Maksymenko Andrii
Postgraduate Student,
National University "Yuri Kondratyuk Poltava Polytechnic"

DOI: https://doi.org/10.36059/978-966-397-364-7-7

TRANSNATIONAL INSTRUMENTS TO ENSURE THE SECURITY OF THE EU DIGITAL ECONOMY

Costs of cybercrime are growing faster than the number of Internet users and world trade (Figure 1). This leads us to a threatening trend for the future if the dynamics of cybercrime are not slowed down soon or if the potential harms of these attacks and the benefits from the attacks for their beneficiaries stay the same or do not decrease.

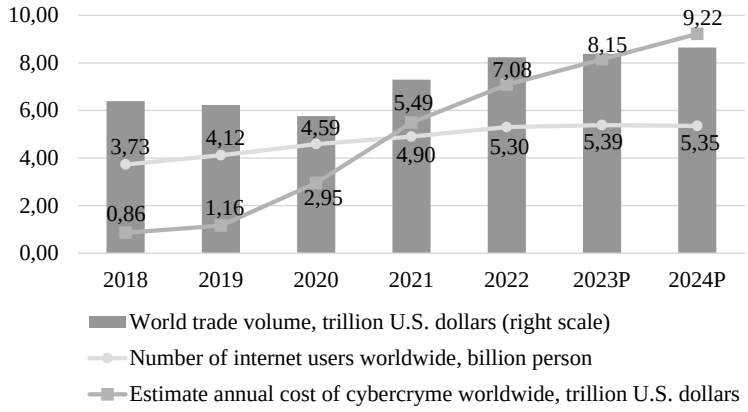

Figure 1. The dynamics of the digital economy and its threats 2018–2024 years

Source: created by the authors based on [1–4]

The figure shows that the main increase in cybercrime occurred in 2020–2022, despite the rather steady dynamics of growth in Internet users number and a slight drop in trade volumes related to the COVID-19 crisis.

This brings forward several questions: what is the reason for this increase and what countermeasures are there and can be further applied?

Several factors contributed to this almost twofold increase.

1. New Internet users come from crime-prone and less economically developed regions of Africa and Asia [5]. This contributes to an increase in the number of users interested in misusing the Internet.

2. Generally low level of technical literacy. Thus, almost 87% of personal data loss is due to social engineering [6].

3. As a result of the COVID-19 crisis, the workload of service providers has also increased, affecting their ability to prevent cyberthreats. Quick decisions made in times of crisis may contain many risk factors.

4. This is showcased by a change in the proportion between the interests of cyberattacks: if in 2020 financial motives outweighed espionage by about 6 times [6], as of 2022, the proportion is 1 to 1.5. Almost 25% of cybercrime in Europe was targeted at government agencies and administrations [7].

Consequently, there is a need to develop a supranational security system at the EU and European level, as well as relevant strategies and instruments.

Thus, the EU Economic Security Strategy aims to minimize the risks arising from certain economic flows in the context of increased geopolitical tensions and accelerated technological change while maintaining the maximum level of economic openness and dynamism. The debate on the formation and creation of the strategy began in 2023, and it was approved in 2024. The EU Cybersecurity Strategy aims to build collective capabilities to respond to major cyberattacks and outlines plans for cooperation with partners around the world to ensure international security and stability in cyberspace. It was first approved in 2013, and the latest version was published in 2020. The disharmony in regulatory support is emphasized by the formation of a strategy for providing infrastructure without protecting the object it serves. This leads to irrelevant spending on combating the consequences, rather than the causes, of threats to the digital economy.

Table 1

List of key transnational tools to ensure the security of the EU digital economy

Name	Description
The European Chips Act	It is on chips that a significant area of economic life relies. The dependence of the digital economy on semiconductors, and technological and production vulnerabilities from unstable supply chains have contributed to the deepening of the COVID-19 crisis. Countermeasures include the creation of joint scientific and technical capacity, financial investments and fundraising for risky domestic production, and the development of monitoring systems.
The Anti-Coercion Instrument	Allows for measures to be taken in cases of economic influence against the EU or its member states by third countries. The goal is to regulate coercion and to ensure adequate response to it, in order to protect union's interests through cooperation and concentration of joint efforts.
The Security of Network and Information Systems	Was introduced in 2016, and its revised version was adopted in 2022. It established security obligations for operators of key services in critical sectors and for digital service providers, and the updated version provides for increased diversification and competition of suppliers, which should limit dependence and stimulate system flexibility.
Cyber Resilience Act	Mandatory cybersecurity requirements for hardware and software products with a connected digital element.
The EU Toolbox For 5G Security	Is a tool for shaping the global digital economy, which concerns billions of connected objects and systems used in critical sectors. The mechanisms include support for a diverse and resilient 5G supply chain, regulatory frameworks, and access rules.
Dual-Use Export Controls	An important tool in the context of growing geopolitical instability and the Russian-Ukrainian war instrument, which establishes different regime options for EU countries regarding export controls, brokering, technical assistance, transit, and transfer of dual-use goods.
The European instrument for temporary support to mitigate Unemployment Risks in an Emergency (SURE)	Mobilized significant financial resources to combat the negative economic and social consequences of the coronavirus outbreak in the EU. It was created to help member states protect jobs. The advantage of such an instrument is the spread of positive impact from recipient members to the entire system through spillover effects of investment and economic stabilization.

