ISRG Journal of Economics, Business & Management (ISRGJEBM)

ISRG PUBLISHERS
Abbreviated Key Title: Isrg J Econ Bus Manag
ISSN: 2584-0916 (Online)
Journal homepage: https://isrgpublishers.com/isrgjebm/
Volume – III, Issue -I (January- February) 2025
Frequency: Bimonthly

Economy and cybersecurity in the European Union

Lect. Univ. Dr. Leonard Artur Horvath

Faculty of Economic Sciences and Business Management, Babes-Bolyai University, Cluj-Napoca,400084, Romania.

| **Received:** 10.02.2025 | **Accepted:** 15.02.2025 | **Published:** 17.02.2025

***Corresponding author:** Lect. Univ. Dr. Leonard Artur Horvath

Faculty of Economic Sciences and Business Management, Babes-Bolyai University, Cluj-Napoca,400084, Romania.

Abstract

The present study aims to answer a few questions related to the new cybersecurity and economic strategy of the European Union in recent years, but also to the future one, including public policies in the field, which the EU wants to implement. All of these ideas and issues have become a priority for the European Commission and EU Member States with new cyber-attacks that have multiplied during the COVID-19 pandemic, decreed by WHO in all areas of activity, following the imposition of the rapid process of digitization of states, in the middle of the period of fighting the virus.

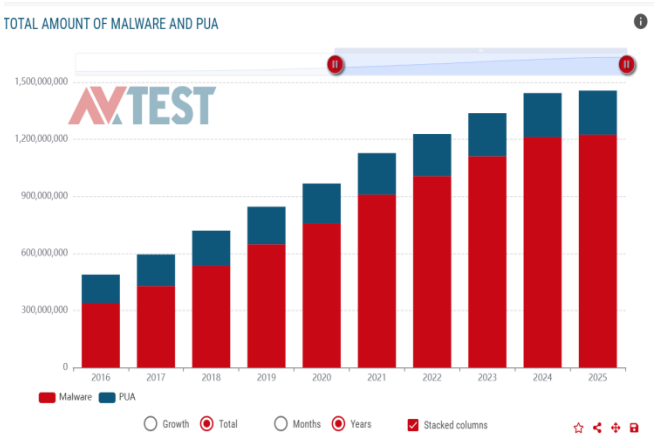
Keywords: *economy, cybersecurity, european union, geopolitic, globalization.*

Introduction

Nowadays it is almost obvious that globalization, economic security and cyber security are becoming more and more present in our lives or in the international relations arena. The global economy is connected in all countries thanks to new technologies, from facilitating the Internet as a means of communication to economic transactions, stock exchanges and online bank accounts, which make the system vulnerable both at the level of society and at that of a region or nation.

In recent years, but especially during the COVID-19 outbreak, the digital world has been found to bring enormous benefits to society, but it is also very vulnerable. The number of cybersecurity incidents, whether intentional or accidental, is growing at an alarming rate and could disrupt the provision of essential services that we consider essential, such as water or electricity, healthcare, or mobile phone services. Threats can come from various sources, such as criminal, terrorist, politically motivated, or state-ordered attacks, as well as natural disasters or unintentional mistakes.

DOI: 10.5281/zenodo.14881946



General situation regarding malware and software attacks according to AVATLAS source https://portal.av-atlas.org/malware

Nowadays, IT networks and systems are widely used by citizens, organizations and businesses across the European Union. Digitization and connectivity are becoming key features of an increasing number of products and services, with the advent of the internet in the 1990s, an extremely high number of connected digital devices are expected to enter into use in the European Union in the next decade. Although the number of devices connected to the Internet is increasing, security and resilience are not analyzed, treated and included by the manufacturer as building blocks at the production stage, resulting in poor cyber security and exposed to attacks.

