A cybersecure digital transformation in a complex threat environment - brochure

This brochure gives you a quick overview of the new EU Cybersecurity Strategy.

European Commission

Building Strong Cybersecurity

> "*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.*"

Thierry Breton, Commissioner for the Internal Market

- Connected devices are forecast to rise to **25 billion by 2025**. A quarter of these will be in

Europe.
- Changes in working patterns has been accelerated by the COVID-19 pandemic – **40%** of EU workers switched to telework in early 2020.
- **Two in five** EU users have experienced security-related problems.
- **One in eight** businesses have been affected by cyberattacks.
- The annual cost of cybercrime to the global economy is estimated to have reached **€5.5 trillion** at the end of 2020, double the figure of 2015.
- EU funding in the 2021-2027 Multiannual Financial Framework could amount to **€2 billion** overall plus Member States and industry investment.
- EU investments in digital projects should amount to at least 20% — equivalent to **€134.5 billion** - of the **€672.5 billion** Recovery and Resilience Facility.

The EU's Cybersecurity Strategy for the Digital Decade

In December 2020, the European Commission and the High Representative of the Union for Foreign Affairs and Security Policy presented a new EU Cybersecurity Strategy. The 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.

The new strategy aims to ensure a global and open Internet with strong guardrails to address the risks to the security and fundamental rights and freedoms of people in Europe. Following the progress achieved under the previous strategies, it contains concrete proposals for deploying three principal instruments – regulatory, investment and policy instruments – to address three areas of EU action:

1. resilience, technological sovereignty and leadership,
2. building operational capacity to prevent, deter and respond,
3. advancing a global and open cyberspace.

How?

1. By boosting the security of essential services and connected things.

Revised rules on the security of network and information systems

Development of a European Cyber Shield through a network of AI-enabled Security Operations Centres that can detect signs of cyberattack and enable preventive action before damage occurs

High standards of cybersecurity for all connected objects

Dedicated support to SMEs

Attracting and retaining the best cybersecurity talent

Investing in research and innovation

Securing 5G networks and supply chains

2. By strengthening collective capabilities to respond to major cyberattacks

- Support to Member States to defend their citizens and national security interests.
- Working together on preventing, discouraging, deterring and responding to cyber threats with:

Civilian and disaster responses

Police and judiciary

Cyber diplomacy

The Joint Cyber Unit is a platform that will help to better protect the EU from the most impactful cybersecurity attacks, especially cross-border ones.

3. By working with partners around the world to ensure international security and stability in cyberspace

Stepping up the work with international partners to advance and promote a global, open, stable and secure cyberspace where international law, human rights, fundamental freedoms and democratic values are respected.

What?

Regulatory, Investment and Policy instruments to implement EU actions

Regulatory

- EU Cybersecurity Act Regulation
- General Data Protection Regulation (GDPR)
- Electronic Identification Regulation (eIDAS)

Policy

- Security of Network & Information Systems Directive (NIS2)
- 5G Security
- EU cyber-crisis blueprint
- a Joint Cyber Unit
- Cyber diplomacy
- 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

Investment

- increase in the EU investment in cybersecurity research, innovation and deployment
- Cybersecurity public-private partnership competence center
- Digital Europe Programme
- Horizon Europe/EU research programme
- Connecting Europe Facility
- Recovery and Resilience Facility

Europe’s strength lies in its diversity, skills and commitment to strong cybersecurity

Our assets:

- cybersecurity as a top EU priority
- high-level cybersecurity expertise
- strong cybersecurity industry with our innovative SMEs
- a growing Digital Single Market
- EU solidarity

NIS Directive and NIS2 Proposal

The Directive on security of network and information systems (NIS) and the Proposal for directive on measures for high common level of cybersecurity across the Union (NIS2)

The NIS Directive is the cornerstone of the EU's cybersecurity architecture. It provides legal measures to boost the overall level of cybersecurity and preparedness in the EU:

- preparedness of Member States by requiring them to be appropriately equipped, e.g. via a Computer Security Incident Response Team (CSIRT) and a competent national NIS authority,
- cooperation among all the Member States, by setting up a Cooperation Group, in order to support and facilitate strategic cooperation and the exchange of information among Member States. They will also need to set a CSIRT Network, in order to promote swift and effective operational cooperation on specific cybersecurity incidents and sharing information about risks,
- a culture of security across sectors which are vital for our economy and society and moreover rely heavily on ICTs, such as energy, transport, water, banking, financial market infrastructures, healthcare and digital infrastructure. Businesses in these sectors that are identified by the Member States as operators of essential services will have to take appropriate security measures and to notify serious incidents to the relevant national authority. Also key digital service providers (search engines, cloud computing services and online marketplaces) will have to comply with the security and notification requirements under the new Directive.