ORBIS	Is a powerful comparative resource of data on private companies, their owners and ownership history, counterparties, and potential financial risks. This allows market participants to conduct financial intelligence to reduce their risks associated with contractors and reduces, transaction costs, as well as serves law enforcement agencies in their efforts to combat financial crime.

Turning to the specific instruments introduced in the EU, it is worth noting the trendsetting role of the Union on the continent, forcing other actors in the market to join the system. In the extensive list of tools available to the EU, we can identify the following regulatory acts and recommendations that form the basis and best convey the concept of ensuring the security of the digital economy in Europe (Table 1).

The main trends of these instruments are cooperation, communication, high-risk financing, advantages of the market economy, diversification of intermediaries, and strict legislative standardization of digital market participants. As a result, transnational instruments for ensuring the security of the digital economy are superior, since if the area of operation is limited to the national economy, the architecture will lack resources, capacity, and flexibility to counter the growing number of threats. This encourages deeper cooperation, both on the part of security actor states and organized crime or states that exploit threats and risks to their advantage.

The disadvantages of such instruments are their multiplicity, complexity, the need for significant political will for implementation, the cost of application, and their slowness. Since all participants have to accept the same conditions and regulatory restrictions, this contributes to lengthy negotiations, allowing risks to develop into threats and create excessive hazards in the system before a solution is developed.

Therefore, reactive urgent actions at the level of national economies will remain relevant for a long time until overall stabilization in the security of the digital economy and infrastructure, if it happens at all.

References:

1. Fleck A. Infographic: Cybercrime Expected to Skyrocket in Coming Years. *Statista Daily Data*. Available at: https://www.statista.com/chart/28878/expected-cost-of-cybercrime-until-2027/ (accessed March 1, 2024).

2. Lambert S. Number of Internet Users in 2024: Statistics, Current Trends, and Predictions. *Financesonline.com*. Available at: https://financesonline.com/number-of-internet-users/ (accessed March 2, 2024).

3. Evolution of trade under the WTO: handy statistics. *World Trade Organization*. Available at: https://www.wto.org/english/res_e/statis_e/trade_evolution_e/evolution_trade_wto_e.htm (accessed March 2, 2024).

4. Global Trade Outlook and Statistics (2023). Geneva: World Trade Organization, 28 p. Available at: https://www.wto.org/english/res_e/booksp_e/trade_outlook23_e.pdf (accessed March 2, 2024).

5. World Internet Users Statistics and 2023 World Population Stats. *Internet World Stats*. Available at: https://www.internetworldstats.com/stats.htm (accessed March 3, 2024).

6. Lourenço M. B., Marinos L. (eds.) (2020) Main incidents in the EU and worldwide / Attiki, Greece: European Union Agency for Cybersecurity (ENISA), 26 p. DOI: https://doi.org/10.2824/552242 (accessed March 3, 2024).

7. Svetozarov N. R., Lella M. (20220 A. Enisa Threats Landscape 2022 / ed. by N. R. Svetozarov et al. Attiki, Greece: European Union Agency for Cybersecurity (ENISA), 150 p. DOI: https://doi.org/10.2824/764318 (accessed March 3, 2024).

8. On "European Economic Security Strategy": Joint Communication To The European Parliament, The European Council And The Council of 20.06.2023 no. 52023JC0020: as of 26 January 2024. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52023JC0020&qid=1687525961309 (accessed March 3, 2024).

9. The EU's Cybersecurity Strategy for the Digital Decade: Joint Communication To The European Parliament And The Council of 16.12.2020: as of 24 December 2022. Available at: https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0 (accessed March 3, 2024).

10. Maksymenko A. REAL AND POTENTIAL THREATS TO THE DIGITAL ECONOMY IN WAR. Economic scope. 2023. DOI: https://doi.org/10.32782/2224-6282/188-7 (accessed March 3, 2024).