European Commission - Questions and answers

New EU Cybersecurity Strategy and new rules to make physical and digital critical entities more resilient – Questions and Answers

Brussels, 16 December 2020

Index

1. EU Cybersecurity Strategy for the Digital Decade
2. Proposal for a Directive on measures for high common level of cybersecurity across the Union (‘NIS 2')
3. Report on the impact of the Commission Recommendation on 5G Cybersecurity
4. Proposal for a Directive on the resilience of critical entities

1. EU Cybersecurity Strategy for the Digital Decade

What is the new EU Cybersecurity Strategy about?

The new Cybersecurity Strategy aims to safeguard a global and open Internet by harnessing and strengthening all tools and resources to ensure security and protect European values and the fundamental rights of everyone.

What is new in this Cybersecurity Strategy?

The strategic initiatives include:

- An EU-wide Cyber Shield composed of Security Operations Centres that use AI and Machine Learning to detect early signals of imminent cyberattack and allow action to be taken before damage is done;
- A Joint Cyber Unit that will bring together all of the cybersecurity communities to share awareness of threats and respond collectively to incident and threats;
- European solutions for strengthening Internet security globally, including an public EU DNS Resolver Service;
- Regulation to ensure an Internet of Secure Things;
- A stronger EU cyber diplomacy toolbox to prevent, deter and respond to cyber-attacks;
- Enhanced cyber defence cooperation, notably through the review of the Cyber Defence Policy Framework;
- A Programme of Action in the United Nations to address international security in cyberspace;
- More and stronger cyber dialogues with third countries and regional and international organisations, including NATO;
- An EU External Cyber Capacity Building Agenda and an EU inter-institutional Cyber Capacity Building Board to increase the effectiveness and efficiency of EU external cyber capacity building.

What do you mean by a ‘cyber shield'?

The EU needs an agile means for detecting and deflecting cyberattacks.

Currently Information Sharing and Analysis Centres, or ISACs, help stakeholders in industry and public authorities to exchange threat information. But we need also to constantly monitor networks and computer systems to detect intrusions and anomalies in real time.

Many private companies, public organisations and national authorities do this through Security Operations Centres.

This is a highly demanding and fast-paced work, which is why AI and in particular machine learning techniques can provide invaluable support to practitioners.

The Commission proposes to build a network of Security Operations Centres across the EU, and to support the improvement of existing centres and the establishment of new ones. It will also support the training and skill development of staff operating these centres. This network will provide timely warnings on cybersecurity incidents to authorities and all interested stakeholders, including the Joint Cyber Unit, like a mesh of watchtowers.

What is the Joint Cyber Unit and why do we need it?

The Commission President called for a Joint Cyber Unit in her political guidelines in 2019.

It would plug the gaps in and give a significant boost to reinforce the existing cooperation between EU institutions, bodies and agencies and Member States authorities in the event that various cyber communities are required to work closely together against major cross border cyber incidents or threat.

First, it would provide a space for the civilian, diplomatic, law enforcement and defence cybersecurity communities to work together.

Second, it would give cybersecurity stakeholders a focal point for sharing information about threats.

The Commission is committed to increasing the resources and capacities available for cybersecurity at the EU level to meet evolving threats, and to use such additional resources to contribute to the work of the Joint Cyber Unit.

Which amount of investment is planned in cybersecurity?

EU funding in the 2021-2027 Multiannual Financial Framework is envisaged for cybersecurity under the Digital Europe Programme, and for cybersecurity research under Horizon Europe, with special focus on support for small and medium businesses (SMEs), could amount to €2 billion overall plus Member States and industry investment.

Investments in the entire digital technology supply chain should amount to at least 20% - equivalent to €134.5 billion - of the €672.5 billion Recovery and Resilience Facility consisting of grants and loans.

The European Defence Fund (EDF) will support European cyber defence solutions.

How will the EU advance a global, open, stable and secure cyberspace?

The EU will step up its work to strengthen the rules-based global order, promote international security and stability in cyberspace, and protect human rights and fundamental freedoms online.

