



A Brief Overview

AN ESSENTIAL LEGISLATIVE FRAMEWORK TO CYBERSECURITY IN THE EU

Radoslav Repa

radca

Kybernetická bezpečnosť a dôveryhodné služby

Stále zastúpenie SR pri EÚ v Bruseli



NÁRODNÝ
BEZPEČNOSTNÝ
ÚRAD

September 2023

KEY CHALLENGES

In the today's interconnected and digitally-driven world, cybersecurity has become a **critical concern** for governments, businesses, and individuals alike.

The European Union recognizes the **growing significance of cybersecurity** among its large-scale policies and over time has developed an unique and comprehensive framework of legislation to address the evolving challenges posed by cybersecurity threats.

A **weakest link concept** has been introduced in order to strengthen the preparedness and resilience of the EU's essential infrastructure to the cybersecurity risks including its Member States.

A fundamental principle has been applied to either **protect, detect, defend and deter** and/or to **prevent, discourage, deter and respond**.



CYBERSECURITY – NO LONGER A PRAISE!

Introducing a coherent cybersecurity legislation in the EU is not only necessary but also a **proactive response** to a rapidly evolving global digital landscape.

The **ever-increasing frequency of cyber attacks** underscores the need for strong and effective legislation. It also makes the case for why governments and organizations must take proactive measures to protect their digital infrastructure, sensitive data, and critical services.

Economic and Reputation Impact: Cyber attacks can result in significant economic losses for businesses, governments, and individuals.

Cross-Border Nature of Cyber Threats: Cyber attacks are not limited by geographical borders. They can be pushed from anywhere and affect entities globally. This emphasizes the necessity for harmonized approach to address cybersecurity challenges collectively.

Building a Secure Digital (European) Society: Robust legislation is a critical component of creating secure digital environment that promotes trust and confidence among users.



FACTS AND FIGURES

- European countries occupy 18 of the top 20 places in the ITU's Global Cybersecurity Index
- The value of the EU cybersecurity market is estimated at more than €130 billion and it is growing at a rate of 17% a year
- The EU has more than 60 000 cybersecurity companies and more than 660 centres of cybersecurity expertise



A few remarks on how it is made

Basically, the initiatives on cybersecurity within the complex institutional system of the EU are driven by focused policies promoted by **the European Commission** and/or the **High Representative** for Common Foreign and Security Policy.

In line with the European Commission's current priorities **to make Europe fit for the digital age** and **to build a future-ready economy that works for the people**, a current **EU Cybersecurity Strategy for 2020-2025** has been adopted.

In general, the initiatives can have either **legislative** (regulations, directives and decisions) or **non-legislative** nature (communications, recommendations, etc.).

When a legislation is published, the European Parliament and the Council start negotiating it. A good practice for the **Council**, depending on the leading presidency (a Member State), is to take its own position on a non-legislative communication in form of so called **conclusions** or resolutions. In the similar vein the EP can adopt its resolutions.

The Council is a place where Member States' official governments are represented and where the most intricate discussions of experts happen.



How does it look like?

The EU's cybersecurity legislation in most of cases is designed to address a whole range of stakeholders aiming at processes, methodology, competences/collaboration and sharing of information in order to **enhance functioning and harmonisation of the single market.**

Typical stakeholders can stand for:

- *Government Agencies and Regulatory Bodies*
- *Private Sector/Businesses*
- *Essential Service (Critical Infrastructure) Operators*
- *Digital Service Providers*
- *Consumers/Users*
- *International Collaboration*
- *Educational Institutions*



Introduction

I.-II. NIS/NIS2 Directive

III. Cybersecurity Act

IV. The European Cybersecurity Competence Centre and Network of National Coordination Centres Regulation

V. Cyber Resilience Act

VI. New Legislative Package

VII. Initiatives in Cybersecurity Related Domains

VIII. Latest Council's non-legislative initiatives

Questions and Answers?



I. NIS Directive

Directive on Security of Network and Information Systems is a cornerstone legislation which came into force in May 2018 to ensure a high common level of cybersecurity within the EU's Member States. The directive aims notably at organizations that provide services vital to society and economy.

The NIS Directive focused mainly on the following points:

Security Requirements: The directive mandates that operators of essential services (OES) and digital service providers (DSPs) take appropriate measures to manage risks and ensure the security of their network and information systems.

Incident Reporting: OES and DSPs are required to report significant cybersecurity incidents to the relevant national authority. This reporting helps in monitoring and responding to cyber threats more effectively.