In this context, due to the limited use of system certification, individual users, organizations or businesses do not have sufficient information about the cybersecurity features of Information and Communication Technology products, which erodes trust in digital solutions. Network and information systems are capable of supporting all aspects of our lives, but also of bringing about the economic growth of the European Union. All these are fundamental elements for the realization of the Digital Single European Market.

In order to mitigate those risks, it is necessary to take all measures to improve cybersecurity within the European Union so that networks and information systems, communication networks, products, economic services and digital devices used by citizens and organizations become much safer.

With cyber attacks on the rise, a connected economy and society becomes more vulnerable to cyber threats and attacks, which requires stronger protection from the bodies managing these areas of digitalization and cyber security. However, while cyber attacks are often cross-border, the competence and responses provided by cybersecurity and law enforcement authorities' policies are predominantly national.

Thus, reconsidering the role of the state as an active player in the area of computer-economic security environment and delimiting new categories of threats that are specific to the globalization process, have led to a questioning of the concept of security through different concepts and questions about: "Who is threatening?" "What is threatening?" "What is the sector, branch or part of the economy that is most exposed and vulnerable to these threats in order to react, develop and counter these threats that make an important element of the social-economic and implicitly state security weaken?".

The European Union is a stable economic factor in the IT area

States remain responsible for the national security, scale and cross-border nature of the threat. All this makes a strong case for European Union action to provide incentives and support to Member States to develop and maintain enhanced and improved national capabilities in the field of cybersecurity, which relate to the security of physical and economic data, while also building European Union-wide capabilities and capabilities to protect economic transactions in the online system.

This approach aims to mobilize all European Union actors, Member States, industry and citizens in order to give cybersecurity the necessary priority to strengthen this area and to provide a better response from the European Union to cyber attacks (The EU's Cybersecurity Strategy for the Digital Decade, p. 14-17).

However, we can see that the European Union has taken important steps in time to ensure cyber security and to increase confidence in digital technologies. In 2013, the European Union's Cybersecurity Strategy was adopted to guide policies, by which the EU responds to cyber threats and cybersecurity risks.

As part of the efforts to better protect citizens online, the first Union legislative act in the field of cybersecurity was adopted in 2016 in the form of Directive (EU) 2016/1148 of the European Parliament and of the European Council.

The Directive established requirements on national capabilities in the field of cybersecurity, created the first mechanisms to enhance strategic and operational cooperation between Member States and introduced obligations on security measures and incident notifications in sectors vital to the economy and society, such as energy, transport, drinking water supply and distribution, banks, financial market infrastructure, healthcare, digital infrastructure, as well as providers of digital services essential to the economic area.

But with the changes following the growth of cyber attacks during the COVID-19 pandemic in 2020 (Eurostat Press release, ICT security measures taken by vast majority of enterprises in the EU', 6/2020 - 13 January 2020. Cyberattacks on critical infrastructure have become the new normal across sectors such as energy, healthcare and transportation; WEF, The Global Risks Report 2020), the European Union has adopted a new cybersecurity strategy which aims to ensure internet access for all economic actors, but also for European citizens, and which also provides safeguards not only to ensure security, but also to protect the European economy and values. Based on the situation of the last few years, the strategy includes concrete proposals for regulatory initiatives, investment in economic infrastructure, but also policies in vital areas of the EU such as that of standardization in the collection of taxes in the economic sector. The existing measures together with the new ones proposed at EU level are intended to protect its essential economic services and infrastructure against physical risks and cyber attacks. Cybersecurity risks continue to evolve with increasing digitalization and interconnection. In this way, the European banking sector is always seeking to offer its customers high-performance digital products protected from cyber attacks. Physical risks have also become more complex since the adoption of the 2008 EU rules on critical and economic infrastructure, which currently cover only important economic sectors such as energy and transport.

Cybersecurity is thus one of the main priorities of the European Commission and one of the cornerstones of the digital and connected Europe. The increase in cyber attacks during the

DOI: 10.5281/zenodo.14881946

COVID-19 crisis has shown how important it is to protect hospitals, research centers and other key economic infrastructure. Firm action in this area is needed to guide the EU economy and society towards the future.

