Cybersecurity, the challenge of the present

Cristiana SÎRBU,
University of Agricultural Sciences and Veterinary Medicine Bucharest, Faculty of Land Improvement and Environmental Engineering, "Gheorghe Ionescu Șișești" Academy of Agricultural and Forestry Sciences, Soil Science, Land Improvement and Environmental Protection Section, The Ecological Initiative and Sustainable Development Group Foundation
cris_sirbu@yahoo.com

Abstract
Cyber security can be defined as a sum of rules, technologies, processes, and controls to protect systems, networks, programs, devices and data from cyber attacks.Cybersecurity plays an important role in the field of information technology .Securing the information have become one of the biggest challenges in the present day. This paper mainly focuses on challenges faced by cyber security in the European Union and presents the latest policies in cyber security and the trends that changes the world daily.

Keywords: security, strategy, policies, digital.

1. Introduction

Nowadays, the whole world is talking about cyber security and cyber defence.

The digital transformation of society has expanded the threat landscape and is bringing about new challenges, which require adapted and innovative responses. The cyberworld and cyberspace are seen as another domain of war, as important as military, air, land or sea.

The number of cyber-attacks continues to rise, with increasingly sophisticated attacks coming from a wide range of sources both inside and outside the European Union.

The future is uncertain, with the trend expected to continue to grow.

2. Results and discussions

Cybersecurity is considered an extremely important part of national security. There is therefore a need to develop a cyber security culture among users of information and communication systems, who are often insufficiently informed about potential risks and solutions to counter them.

Cybersecurity is essential for people to trust, use, and benefit from innovation, connectivity and automation, and for safeguarding fundamental rights and freedoms, including the rights to privacy and to the protection of personal data and the freedom of expression and information [1].

As mention in the paper "Cybersecurity: information and defence against data phishing" by C. Sîrbu a number of critical sectors such as transport, energy, healthcare and finance have become increasingly dependent on digital technologies to run their core businesses. Digitalization offers enormous opportunities and provides solutions to many of the challenges facing Europe.

Enhancing cyber security and protecting critical information infrastructures are essential to each nation's security and economic wellbeing. Making the Internet safer (and protecting Internet users) has become integral to the development of new services as well as governmental policy.

In recent years, state and non-state actors have stepped up cyber-attacks, espionage and disinformation campaigns targeting the EU and its Member States, including the defence sector. The malicious activity of these actors has increased exponentially following Russia's military aggression against Ukraine.

European Union addresses cyber security with three pillars – network and information security, law enforcement, and defence – and defines national and EU-level entities responsible for ensuring cyber security.

The EU's cyber defence policy aims to strengthen cooperation and investment to better detect, deter, protect against and defend against a growing number of cyber attacks.

Cybersecurity involves protecting network and information systems (NIS), their users, and other affected individuals from cyber incidents and threats. To respond to the increased exposure of Europe to cyber threats, Directive 2022/2555, also known as NIS2, replaced its predecessor, Directive 2016/1148 or NIS1. NIS2 raises the EU common level of ambition on cyber-security, through a wider scope, clearer rules and stronger supervision tools.

NIS2 has the role to create a high common level of cybersecurity across the EU, keep essential services running, and protect the economy (and society) from cyber incidents.

The new strategy aims to ensure a global and open internet with strong safeguards where there are risks to the security and fundamental rights of people in Europe.

Building on progress made in previous strategies, it contains concrete proposals for the use of three main instruments. These three instruments are regulatory, investment and policy initiatives. They will address three areas for EU action:

- resilience, technological sovereignty and leadership;
- operational capability for prevention, deterrence and response;
- co-operation to promote a global and open cyberspace.

Recognizing the increasing scale, complexity, and frequency of cyber threats, exacerbated by global geopolitical tensions it is important to focus on a several key areas as [2]:

- Implementation and harmonization of the cybersecurity frameworks;
- Support for small and medium-sized enterprises and innovation for implementing cybersecurity measures;
- International cooperation;
- Addressing emerging threats;
- Strengthening institutional frameworks;

- Cybersecurity crisis management;
- Private sector engagement.

Moving into the future, it is not unreasonable to assume that technological dependency on others will increase.

While a cybersecurity strategy can help prevent a data breach or reduce the risk of malicious activity, a cyber resilience strategy specifically helps attenuate the impacts of these attacks.

Cyber Resilience is the ability to prepare, respond and recover from ciber attacks. It involves:

- Rapid and proactive threat detection using AI/ML technologies, coupled with continuous infrastructure monitoring;
- Coordinated incident response through continuity plans, CSIRT teams and clear communication processes;
- Accelerated recovery from any potential breach so that the business does not suffer significant disruption;
- Alignment with standards and regulations (NIS2, CRA, DORA), which emphasise the importance of rapid incident reporting and remediation plans;
- Public-private collaboration to share intelligence on new threats and defence tactics, including at the critical infrastructure level [3].

Cyber resilience is a concept that brings business continuity, information systems security and organizational resilience together.

3. Conclusions

In terms of emerging technologies, two topics have gained traction over the past two years, namely artificial intelligence (AI) and post-quantum cryptography (PQC). It is critical to ensure that research, development, and innovation funding is available for critical technologies and applications to boost global competitiveness in cybersecurity and to strengthen the EU's cybersecurity capabilities.

In 2025 cybersecurity becomes more than a protective shield. Trends over the past year, both globally and in Romania, show that the ability to resist, respond and recover quickly after an attack is the a top priority.

Acknowledgements

The study was conducted by The "Ecological Initiative and Sustainable Development Group" Foundation with the main purpose to be a connection between institutions, academia and civil society in order to inform and facilitate the access to information.

References

[1] European Commission, "Joint Communication To The European Parliament And The Council The EU's Cybersecurity Strategy for the Digital Decade," 16 December 2020. [Online]. Available: https://eurlex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020JC0018&from=ga.

[2] A. Pingen, "Council conclusions on the Future of Cybersecurity," EUCRIM Issue 2/2024, 21 June 2024. [Online]. Available: https://eucrim.eu/news/council-conclusions-on-the-future-of-cybersecurity/.

[3] Ziarul Financiar, "Cybersecurity Trends 2025 - How do we build resilience in the face of attacks?," 2025. [Online]. Available: https://evenimente.zf.ro/eveniment-zf-cybersecurity-trends-2025-22769143/despre-eveniment-22769133.