Cooperation: The directive emphasizes the importance of cooperation and information sharing among EU Member States to handle cross-border incidents.

National Authorities: Member states are required to designate competent national authorities responsible for implementing and enforcing the provisions.

Penalties and Sanctions: The directive allows Member States to set penalties and sanctions for non-compliance with its requirements.



II. NIS2 Directive

While NIS has increased the Member States' cybersecurity capabilities, its implementation has resulted in fragmentation at different levels across the EU's internal market.

To respond to the imminent risks posed with digitalization and the surge in cyber attacks, the EU made a new proposal – **NIS2 Directive**, which entered into force in January 2023.

Its focus has been targeted to strengthen the **security requirements**, to address the **security of supply chains**, to streamline **reporting obligations**, and to introduce **more stringent supervisory measures and stricter enforcement requirements**, including **harmonised sanctions** across the EU.

The proposed expansion of the scope covered by NIS2, by **effectively obliging more entities and sectors to take measures**, would assist in further increasing the level of cybersecurity in Europe in the longer term.



III. Cybersecurity Act

The **Cybersecurity Act**, which became operational in June 2019, aimed at strengthening the EU's cybersecurity capabilities and readiness to create a more secure and trustworthy digital environment for individuals, businesses, and governments within the EU. This regulation introduced several important novelties and complemented the NIS Directive, by establishing a unified approach to cybersecurity certification and collaboration across EU Member States.

Key components of the Cybersecurity Act include:

European Cybersecurity Certification Framework (ECCF): The act establishes a framework for the certification of cybersecurity products, services, and processes across the EU. This framework aims to create a common standard for evaluating and certifying the cybersecurity of various digital products and services.

EU-wide Cybersecurity Certification Scheme: The act introduces the concept of EU-wide recognized cybersecurity certification schemes. These schemes are developed to ensure that products, services, and processes meet specific cybersecurity standards. This promotes trust and interoperability across the EU's digital landscape.

ENISA's Enhanced Role: The European Union Agency for Cybersecurity (ENISA) receives an enhanced mandate under the Cybersecurity Act. ENISA plays a pivotal role in supporting EU Member States in improving their cybersecurity capabilities and responding to cyber threats. The agency provides advice, guidelines, and expertise.

Cooperation and Information Sharing: The Act encourages cooperation and information sharing between MS and relevant stakeholders to enhance overall cybersecurity readiness and response. This cooperation is crucial for addressing cross-border cyber threats effectively.



IV. European Cybersecurity Competence Centre and Network Regulation

This regulation aims at increasing **cybersecurity expertise, research, and collaboration** within the EU. It came into force in June 2021. It establishes **the European Cybersecurity Competence Centre and Network of National Coordination Centres** and seeks to strengthen the EU's cybersecurity capabilities, promote innovation and collaboration among MS, industry and research institutions.

Key points of the regulation include:

European Cybersecurity Competence Centre (ECCC) focuses on cybersecurity research, innovation, and development. The centre established in Bucharest (Romania) seeks to work on advanced technological solutions, including new technologies and tools to counter cyber threats effectively.

Network of National Coordination Centres (NCC) collaborates with the ECCC and contributes to the development of cybersecurity solutions. This also supports capacity building and expertise sharing at the national level. „KCCKB“ in Slovakia.

Incident Response and Training: The ECCC and NCCs are designed to contribute to improving incident response capabilities across the EU. This includes sharing threat intelligence, coordinating response efforts, and providing training and capacity-building for cybersecurity professionals.

Research and Development: The ECCC aims to foster research and development in the field of cybersecurity, including emerging technologies such as artificial intelligence or secure communication networks. It facilitates cross-border collaboration among researchers, academia, and industry.

Public-Private Partnerships: The regulation encourages public-private partnerships to enhance collaboration between the public sector, private sector, and academia. These partnerships help to accelerate the development and deployment of innovative cybersecurity solutions.



V. Cyber Resilience Act (a proposal under discussion)

In September 2022 the European Commission presented a draft regulation for the **EU Cyber Resilience Act (CRA)**, which introduces **mandatory cybersecurity requirements for products with digital elements**.

The proposal covers a broad range of devices (incl. IoTs) - it would include **all products that are connected either directly or indirectly to another device or network**, including HW, SW and would **impose obligations on manufacturers, importers, and distributors of these products to provide duty of care across their whole life cycle**.

