European Commission - Press release

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

Brussels, 16 December 2020

Today, the Commission and the High Representative of the Union for Foreign Affairs and Security Policy are presenting a new EU Cybersecurity Strategy. As a key component of Shaping Europe's Digital Future, the Recovery Plan for Europe and the EU Security Union Strategy, the Strategy will bolster Europe's collective resilience against cyber threats and help to ensure that all citizens and businesses can fully benefit from trustworthy and reliable services and digital tools. Whether it is the connected devices, the electricity grid, or the banks, planes, public administrations and hospitals Europeans use or frequent, they deserve to do so with the assurance that they will be shielded from cyber threats.

The new Cybersecurity Strategy also allows the EU to step up leadership on international norms and standards in cyberspace, and to strengthen cooperation with partners around the world to promote a global, open, stable and secure cyberspace, grounded in the rule of law, human rights, fundamental freedoms and democratic values.

Furthermore, the Commission is making proposals to address both cyber and physical resilience of critical entities and networks: a Directive on measures for high common level of cybersecurity across the Union (revised NIS Directive or 'NIS 2'), and a new Directive on the resilience of critical entities. They cover a wide range of sectors and aim to address current and future online and offline risks, from cyberattacks to crime or natural disasters, in a coherent and complementary way.

Trust and security at the heart of the EU Digital Decade

The new Cybersecurity Strategy aims to safeguard a global and open Internet, while at the same time offering safeguards, not only to ensure security but also to protect European values and the fundamental rights of everyone. Building upon the achievements of the past months and years, it contains concrete proposals for regulatory, investment and policy initiatives, in three areas of EU action:

1. **Resilience, technological sovereignty and leadership**

Under this strand of action the Commission proposes to reform the rules on the security of network and information systems, under a Directive on measures for high common level of cybersecurity across the Union (revised NIS Directive or 'NIS 2'), in order to increase the level of cyber resilience of critical public and private sectors: hospitals, energy grids, railways, but also data centres, public administrations, research labs and manufacturing of critical medical devices and medicines, as well as other critical infrastructure and services, must remain impermeable, in an increasingly fast-moving and complex threat environment.

The Commission also proposes to launch a network of Security Operations Centres across the EU, powered by artificial intelligence (AI), which will constitute a real 'cybersecurity shield' for the EU, able to detect signs of a cyberattack early enough and to enable proactive action, before damage occurs. Additional measures will include dedicated support to small and medium-sized businesses (SMEs), under the Digital Innovation Hubs, as well as increased efforts to upskill the workforce, attract and retain the best cybersecurity talent and invest in research and innovation that is open, competitive and based on excellence.

2. **Building operational capacity to prevent, deter and respond**

The Commission is preparing, through a progressive and inclusive process with the Member States, a new Joint Cyber Unit, to strengthen cooperation between EU bodies and Member State authorities responsible for preventing, deterring and responding to cyber-attacks, including civilian, law enforcement, diplomatic and cyber defence communities. The High Representative puts forward proposals to strengthen the EU Cyber Diplomacy Toolbox to prevent, discourage, deter and respond effectively against malicious cyber activities, notably those affecting our critical infrastructure, supply

chains, democratic institutions and processes. The EU will also aim to further enhance cyber defence cooperation and develop state-of-the-art cyber defence capabilities, building on the work of the European Defence Agency and encouraging Member States to make full use of the Permanent Structured Cooperation and the European Defence Fund.

3. **Advancing a global and open cyberspace through increased cooperation**

The EU will step up work with international partners 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. The EU will further strengthen its EU Cyber Diplomacy Toolbox, and increase cyber capacity-building efforts to third 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. The EU will also form an EU Cyber Diplomacy Network around the world to promote its vision of cyberspace.

The EU is committed to supporting the new Cybersecurity Strategy with an unprecedented level of investment in the EU's digital transition over the next seven years, through the next long-term EU budget, notably the Digital Europe Programme and Horizon Europe, as well as the Recovery Plan for Europe. Member States are thus encouraged to make full use of the EU Recovery and Resilience Facility to boost cybersecurity and match EU-level investment. The objective is to reach up to €4.5 billion of combined investment from the EU, the Member States and the industry, notably under the Cybersecurity Competence Centre and Network of Coordination Centres, and to ensure that a major portion gets to SMEs.