The new cybersecurity strategy proposes to integrate cybersecurity into every element of the economic supply chain and to better link EU activities and resources across the four cybersecurity communities — the internal market, law enforcement, diplomacy and defense. All this depends on IT investments as an integral part of a high performing economic sector. It builds on the EU approach to shaping Europe's digital future and the EU Security Union Strategy (The EU Cybersecurity Strategy) and builds on a number of legislative acts, actions and initiatives that the EU has implemented to strengthen cybersecurity capabilities and to ensure a more economically resilient and cyber-resilient Europe.

These include the 2013 cybersecurity strategy, revised in 2017, and the European Commission's European security agenda for 2015-2020. The new strategy also recognizes the increasing interconnection between internal and external security, in particular through the common foreign and economic security policy.

However, the risk of cyber attacks also in important sectors of the economy remains difficult to estimate, as sometimes the data needed to predict with certainty their probability and consequences is missing, giving rise to subjective interpretations.

As a rule, for security institutions such as the banking sector, the disastrous consequences of a large-scale cyber attack outweigh the low probability of this happening. Thus, there is a tendency to overstate the risk of terrorism and cyber war. At the same time, for individuals or economic companies, the low impact of some episodes of cybercrime and hacking leads to an understatement of risk, despite the high frequency of these incidents and significant cumulative losses.

Studies in the field and beyond suggest that the economic impact of cybercrime has increased fivefold between 2014 and 2019 and could increase up to four times by 2022 (McAfee & Center for Strategic and International Studies Net losses: Estimating the Global Cost of Cybercrime, 2014). Ransomware has developed in particular, with the latest attacks reflecting a dramatic increase in cybercrime activities in the economic area. In May 2017, the "WannaCry" cyberattack using a digital blackmail program affected more than 400,000 computers in more than 150 countries. A month later, the cyber attack "Petya", which used a digital blackmail program, hit Ukraine and a number of societies around the world.

In order to combat these cyber attacks, in October 2019, but also in 2020, EU Member States discussed the creation of an innovation laboratory within Europol, which could be in charge of monitoring new technological developments and stimulating innovation in the area of internal security, and one important chapter is the economic area.

Cyber threats come from both state and non-state actors. They are generally profit-driven, but can also be political, economic and strategic. Failure to protect the devices that will control our power grids, cars and transport networks, factories, finances, hospitals and homes could have devastating consequences and profoundly affect consumer confidence in emerging technologies. The risk of politically motivated attacks on civilian targets and shortcomings in military defense against cybercrime further increase the danger.

The digital transformation of society, intensified by the COVID-19 crisis, has expanded the threat landscape and creates new challenges requiring tailored and innovative responses. The number of cyber attacks continues to grow, including in 2024, have become increasingly sophisticated from a wide range of sources, both within and outside the European Union, and have affected multiple sectors of the economy.

Therefore, the European Union should lead efforts towards secure digitization. This should lead to the adoption of rules for world-class solutions and cybersecurity standards for essential services and critical infrastructure, including in the area of the economy, as well as to the development and application of new technologies. Governments, businesses and citizens will all have the responsibility to ensure a secure digital transformation on the Internet that does not cause major fluctuations in the economy.

What is the 2020 strategy proposing?

It describes how the EU can leverage and consolidate all its instruments and resources to be technologically sovereign. It also shows how the EU can enhance its cooperation with partners around the world who share the values of democracy, the rule of law and human rights.

The new security strategy has expanded and covers the old one, including key areas such as hospitals, energy networks, railways and an increasing number of connected objects in homes, offices and businesses. The strategy aims to build collective capacities to respond to major cyber attacks in all sectors of the economy. It also outlines plans to work with partners around the world to ensure international security and stability in cyberspace as a factor for economic stability. In addition, it highlights how a joint IT unit can ensure the most effective response to cyber threats, using the resources and collective expertise available to Member States and the EU.

