NOTE ON CYBERSECURITY PACKAGE

DECEMBER 2020

On 16 December, **the Commission proposed a Cybersecurity Package which is an important part of the EU's digital transformation and recovery efforts**. The package consist of one strategic initiative and two legislative proposals:

1. EU Cybersecurity Strategy for the Digital Decade
2. Proposal for a Directive on measures for a high common level of cybersecurity across the Union ('NIS 2')
3. Proposal for a Directive on the resilience of critical entities (RCE)

EU CYBERSECURITY STRATEGY FOR THE DIGITAL DECADE

The EU Cyber Security Strategy aims to strengthen Europe's collective resilience against cyber threats, and to strengthen cooperation with partners around the world to promote a global, open, stable and secure cyberspace. Its actions are grouped into several pillars.

I. Resilience, technological sovereignty and leadership

Objective: Ensure resilience as well as industrial and technology capacities in cybersecurity through regulatory, investment, and policy instruments.

Key actions include:
- Adoption of **revised NIS Directive** (*see below for more details*)
- Regulatory **measures for an Internet of Secure Things**
  - These could include new horizontal rules to improve the cybersecurity of IoT, including a new duty of care for connected device manufacturers to address software vulnerabilities
- **Implementation of the 5G Toolbox** (by Q2 2021)
- Development of an **EU Domain Name System resolver service** as a safe and open alternative for citizens and businesses to access the Internet
  - This will offer an alternative EU service for accessing the global Internet, and become an element of the European Industrial Alliance for Data and Cloud
- **Investment in and adoption of cybersecurity technologies**, including through Digital Innovation Hubs

II. Building operational capacity to prevent, deter and respond

Objective: Assist Member States, through regulatory tools and increased cooperation, to prevent and deter cyberattacks that could impact economic and national security interests

Key actions include:
- Take steps towards the establishment of the **Joint Cyber Unit (JCU)**
  - The JCU will serve as a **platform for cooperation** between the different cybersecurity communities in the EU to ensure cyber **preparedness, situational awareness** and **coordinated response**.
- Review the **Cyber Defence Policy Framework**
  - The review will enhance cooperation between the member states in regards to Common Security and Defence Policy operations
- **Implement the cybercrime agenda** under the Security Union Strategy

- Support **synergies between civil, defence and space** industries (**Q1 2021**)
- Present the EU "**Military Vision and Strategy on Cyberspace**"

III. Advancing a global and open cyberspace

Objective: Promote, with international partners, a political model and vision of cyberspace based on EU values and norms.

Key actions include:

- **Define objectives in international standardisation processes** to ensure EU leadership in cyber standardisation
- Advance **international security and stability** in cyberspace
- Reinforce **exchanges with the multi-stakeholder community** (e.g. African Union, the ASEAN Regional Forum, OSCE) and expand EU cyber **dialogue with third countries**
- Propose an **EU External Cyber Capacity Building Agenda** to support EU partners in strengthening their cyber resilience

The last point of the Strategy relates to **renewed efforts to increase the cyber resilience of the EU bodies** and to establish common cybersecurity rules for those bodies.

PROPOSAL FOR A DIRECTIVE ON MEASURES FOR HIGH COMMON LEVEL OF CYBERSECURITY ACROSS THE UNION ('NIS 2')

Scope

NIS 2 is proposed in the form of a minimum harmonisation[1] directive. The proposal expands the scope of the current NIS Directive by adding new sectors **based on their criticality** by introducing **a size cap.** This means that **all medium and large companies** in chosen sectors will be included in its scope. It also leaves open the possibility of Member States identifying smaller entities with a high-security risk profile. Further, NIS 2 eliminates the distinction between operators of essential services and digital service providers, and **categorises entities into essential and important,** with the consequence of being subjected to different supervisory and penalty regimes, but having the same risk management requirements and reporting obligations.

Its **Supervisory regime** distinguishes between an ex-ante supervisory regime for essential entities and an ex-post supervisory regime for important entities, with the latter obliging competent authorities to take action when provided with evidence or indication that an important entity does not meet the security and incident notification requirements.

Penalties could reach a maximum **10 M EUR or up to 2% of total worldwide annual turnover** of the undertaking to which the essential or important entity belongs in the preceding financial year (whichever is higher).

Essential entities: Energy (electricity, district heating and cooling, oil, gas and hydrogen); Transport (air, rail, water and road); Banking; Financial market infrastructures; Health; Manufacture of pharmaceutical products including vaccines, and of critical medical devices; Drinking water; Wastewater; Digital infrastructure (internet exchange points; DNS providers; TLD name registries; cloud computing service providers; data centre service providers; content delivery networks; trust service providers; and public electronic communications networks and electronic communications services); Public administration; and Space.

[1] Minimum harmonisation means that the Member States could adopt or maintain provisions ensuring a higher level of cybersecurity when transposing its provisions to the national law.

Important entities: Postal and courier services; Waste management; Chemicals; Food; Manufacturing of other medical devices, computers and electronics, machinery equipment, motor vehicles; and Digital providers (online market places, online search engines, and social networking service platforms).

Cybersecurity risk management and reporting obligations

All entities which fall under the scope of NIS 2 must undertake **specific cybersecurity-related training,** and **approve the following technical and organisational cybersecurity risk management** measures:

- Risk analysis and information system security policies;
- Incident handling (prevention, detection, and response to incidents);
- Business continuity and crisis management;
- Supply chain security including security-related aspects concerning the relationships between each entity and its suppliers or service providers such as providers of data storage and processing services or managed security services;
- Security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure;
- Policies and procedures (testing and auditing) to assess the effectiveness of cybersecurity risk management measures;
- The use of cryptography and encryption.

The technical and methodological specifications of the elements will be specified by implementing acts.