The Commission also aims at reinforcing the EU's industrial and technological capacities in cybersecurity, including through projects supported jointly by EU and national budgets. The EU has the unique opportunity to pool its assets to enhance its strategic autonomy and propel its leadership in cybersecurity across the digital supply chain (including data and cloud, next generation processor technologies, ultra-secure connectivity and 6G networks), in line with its values and priorities.

Cyber and physical resilience of network, information systems and critical entities

Existing EU-level measures aimed at protecting key services and infrastructures from both cyber and physical risks need to be updated. Cybersecurity risks continue to evolve with growing digitalisation and interconnectedness. Physical risks have also become more complex since the adoption of the 2008 EU rules on critical infrastructure, which currently only cover the energy and transport sectors. The revisions aim at updating the rules following the logic of the EU's Security Union strategy, overcoming the false dichotomy between online and offline and breaking down the silo approach.

To respond to the growing threats due to digitalisation and interconnectedness, the proposed **Directive on measures for high common level of cybersecurity across the Union (revised NIS Directive or 'NIS 2')** will cover medium and large entities from more sectors based on their criticality for the economy and society. NIS 2 strengthens security requirements imposed on the companies, addresses security of supply chains and supplier relationships, streamlines reporting obligations, introduces more stringent supervisory measures for national authorities, stricter enforcement requirements and aims at harmonising sanctions regimes across Member States. The NIS 2 proposal will help increase information sharing and cooperation on cyber crisis management at national and EU level.

The proposed **Critical Entities Resilience (CER) Directive** expands both the scope and depth of the 2008 European Critical Infrastructure directive. Ten sectors are now covered: energy, transport, banking, financial market infrastructures, health, drinking water, waste water, digital infrastructure, public administration and space. Under the proposed directive, Member States would each adopt a national strategy for ensuring the resilience of critical entities and carry out regular risk assessments. These assessments would also help identify a smaller subset of critical entities that would be subject to obligations intended to enhance their resilience in the face of non-cyber risks, including entity-level risk assessments, taking technical and organisational measures, and incident notification. The Commission, in turn, 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.

Securing the next generation of networks: 5G and beyond

Under the new Cybersecurity Strategy, Member States, with the support of the Commission and

ENISA - the European Cybersecurity Agency, are encouraged to complete the implementation of the EU 5G Toolbox, a comprehensive and objective risk-based approach for the security of 5G and future generations of networks.

According to a report published today, on the impact of the Commission Recommendation on the Cybersecurity of 5G networks and the progress in implementing the EU toolbox of mitigating measures, since the progress report of July 2020, most Member States are already well on track of implementing the recommended measures. They should now aim to complete their implementation by the second quarter of 2021 and ensure that identified risks are adequately mitigated, in a coordinated way, particularly with a view to minimising the exposure to high-risk suppliers and avoiding dependency on these suppliers. The Commission also sets out today key objectives and actions aimed at continuing the coordinated work at EU-level.

Members of the College said:

Margrethe **Vestager**, Executive Vice-President for a Europe Fit for the Digital Age, said: *"Europe is committed to the digital transformation of our society and economy. So we need to support it with unprecedented levels of investment. The digital transformation is accelerating, but can only succeed if people and businesses can trust that the connected products and services - on which they rely – are secure."*

Josep **Borrell**, High Representative, said: *"International security and stability depends more than ever on a global, open, stable and secure cyberspace where the rule of law, human rights, freedoms and democracy are respected. With today's strategy the EU is stepping up to protect its governments, citizens and businesses from global cyber threats, and to provide leadership in cyberspace, making sure everybody can reap the benefits of the Internet and the use of technologies."*

Margaritis **Schinas**, Vice-President for Promoting our European Way of Life, said: *"Cybersecurity is a central part of the Security Union. There is no longer a distinction between online and offline threats. Digital and physical are now inextricably intertwined. Today's set of measures show that the EU is ready to use all of its resources and expertise to prepare for and respond to physical and cyber threats with the same level of determination."*

Thierry **Breton**, Commissioner for the Internal Market said: *"Cyber threats evolve fast, they are increasingly complex and adaptable. To make sure our citizens and infrastructures are protected, we need to think several steps ahead, Europe's resilient and autonomous Cybersecurity Shield will mean we can utilise our expertise and knowledge to detect and react faster, limit potential damages and increase our resilience. Investing in cybersecurity means investing in the healthy future of our online environments and in our strategic autonomy."*

Ylva **Johansson**, Commissioner for Home Affairs, said: *"Our hospitals, waste water systems or transport infrastructure are only as strong as their weakest links; disruptions in one part of the Union risk affecting the provision of essential services elsewhere. To ensure the smooth functioning of the internal market and the livelihoods of those living in Europe, our key infrastructure must be resilient against risks such as natural disasters, terrorist attacks, accidents and pandemics like the one we are experiencing today. My proposal on critical infrastructure does just that."*

Next Steps

The European Commission and the High Representative are committed to implementing the new Cybersecurity Strategy in the coming months. They will regularly report on the progress made and keep the European Parliament, the Council of the European Union, and stakeholders fully informed and engaged in all relevant actions.