Article 23 of the Directive requires the European Commission to review the functioning of this Directive periodically. Review of the Directive was accomplished and the **Proposal for directive on measures for high common level of cybersecurity across the Union (NIS2)** was presented on 15 December 2020. The new Commission proposal aims to address the deficiencies of the previous NIS Directive, to adapt it to the current needs and make it future-proof. Key elements of NIS2:

- 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
- Eliminates the distinction between operators of essential services and digital service providers
- Strengthens and streamlines security and reporting requirements for the companies
- Addresses security of supply chains and supplier relationships
- Introduces more stringent supervisory measures for national authorities, stricter enforcement requirements and aims at harmonising sanctions regimes across Member States
- Enhances the role of the Cooperation Group and increases information sharing and cooperation between Member State authorities.

In order to ensure a consistent approach as announced under the Security Union Strategy 2020-2025, the reformed Directive is proposed together with other initiatives in the field:

- **Review of the legislation on the resilience of critical infrastructure**
- **'Network code'** setting rules for **cybersecurity in cross-border electricity flows** for adoption by end 2022
- Strengthening **digital operational resilience in financial sector** and ensure an ability to withstand all types of ICT-related disruptions and threats
- Provisions on cybersecurity to the EU legislation on **aviation security** and continuation of efforts to enhance cyber resilience across all transport modes
- Strengthening the cyber resilience of democratic processes and institutions as a core component of the **European Democracy Action Plan** for safeguarding and promoting free elections, and democratic discourse and media plurality
- **Security of infrastructure and services under the future Space Programme**, deepening

of **the Galileo cybersecurity strategy** for the next generation of Global Navigation Satellite System services, and other new components of the Space Programme.

A network of Security Operation Centres (SOCs)

The Cybersecurity Strategy 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. The goal is to improve incident detection, analysis and response speeds, notably through state-of-the-art AI and machine learning capabilities, complemented by supercomputing infrastructure. This will allow for more timely warnings on cybersecurity incidents to authorities and all interested stakeholders, so that potential threats are tackled before they can cause large-scale damage.

Investment in cybersecurity research, innovation & deployment

The European Union has been investing in cybersecurity and privacy research and innovation since the early ’90s, with also **European Commission and cybersecurity industry public-private partnership.**

Since 2014 to date, 2,059 participants have been involved in 132 EU cybersecurity R&I projects across Europe, with a total EU funding of more than €600 million (from the Horizon 2020 programme). The following areas were represented: Identity, Privacy & Trust; Protection of critical sectors/infrastructures; Risk preparedness and response; Technological building blocks for cybersecurity and Competence, governance, community.

The large number of organisations participating in EU funded cybersecurity and privacy related projects positively impacts the European Union as it:

- advances research and innovation
- supports a cross-border and transgovernmental collaboration
- promotes the sharing of knowledge
- provides input to shape the future EU policies

A Joint Cyber Unit

A Joint Cyber Unit would serve as a virtual and physical platform for cooperation for the different cybersecurity communities in the EU, with a focus on operational and technical coordination against major cross border cyber incidents and threats.

It main objectives are:

1. ensure preparedness across cybersecurity communities;
2. provide continuous shared situational awareness through information sharing;
3. reinforce coordinated response and recovery.

The EU’s Cybersecurity Act sets:

- A permanent mandate and stronger role for the European Union Agency for Cybersecurity (ENISA)
- A framework for European Cybersecurity Certification for digital products, processes and services that will be valid throughout the European Union.

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.

Cyber Diplomacy

The European Union and its Member States strongly promote global, open, stable and secure cyberspace where human rights and fundamental freedoms and the rule of law fully apply for the social well-being, economic growth, prosperity and integrity of free and democratic societies.

To this end the EU and its Member States:

- reaffirm the importance of the application of international law, adherence to norms of responsible state behaviour and the use of confidence building measures.
- stress the importance of cooperation, outreach and capacity building to promote responsible state behaviour and advance global cyber resilience.
- commit to prevent conflicts, and advance cyber stability, notably through the use of law-enforcement, legal and economic and diplomatic instruments, including if necessary sanctions.

The Cybersecurity strategy announces several proposals to strengthen the EU cyber diplomacy response, notably:

- a Member States' cyber intelligence working group.
- a proposal for the EU to further define its **cyber deterrence posture**.
- a review the Cyber Defence Policy Framework.

Awareness and skills

The human factor is often the weak link in cybersecurity; someone clicking on a phishing link can have huge consequences. Therefore, the Commission raises awareness of cybersecurity and promotes best practices among the general public. For instance, once a year it organises the European Cyber Security Month together with ENISA.

We need to ensure that we have experts with the right knowledge and skills, and there are currently not enough. That is why the Commission does many things to stimulate the development of cybersecurity skills. An attention is also given to the role of women, who are underrepresented. That is why the Commission has set up the Women4Cyber Registry, in cooperation with the European Cybersecurity Organization (ECSO)'s Women4Cyber initiative.

Related topics

Cybersecurity
Strengthening trust and security