It will advance international norms and standards that reflect these EU core values, by working with its international partners in the United Nations and other relevant fora.

In addition, the EU will further strengthen its EU Cyber Diplomacy Toolbox, and increase cyber capacity building efforts in partner countries by developing an EU External Cyber Capacity Building Agenda.

Cyber dialogues with third countries, regional and international organisations as well as the multi-stakeholder community will be intensified.

2. Proposal for a Directive on measures for high common level of cybersecurity across the Union ('NIS 2')

Why does the Commission propose a new NIS Directive?

The digital transformation of society, which has been greatly (intensified during the coronavirus crisis) has expanded the threat landscape and is bringing about new challenges, which require adapted and innovative responses.

To be able to analyse the impact and identify the deficiencies of the current NIS Directive, the Commission carried out an extensive stakeholder consultation and identified the following main issues: (1) insufficient level of cyber resilience of businesses operating in the EU; (2) inconsistent resilience across Member States and sectors; and (3) insufficient common understanding of the main threats and challenges among Member States and lack of joint crisis response.

What are the key elements of the Commission proposal?

The new Commission proposal aims to address the deficiencies of the previous NIS Directive.

The Commission proposal expands the scope of the current NIS Directive by adding new sectors based on their criticality for the economy and society, and by introducing a clear size cap – meaning that all medium and large companies in selected sectors will be included in its scope. At the same time, it leaves some flexibility for Member States to identify smaller entities with a high security risk profile.

The proposal also eliminates the distinction between operators of essential services and digital service providers.

The proposal strengthens and streamlines security and reporting requirements for the companies.

Furthermore, the Commission is proposing to address security of 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 – the European Union Agency for Cybersecurity - may carry out coordinated risk assessments of critical supply chains, building on the successful approach taken in the context of the Commission Recommendation on Cybersecurity of 5G networks.

The proposal introduces more stringent supervisory measures for national authorities, stricter enforcement requirements and aims at harmonising sanctions regimes across Member States.

The proposal also enhances the role of the Cooperation Group and increases information sharing and cooperation between Member State authorities.

Which sectors and types of entities will the Commission proposal cover?

The Commission's proposal covers the following sectors and subsectors:

- **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; waste water; 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.
- **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).

What are the next steps?

The proposal will be subject to negotiations between the co-legislators, notably the Council of the European Union and the European Parliament. Once the proposal is agreed and consequently adopted, Member States would then have to transpose the NIS 2 Directive within 18 months of its entry into force. The Commission has to periodically review the Directive and report for the first time 54 months after its entry into force.

3. Report on the impact of the Commission Recommendation on 5G Cybersecurity

What are the main findings of the review of the Commission Recommendation?

The review shows that Member States have been highly appreciative of the process initiated by the Commission Recommendation of March 2019 on the Cybersecurity of 5G networks and are keen to continue the coordinated work on this topic at EU level. The Toolbox of mitigating measures is perceived as a **useful instrument** providing comprehensive guidance, based on risks and an objective methodology.

The review also shows that most Member States have made **further progress** in implementing the Toolbox measures at national level since the progress report was published in July 2020. While national processes are still underway, most Member States are well on track to complete them in the coming months. However, there are some differences between individual measures.

Where do Member States stand in implementing the Toolbox measures?

Since the Progress report was published in July 2020, most Member States have made further progress in implementing the various measures of the Toolbox at national level. Overall, nearly all

Member States estimated that they would complete the ongoing implementation process by **mid-2021**. However, a number of areas require specific attention and there are still a few Member States where no clear plans have yet been communicated as regards certain measures.

Specifically:

- **Regulatory powers of national authorities** have been strengthened in a large majority of Member States.
- Most Member States have put in place concrete activities to **strengthen requirements for** Mobile Network Operators.
- In nearly all Member States, with few exceptions, measures aimed at applying **restrictions based on the risk profile of suppliers** have been adopted, proposed or planned. The reliance on high-risk suppliers is therefore expected to decrease in the coming year(s).
- Several Member States have introduced measures on **diversification**.
- Fifteen Member States have now **national Foreign Direct Investment (FDI) screening mechanisms** in place.

