter and respond; collaboration to promote a global and open cyberspace.

The EU aims to support this new European strategy with new digital investments over a period of years. This target would greatly increase previous investments made by the EU. Also, this objective signifies the real involvement of the EU in new industrial policies and new technologies and in a recovery agenda.

I. EUROPEAN UNION LEGAL INSTRUMENTS IN THE FIELD OF CYBER SECURITY

The European Union Cybersecurity Regulation entered into force in June 2019 and introduced: an European Union wide certification system; a new, stronger mandate for the European Union Cyber-Security Agency.

On 18 April 2023, the European Commission proposed a specific amendment to the European Union Cyber-security Act, which refers to the Regulation (EU) 2019/881 as regards managed security services. The proposed change will allow the future adoption of European certification schemes for managed security services covering areas such as incident response, penetration testing, security audits and consulting. We underline that the proposed specific amendment aims to enable, through Commission implementing acts, the adoption of European cybersecurity certification systems for "managed security services, in addition to information and communication technology (ICT) products, ICT services and ICT processes, which are already covered by the Cyber Security Regulation (proposal for a regulation amending Regulation (EU) 2019/881 as regards managed security services, 2023, p. 1). Managed security services are playing an increasingly important role in preventing and mitigating cybersecurity incidents.

The proposed changes are limited to what is strictly necessary and do not change the operation or features of the Cyber-security Regulation.

Through the Cybersecurity Regulation, the European Union has introduced a unique EU-wide certification framework, which: builds trust; further drives the growth of the cyber security market; facilitates trade across the European Union.

The certification framework will convey certification policies at European level similar to a grouping of procedural norms, rules, and guidelines and standardization. The new regulatory framework will have as its central point an EU-level agreement on the possibility to evaluate the security features of ICT-based products or services. It will certify that ICT products and services that have been certified under such a scheme comply with specified requirements.

We would like to highlight that each European system should specify: the categories of products and services covered; cybersecurity requirements, such as standards or technical specifications; the type of assessment, such as self-assessment or third-party; desired insurance level.

Moreover, the single certification framework provides a comprehensive set of rules, technical requirements, standards and procedures.

A body that has a decisive par in cyber-security at the level of the European Union is the European Union Agency for Cyber-Security. The new European Union Cyber-Security Agency is based on the same structural system of its predecessor, the European Union Agency for Network and Information Security, now having a stronger part and a stronger mandate that is characterized by permanence. In addition, the agency has the same abbreviation, ENISA (Regulation EU 2019/881 of 17 April 2019 on ENISA and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013, 2019, pp. 3-21). The European Union Agency for Cyber-Security supports Member States, European Union institutions and other stakeholders to manage cyber-attacks.

The European Union Cyber-Security Agency's target is to obtain a powerful and efficient level regarding the securing of network system and information within the EU. The agency, together with the bodies of the EU and the member states of the EU, aims to develop a culture of cyber security for the benefit of citizens, consumers, public sector organizations and businesses within the EU. The agency also helps the European Commission, the member states of the EU and the business community to address, respond to and prevent cyber-security issues (Dupré, 2014, p. 2). The European Union Cyber-Security Agency supports the Member States of EU to implement the relevant legislation at the level of EU and to improve the resilience of the critical information infrastructure in the European Union.

Therefore, the European Union Cyber-Security Agency aims to strengthen the existing expertise in the national countries of the EU by supporting the development of cross-border communities, obliged to improve the security of networks and information in Europe.

At the level of the European Union, in addition to the the European Union Cyber-Security Agency, we emphasize that there are also other actors involved in the field of cyber security, such as: Europol and the Digital Agenda for Europe.

THE EUROPEAN UNION STRATEGY IN THE FIELD OF CYBER-SECURITY

At the Europol level, the European Center for Combating Cybercrime has been operating since 2013. The European Center for Combating Cybercrime aims to track illegal online activities carried out by organized crime groups, in particular attacks on electronic banking and other online financial activities, online sexual exploitation of children and those crimes affecting critical infrastructure and IT systems within the European Union. In order to dismantle more cybercrime networks and to prosecute more suspects, the European Center for Combating Cybercrime collects and processes cybercrime data and provides a support service for law enforcement bodies in the Union countries European. It provides operational support to European Union countries. e.g. against intrusion, fraud, online child sexual abuse and high-level technical, analytical and forensic expertise in joint investigations within the European Union.

The European Center for Combating Cybercrime enables research, development and capacity-building for law enforcement and conducts threat assessments, including trend analyses, forecasts and early warnings.