What is the major objective of the new 2020 security strategy?

It aims to ensure a global and open internet with strong safeguards where there are risks to the security and fundamental rights of European citizens. Following the progress made in previous strategies, it contains concrete proposals for the implementation of three main instruments. These three instruments are regulatory, economic investment and policy initiatives for the European Union and the Member States.

Technological sovereignty and leadership

Under this strand, the European Union has proposed to reform the rules on the security of network and information systems in a Directive on measures for a high common level of cybersecurity in the European Union, known as the NIS 2 Directive, in order to strengthen the cyber resilience of critical public, economic and private sectors: hospitals, energy networks, railways, but also data centers, public administrations, research laboratories and centers manufacturing critical medical devices and medicines as well as other critical infrastructure and services must remain impermeable in an environment where threats are increasingly complex and evolving rapidly (New Cybersecurity Strategy EU Digital Decade and its impact for Romania).

The European Commission proposed to launch an EU-wide network of security operations centers based on artificial intelligence, which would constitute a real cybersecurity shield for the EU, capable of detecting signs of a cyber attack early and allowing action to be taken before material or economic damage occurs. The EU's Cybersecurity Strategy in the Digital Decade.

DOI: 10.5281/zenodo.14881946

Other measures are targeted at providing targeted economic support to small and medium-sized enterprises in digital innovation centers, increasing efforts to upgrade the skills of the workforce, attract and retain the most talented people in cybersecurity, and investing in open, competitive and excellence-based research and innovation.

Strengthening prevention operational capacity

The European Union is preparing, through a progressive and inclusive process with the Member States, the creation of a new common cybersecurity unit. It will strengthen cooperation between EU bodies and Member States' authorities responsible for preventing and deterring cyber attacks and responding to them, including the civil community, law enforcement authorities, the diplomatic environment and cyber defense entities.

At the forefront are cyber activities that can affect critical and economic infrastructure, supply chains, democratic institutions and processes. The EU will also work to further strengthen cooperation in the field of cyber defense and develop state-of-the-art cyber defense capabilities. To do this, the European Union will build on the work of the European Defense Agency and encourage Member States to make full use of the permanent structured cooperation and European Defense Fund.

Promoting a global cyberspace

The European Union is committed to supporting the new cybersecurity strategy through unprecedented investments in the EU's digital transition over the next seven years, the EU 2021-2027 budget, in particular the Digital Europe Program and Horizon Europe, and the Recovery Plan for Europe. Member States are therefore encouraged to make full use of the EU Recovery and Resilience Facility to increase cybersecurity and reflect the level of EU investments. The objective is to achieve combined investment by the EU, the Member States and the IT sector, in particular within the Cybersecurity Competence Center and the network of coordination centers in different European Union countries.

Conclusions

The European Commission aims to strengthen the EU's industrial and technological capabilities in the area of economic and cyber security, including through projects supported jointly with funds from the EU and national budgets. The EU has a unique opportunity to pool its resources to strengthen its strategic autonomy and leadership in cybersecurity throughout the digital supply chain, including data and cloud, next-generation processor technologies, highly secure connectivity and 5G networks, in line with its values and priorities.

Under the new cybersecurity strategy, Member States, with the support of the European Commission and the European Union Agency for Cybersecurity, are encouraged to complete the implementation of the EU 5G toolbox, which provides a comprehensive and objective risk-based approach to the security of 5G networks and future generations of networks.

According to a recently published report on the impact of the European Commission Recommendation on 5G cybersecurity and on the state of implementation of the EU toolbox of mitigation measures since the July 2020 progress report, most Member States are already at an advanced stage in implementing the recommended measures. They should now aim to complete implementation by the second quarter of 2021 and ensure that the identified risks are adequately mitigated in a coordinated manner, in particular with a view to minimizing exposure to and avoiding dependency on high-risk providers. The Commission is also today setting out the main objectives and actions for further coordinated work at EU level.