All entities would need **to notify the competent national authorities or the CSIRTs**[2] of any cybersecurity **incident having a significant impact** on the provision of the service they provide. An incident is considered significant if: (a) the incident has caused or has the potential to cause substantial operational disruption or financial losses for the entity concerned; (b) the incident has affected or has the potential to affect other natural or legal persons by causing considerable material or non-material losses. Where appropriate, entities are also required to inform their service recipients of particular and significant threats and of measures they can take to mitigate the resulting risk to themselves.

The proposal foresees a **two-stage approach** to incident reporting. **First,** entities are required to submit an initial notification within 24 hours. The initial notification should only include the information strictly necessary to make the competent authorities aware of the incident and allow the entity to seek assistance if required. The CSIRT shall provide additional technical support if the concerned entity so requests. Where the incident is suspected to be of criminal nature, it shall be reported to law enforcement authorities. **Second,** entities are required to provide a final detailed report no later than one month after the submission of the initial report.

Supply chain security

NIS 2 addresses security of **supply chains and supplier relationships** by requiring individual companies **to address cybersecurity risks in supply chains and supplier relationships**. At the European level, the proposal strengthens supply chain cybersecurity for key information and communication technologies. Member States in cooperation with the Commission and ENISA will carry **out coordinated risk assessments of critical supply chains, building on 5G security toolbox,** with the aim of identifying per sector the critical ICT services, systems or products, relevant threats and vulnerabilities.

National cybersecurity frameworks and cooperation

Member States are required to adopt **national cybersecurity strategies** defining the strategic objectives and appropriate policy and regulatory measures with a view to achieving and maintaining a high level of cybersecurity. NIS 2 also **establishes a framework for Coordinated Vulnerability**

[2] The CSIRTs Network provides a forum where Member States can cooperate, exchange information, and improve the handling of cross-border incidents and even discuss how to respond in a coordinated manner to specific incidents.

Disclosure and requires Member States to **designate CSIRTs** to act as trusted intermediaries and facilitate the interaction between the reporting entities and the manufacturers or providers of ICT products and ICT services.

ENISA is required to develop and maintain a European vulnerability registry for the discovered vulnerabilities. Member States are **required to put in place National Cybersecurity Crisis Management Frameworks** by designating competent national authorities responsible for the management of large-scale cybersecurity incidents and crises. Member States are also required to designate one or more national competent authorities **on cybersecurity for the supervisory tasks and a single national point of contact on cybersecurity (SPOC) to exercise a liaison function to ensure cross-border cooperation** of Member State authorities.

The proposal also enhances the role of the **NIS Cooperation Group** in shaping strategic policy decisions on emerging technologies and trends, and increases information sharing and cooperation between Member State authorities. It also enhances operational cooperation, including on cyber crisis management.

Certification and standardisation

NIS 2 designates power to the Commission to adopt delegated acts establishing which **categories of essential entities shall be required to obtain a certificate** and under which specific European cybersecurity certification schemes.

NIS 2 also foresees that ENISA, in collaboration with Member States, will be responsible for adopting **guidelines regarding the technical areas** in which Member States should encourage the use of standards.

DIRECTIVE ON THE RESILIENCE OF CRITICAL ENTITIES

The proposal for a Directive on the resilience of critical entities (RCE) expands the scope of the existing EU rules on critical infrastructure. Ten sectors are now covered**: energy, transport, banking, financial market infrastructures, health, drinking water, wastewater, digital infrastructure, public administration, and space**. In contrast, existing EU rules had only applied to the energy and transport sectors.

This proposal is complementary to the NIS 2 directive and **does not regulate cybersecurity matters**, without prejudice to the particular regime for entities in the digital infrastructure sector[3], and covers all other relevant hazards, meaning that it accounts for all relevant natural and man-made risks, including accidents, natural disasters, antagonistic threats, including terrorist offences, and public health emergencies, including pandemics. **This is different from the European Critical Infrastructure Directive, which was primarily focused on terrorism.**

New rules to strengthen the resilience of critical entities

Obligations for critical entities:

- Critical entities would be required **to carry out a risk assessment**. This entity-level assessment would need to account for both the outcomes of the national-level risk assessment and local conditions and specificities.
- Critical entities would be subject to **common reporting obligations**, including entity-level risk assessments and incident notification, and would have **to take technical and organisational measures** to ensure their resilience.

[3] Entities pertaining to the digital infrastructure sector are in essence based on network and information systems and fall within the scope of the NIS 2. However, Member States should identify entities pertaining to the digital infrastructure sector that should be treated as equivalent to critical entities.

Obligations for Member States:

- Member States would be required to **adopt a strategy** for ensuring the resilience of critical entities, carry out an **all-hazards risk assessment**, and designate competent authority/authorities and a national point of contact.
- Member States would need to ensure that national authorities have the powers and means to **conduct on-site inspections of critical entities**. Member States should also introduce **penalties in case of non-compliance**.
- On the basis of the risk assessment, each Member State would have **to identify critical entities in different sectors**.

European cooperation:

- A Critical Entities Resilience Group, bringing together Member States and the Commission, will **evaluate national strategies** and facilitate **cooperation and exchange of best practices**.
- The Commission would provide **complementary support to Member States and critical entities,** for instance by developing a Union-level overview of cross-border and cross-sectoral risks, best practice, methodologies, cross-border training activities and exercises to test the resilience of critical entities.

NEXT STEPS

- NIS 2 and RCE will be subject to **negotiations between the Council and the European Parliament.**
- Member States would then have **to transpose the NIS 2 and RCE within 18 months of their entry into force**, once the proposals are agreed and consequently adopted.
- The Commission will have to **periodically review NIS 2** and report for the first time 54 months after its entry into force.