The Digital Agenda for Europe represents one the key points of the Europe 2020 Strategy developed by the European Commission and aims to elaborate the essential driving part, that the utilization of information and communications technology will have to play in achieving the objectives of the Europe 2020 Strategy. The objective of the Digital Agenda for Europe refers to exploiting to the maximum the potential of information and communications technology to encourage scientific discovery, the development and economic progress. It also supports the development of a digital single market to deliver smart, sustainable and inclusive growth in Europe. We highlight the fact that the Digital Agenda for Europe also has concerns in the field of cyber security. As the Internet has now become such an important information infrastructure for citizens and for the European economy in general, the Digital Agenda for Europe believes that IT systems and networks must be secured and made to withstand a multitude of new threats.

By Regulation (EU) 2019/1020, known as Cyber Resilience Act, which is another important legal instrument in cyber-security field, ensures that businesses and consumers are effectively protected against cyber-threats.

In order to ensure that products with digital components, such as home cameras, refrigerators, TVs and smart connected toys, are safe before they enter the market, representatives of Member States have reached a common position on legislative proposal of 15 September 2022 on horizontal cybersecurity requirements for products with digital elements, such as the proposal for a regulation on horizontal cybersecurity requirements for products with digital elements digital and amendment elements of Regulation (EU) 2019/1020.

The proposed regulation introduces mandatory cybersecurity requirements for the design, development, production and making available on the market of hardware and software products to avoid overlapping requirements arising from

different pieces of legislation in European Union Member States (Proposal for a regulation on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020, 2022, pp. 1-40) .

II. DIRECTIVE ON THE SECURITY OF NETWORKS AND INFORMATION SYSTEMS

One of the most important legal instruments at the European level in the field of cyber-security is the Directive on the security of networks and information systems (NIS), which entered in force in 2016, being the first legal tool ever adopted at European Union level with the aim of development of collaboration between national countries from EU in the field of cyber-security.

Through this legal instrument, the NIS Directive, we emphasize that security duties have been established for service providers of services in the following areas, such as energy, transport, medical and sanitary and public finances and for providers of digital services (digital markets and cloud services) (Directive EU 2016/1148 of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, 2016, pp. 3-10) .

In 2022, the European Union adopted a revised NIS Directive, the Directive EU 2022/2555 of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS 2) to replace the 2016 directive NIS.

We noticed that the new rules ensure a high degree of cyber-security at European level, in response to the new cyber-attacks that are constantly increasing and considering the transformations in the digital world, which has been energized and influenced by the worldwide problem of infections with the Covid 19 virus.

The new European Union legislation, such as the NIS 2 Directive (Directive EU 2022/2555 of 14 December 2022 on measures for a high common level of cybersecurity across the Union, 2022, pp. 1-10): identifies new standards at a minimum level for a legal framework; defines effective collaboration mechanisms between law enforcement bodies in each EU member state; reviews the actions and areas that are included in the category of IT security obligations.

The NIS 2 Directive entered into force on 16 January 2023 at the level of the European Union.

The European Union wants to introduce mandatory cyber-security requirements for hardware and software products with a connected digital element, such as smart TVs or other household appliances, baby monitors, toys.

CONCLUSIONS

In conclusion, the development and regulation of a strategy at the level of EU in the field of cyber-security represents an important objective for the the national security policy of each national country from EU.

The European security political actors have highlighted the need to regulate an adequate European framework in the field of cyber-security, which must be effective against the numerous threats in cyberspace.

Moreover, the elaboration of the Cyber-Security Strategy 2020-2025 requires respect for fundamental human rights and freedoms, such as, for example, the right to private life or the protection of personal data in the electronic communications sector.

We believe that the national countries of EU must adopt as quickly as possible a national strategy on the security of Internet networks and IT systems that defines the strategic objectives and the appropriate political and regulatory measures and contained in the Cyber-Security Strategy 2020-2025 at the level of the European Union, in order to obtain and allow maintaining a high level of security of Internet networks and IT systems.

BIBLIOGRAPHY

1. Dupré Lionel (2014), European Union Agency for Network and Information Security, *Four Years of Pan-European Public Private Cooperation*, EP3R 2010-2013, November 2014;
2. European Commission, *Proposal for a regulation of the European Parliament and of the Council amending Regulation (EU) 2019/881 as regards managed security services*, Strasbourg, 18.04.2023, COM(2023) 208 final;
3. European Commission, *Proposal for a regulation of the European Parliament and of the Council* on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020, Brussels, 15.09.2022, COM(2022) 454 final, 2022/0272 (COD);
4. The Regulation EU 2019/881 of the European Parliament and of the Council of 17 April 2019 on 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, 07.06.2019, L 151/15;
5. Directive EU 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, Official Journal of the European Union, 19.07.2016, L 194/1;
6. Directive EU 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive), 27.12.2022, L 333/80.