In conclusion, the European Union's Economic and Cybersecurity Strategy proposes to integrate cybersecurity into the economy, in every element of the supply chain and to better link EU activities and resources across the four cybersecurity communities in the internal market, law enforcement, diplomacy and defense (The EU's Cybersecurity Strategy for the Digital Decade, p 6-9, Brussels).

All these new phenomena and new challenges are in a constant struggle in the era of globalization and are connected to each other thanks to new technologies, facilitating the transition from a world in which power has always been represented by the military force of each state, to a world in which, increasingly, individuals and their communities are facing new threats and challenges, in which many of the known forces and political ideas of recent decades cannot guarantee the national and collective security of a constantly changing society.

Bibliography

Primary sources

1. Council Conclusions call for horizontal measures on the cybersecurity of connected devices; 13629/2020, 2 December 2020
2. 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, available also on (OJ L 194, 19.7.2016, p.1), accessed date 08.01.2025
3. Eurostat Press release, ICT security measures taken by vast majority of enterprises in the EU', 6/2020 - 13 January 2020. Cyberattacks on critical infrastructure have become the new normal across sectors such as energy, healthcare and transportation; WEF, The Global Risks Report 2020
4. McAfee & Center for Strategic and International Studies Net losses: Estimating the Global Cost of Cybercrime, 2014
5. Position of the European Parliament of 12 March 2019 and decision of the Council of 9 April 2019
6. The EU Security Union Strategy 2020-2025, COM (2020) 605, final document
7. European Commission, The EU's Cybersecurity Strategy for the Digital Decade, pp 6-9, Brussels, 16.12.2020

Online sources

8. AV-TEST Institute Germany, available at https://www.av-test.org/en/statistics/malware/, date accessed 20.01.2025
9. Association for Technology and Internet, available on https://apti.ro/intrebari-directiva-securitate-cibernetica , date accessed 14.01.2025
10. CERT-RO, The EU's New Cybersecurity Strategy for the Digital Decade and its Impact for Romania, available at https://cert.ro/citeste/noua-strategie-de-securitate-cibernetica-a-ue-pentru-deceniul-digital-si-impactul-sau-pentru-romania, access date 28.12.2024

DOI: 10.5281/zenodo.14881946

11. European Commission, EU Cybersecurity Strategy, available on https://ec.europa.eu/digital-single-market/en/cybersecurity-strategy, date accessed 15.01.2025
12. European Council of 1-2 October 2020, Conclusions, available at https://www.consilium.europa.eu/ro/meetings/european-council/2020/10/01-02/, accessed 18.01.2025
13. the European Council, the EU Action Plan on Human Rights and Democracy 2020-2024,https://www.consilium.europa.eu/ro/press/press-releases/2020/11/19/council-approves-conclusions-on-the-eu-action-plan-on-human-rights-and-democracy-2020-2024/, date accessed 26.01.2025
14. European Commission, EU Cybersecurity Strategy, https://ec.europa.eu/romania/news/20201216_strategie_securitate_cibernetica_ue_ro, date of access 27.12.2024
15. European Commisson, EU Cybersecurity Strategy, available, https://ec.europa.eu/digital-single-market/en/cybersecurity-strategy?etrans=rodata, accessed 08.01.2025
16. Idem, available, https://ec.europa.eu/digital-single-market/en/news/eus-cybersecurity-strategy-digital-decade, access date 04.01.2025
17. MAE, Romanian Cybersecurity Strategy, 2019, available at http://www.mae.ro/node/28367, access date 23.12.2024
18. Organization for Economic Cooperation and Development, The COVID-19 crisis has placed an unprecedented demand on communication networks, available at https://www.oecd.org/coronavirus/policy-responses/keeping-the-internet-up-and-running-in-times-of-crisis-4017c4c9/, accessed on 06.01.2025

DOI: 10.5281/zenodo.14881946