What are the next steps in the EU coordination process on 5G cybersecurity?

The Commission calls on Member States to complete the implementation of the main Toolbox measures by the second quarter of 2021 and to ensure that identified risks have been mitigated adequately and in a coordinated way, in particular with a view to minimise the exposure to high-risk suppliers and of avoiding dependency on these suppliers.

Concrete actions are:

- **Continue and intensify the exchange of information and best practices** on specific strategic and technical measures, and on updated national risk assessments within the NIS Work Stream;
- **Monitor the evolutions** in 5G technology;
- Make use of the **EU funding opportunities**;
- Define and implement a concrete action plan to **enhance EU representation in standard setting bodies**;
- Prepare a **candidate certification scheme for key 5G components and suppliers' processes**;
- Work on **supply chain resilience**;
- Invest in **research and innovation capacities**.

4. Proposal for a Directive on the resilience of critical entities

What is new in today's proposal?

Infrastructures, networks and operators delivering essential services are increasingly connected, meaning that deficiencies in one business in one sector can cause disruptions in many other economic sectors across the internal market.

The proposal for a Directive on the resilience of critical entities 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, waste water, digital infrastructure, public administration and space, while existing EU rules only applied to the energy and transport sectors.

The proposal also introduces new rules to strengthen the resilience of critical entities:

- Member States would each adopt a **national strategy** for ensuring the resilience of critical entities and carry out regular risk assessments.
- 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.
- A Critical Entities Resilience Group, gathering Member States and the Commission, will **evaluate national strategies** and facilitate **cooperation and exchange of best practices**.
- An **enforcement mechanism** would help ensure that the rules are followed: 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.

- 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.

What kind of risks does the proposal aim to address?

The proposal is 'all-hazards' in nature, 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 like the one that Europe faces today. This is different from the European Critical Infrastructure Directive, which was primarily focused on terrorism.

What kind of obligations would it place on Member States?

Member States would need to adopt a strategy for ensuring the resilience of critical entities, carry out an all-hazards risk assessment, designate competent authority/authorities and a national point of contact. On the basis of the risk assessment, each Member State would have to identify critical entities in different sectors. There are also provisions for better European cooperation.

What kind of obligations would it place on entities?

In addition to the national risk assessment conducted by national authorities, critical entities would be required to carry out a risk assessment of their own. This entity-level assessment would need to account for both the outcomes of the national-level risk assessment and local conditions and specificities. On this basis, they would need to take technical and organisation measures to enhance their resilience. They would also need to provide information regarding incidents and potential incidents to competent authorities.

More Information

Press release: New EU Cybersecurity Strategy and new rules to make physical and digital critical entities more resilient

Factsheet on the new EU Cybersecurity Strategy

Factsheet on the Proposal for a Directive on measures for high common level of cybersecurity across the Union (revised NIS Directive)

Factsheet on Cybersecurity: EU External Action

Proposal for a Directive on measures for high common level of cybersecurity across the Union (revised NIS Directive or 'NIS 2')

Proposal for a Directive on the resilience of critical entities (see also Annex 1 to the proposal, as well as the impact assessment and its summary)

European Security Union

Impact assessment on the revised NIS Directive ('NIS 2')

More on Cybersecurity

More on the NIS Directive

QANDA/20/2392

Press contacts:

Johannes BAHRKE (+32 2 295 86 15)
Adalbert JAHNZ (+ 32 2 295 31 56)
Nabila MASSRALI (+32 2 298 80 93)
Marietta GRAMMENOU (+32 2 298 35 83)
Laura BERARD (+32 2 295 57 21)
Xavier CIFRE QUATRESOLS (+32 2 297 35 82)

General public inquiries: Europe Direct by phone 00 800 67 89 10 11 or by email