It is now for the European Parliament and the Council to examine and adopt the proposed NIS 2 Directive and the Critical Entities Resilience Directive. Once the proposals are agreed and consequently adopted, Member States would then have to transpose them within 18 months of their entry into force.

The Commission will periodically review the NIS 2 Directive and the Critical Entities Resilience Directive and report on their functioning.

Background

Cybersecurity is one of the Commission's top priorities and a cornerstone of the digital and connected Europe. An increase of cyber-attacks during the coronavirus crisis have shown how important it is to protect hospitals, research centres and other infrastructure. Strong action in the area is needed to future-proof the EU's economy and society.

The new Cybersecurity Strategy proposes to integrate cybersecurity into every element of the supply chain and bring further together EU's activities and resources across the four communities of cybersecurity – internal market, law enforcement, diplomacy and defence. It builds on the EU' Shaping Europe's Digital Future and the EU Security Union Strategy, and leans on a number of legislative acts, actions and initiatives the EU has implemented to strengthen cybersecurity capacities and ensure a more cyber-resilient Europe. This includes the Cybersecurity strategy of 2013, reviewed in 2017, and the Commission's European Agenda on Security 2015-2020. It also recognises the increasing inter-connection between internal and external security, in particular through the Common Foreign and Security Policy.

The first EU-wide law on cybersecurity, the NIS Directive, that came into force in 2016 helped to achieve a common high level of security of network and information systems across the EU. As part of its key policy objective to make Europe fit for the digital age, the Commission announced the revision of the NIS Directive in February this year. The EU Cybersecurity Act that is in force since 2019 equipped Europe with a framework of cybersecurity certification of products, services and processes and reinforced the mandate of the EU Agency for Cybersecurity (ENISA).

As regards Cybersecurity of 5G networks, Member States, with the support of the Commission and ENISA have established, with the EU 5G Toolbox adopted in January 2020, a comprehensive and objective risk-based approach. The Commission review of its Recommendation of March 2019 on the cybersecurity of 5G networks found that most Member States have made progress in implementing the Toolbox.

Starting from the 2013 EU Cybersecurity strategy, the EU has developed a coherent and holistic international cyber policy. Working with its partners at bilateral, regional and international level, the EU has promoted a global, open, stable and secure cyberspace guided by EU's core values and grounded in the rule of law. The EU has supported third countries in increasing their cyber resilience and ability to tackle cybercrime, and has used its 2017 EU cyber diplomacy toolbox to further contribute to international security and stability in cyberspace, including by applying for the first time its 2019 cyber sanctions regime and listing 8 individuals and 4 entities and bodies. The EU has made significant progress also on cyber defence cooperation, including as regards cyber defence capabilities, notably in the framework of its Cyber Defence Policy Framework (CDPF), as well as in the context of the Permanent Structured Cooperation (PESCO) and the work of the European Defence Agency.

Cybersecurity is a priority also reflected in the EU's next long-term budget (2021-2027). Under the Digital Europe Programme the EU will support cybersecurity research, innovation and infrastructure, cyber defence, and the EU's cybersecurity industry. In addition, in its response to the Coronavirus crisis, which saw increased cyberattacks during the lockdown, additional investments in cybersecurity are ensured under the Recovery Plan for Europe.

The EU has long recognised the need to ensure the resilience of critical infrastructures providing services which are essential for the smooth running of the internal market and the lives and livelihoods of European citizens. For this reason, the EU established the European Programme for Critical Infrastructure Protection (EPCIP) in 2006 and adopted the European Critical Infrastructure (ECI) Directive in 2008, which applies to the energy and transport sectors. These measures were complemented in later years by various sectoral and cross-sectoral measures on specific aspects such as climate proofing, civil protection, or foreign direct investment.

More Information

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

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

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

IP/20/2391

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

Related media

Illustration 2020/2