The proposal aims to **ensure better protection for consumers** through increasing the **responsibility of manufacturers by obliging them to provide security support and SW updates to address identified vulnerabilities**, and providing them with information about cybersecurity of products they buy and use.

The act would provide a **single set of rules for cybersecurity for companies**, it aims at decreasing the number of cybersecurity incidents and increasing the transparency and trust of consumers in products with digital elements.



V. Cyber Resilience Act (a proposal under discussion)

The proposed measures define:

- **rules for placing on the market** of products with digital elements through a process of conformity assessment (*self-assessment or third party conformity assessment, depending on the category of the product*) to demonstrate fulfilment of specific cybersecurity requirements, resulting in attribution of a CE marking.
- requirement for the **design, development and production** of such products and **reporting obligations for manufactures** to ensure cybersecurity throughout the life cycle of such products.
- **market surveillance and enforcement rules** performed through appointed market surveillance authorities.



VI. New legislative package 2023

In april 2023 European Commission published a **brand new cybersecurity package** with three proposals:

Draft **Cyber Solidarity Act** would seek to strengthen cybersecurity capacities in the EU. It would support detection and awareness of cybersecurity threats and incidents, bolster preparedness of critical entities, as well as reinforce solidarity, concerted crisis management and response capabilities across Member States.

In order to detect major cyber threats quickly and effectively, it suggests to create a **European Cyber Shield, which is a pan-European infrastructure of composed of national and cross-border Security Operations Centres (SOCs) across the EU**. These are entities would be tasked with detecting and acting on cyber threats.

A regulation also aims at creating a new **EU Cybersecurity Reserve** consisting of incident response services from pre-contracted trusted providers ready to intervene in case of a large-scale cybersecurity incident. It **may also provide financial support** for mutual assistance.



VI. New legislative package 2023

The second proposal - Draft Managed Security Services Act represents a **targeted amendment to the existing Cybersecurity Act to enable the future adoption of European certification schemes for managed security services**. These are highly critical and sensitive services provided by cybersecurity service providers, such as incident response, penetration testing, security audits and consultancy, to assist companies and other organisations to prevent, detect, respond or recover from cyber incidents.

The last component of the package is a **Communicaton on EU Cybersecurity Skills Academy** which will bring together private and public training cybersecurity skills initiatives at European and national levels, making them more visible and helping to close the cybersecurity talent gap of cybersecurity professionals in Europe.

The draft pieces of legislation are now under discussion at the Council and the European Parliament. The main goal of the institutions is to close negotiations **before the end the current legislative term (2Q/2024)** due to the forthcoming elections to the EP.



VII. Initiatives in Cybersecurity Related Domains

Several examples of non-exhaustive list:

- General Horizontal legislation (**GDPR**)
- **Digital** (eIDAS/eIDAS2, Data Act, Artificial Intelligence Act, Digital Europe Programme, Digital Services Act, etc)
- **Telco** (Electronic Communications Code, Data Privacy Act, 5G)
- **Finance** (DORA, PSD, Non-cash Means of Payment Frauds Directive, etc)
- **Interior** (Crime): Combatting Child Abuse Online, Attacks on Information Systems Directive, Critical Sectors Resilience Directive)
- **Justice** (Law Enforcement): Access to e-Evidence Regulation, Encryption Resolution (paving the way for a regulatory approach), Data Retention Regulation (no harmonisation after the ECJ's ruling)
- **Defence** (Communication on EU Policy on Cyber Defence)
- **Diplomacy** (Cyber Diplomacy Toolbox (CDT), Implementing Guidelines to CDT)



VIII. Latest Council's non-legislative initiatives

2021

- Council Conclusions on EU's Cybersecurity Strategy

2022

- Council Conclusions on EU Cyber Posture
- Council Conclusions on ICT supply chain security

2023

- Cyber Diplomatic Toolbox Implementing Guidelines revision
- Council Conclusions on Cyber Defense Policy
- Council Conclusions on Digital Diplomacy



QUESTIONS and ANSWERS?





Thank you for your attention

Radoslav REPA

Counsellor

Cyber Security and Trust Services (National Security Authority)



PERMANENT REPRESENTATION
OF THE SLOVAK REPUBLIC
TO THE EU

Avenue de Cortenbergh 79 | 1000 Brussels | Belgium

tel: +32 2 74 36 883 mob. +32 492 51 8686

radoslav.repa@nbu.gov.sk | <http://www.nbu.gov.sk>