The Cybersecurity Strategy

The EU Cybersecurity Strategy aims to build resilience to cyber threats and ensure citizens and businesses benefit from trustworthy digital technologies.

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

The digital transformation of society, intensified by the COVID-19 crisis, has expanded the threat landscape and is bringing about new challenges, which require adapted and innovative responses. The number of cyber-attacks continues to rise, with increasingly sophisticated attacks coming from a wide range of sources both inside and outside the EU.

The EU should therefore be leading the efforts for a secure digitalisation. It should be driving norms for world-class solutions and standards of cybersecurity for essential services and critical infrastructures, as well as driving the development and application of new technologies. Governments, businesses and citizens will all share a responsibility in ensuring a cyber-secure digital transformation.

What is the strategy about?

The strategy describes how the EU can harness and strengthen all its tools and resources to be technologically sovereign. It also lays out how the EU can step up its cooperation with partners around the world who share our values of democracy, rule of law and human rights.

The EU's technological sovereignty needs to be founded on the resilience of all connected services and products. All the four cybercommunities – those concerned with the internal market, with law

enforcement, diplomacy and defence – need to work more closely towards a shared awareness of threats. They should be ready to respond collectively when an attack materialises, so that the EU can be greater than the sum of its parts.

The strategy covers the security of essential services such as hospitals, energy grids, railways and the ever-increasing number of connected objects in our homes, offices and factories. The strategy aims to build collective capabilities to respond to major cyberattacks. It also outlines plans to work with partners around the world to ensure international security and stability in cyberspace. Moreover, it outlines how a Joint Cyber Unit can ensure the most effective response to cyber threats using the collective resources and expertise available to Member States and the EU.

Main aim of the strategy

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

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

The EU is committed to supporting this strategy through an unprecedented level of investment in the EU's digital transition over the next seven years. This would quadruple previous levels of investment. It demonstrates the EU’s commitment to its new technological and industrial policy and the recovery agenda.

The EU’s new Cybersecurity Strategy for the Digital Decade forms a key component of Shaping Europe’s Digital Future, the Commission’s Recovery Plan for Europe and of the Security Union Strategy 2020-2025.

Press Release: Cybersecurity Strategy

Q&A: Cybersecurity Strategy

Joint Communication: Cybersecurity Strategy

Directive on the resilience of critical entities

Follow the latest progress and learn more about getting involved.

Follow the Commission's work on cybersecurity @CyberSec_EU

Latest

The European Cybersecurity Competence Centre and Network moves forward: future Governing Board meets for the first time

The European Commission has organised an informal virtual meeting of the future Governing Board of the European Cybersecurity Competence Centre, gathering representatives from Member States, the Commission and the European Union

Agency for Cybersecurity, ENISA. The meeting focused on the preparations for the establishment of the Centre and discussed the next steps, including practical aspects and the rules of procedure.

Cybersecurity of 5G networks: Commission requests the EU cybersecurity agency to develop a certification scheme

The Commission has tasked the European Union Agency for Cybersecurity, ENISA, to prepare the EU's cybersecurity certification scheme for 5G networks that will help address risks related to technical vulnerabilities of the networks and further enhance their cybersecurity. Certification plays a critical role in increasing trust and security in digital products and services – however, at the moment, there are various security certification schemes for IT products, including 5G networks, in Europe.

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

The Commission and the High Representative of the Union for Foreign Affairs and Security Policy have presented this week 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.

Commission welcomes political agreement on the Cybersecurity Competence Centre and Network

Today, the EU institutions have reached a political agreement, subject to formal approval by the European Parliament and the Council of the EU, on the Cybersecurity Competence Centre and Network, an initiative that aims to improve and strengthen technology and industrial cybersecurity capacities of the EU and help create a safe online environment.

Browse Cybersecurity

Related Content

Big Picture

Cybersecurity Policies

The European Union works on various fronts to promote cyber resilience, safeguarding our communication and data and keeping online society and economy secure.

See Also

22 Cybersecurity projects selected to receive €10.9 million

Operators of Essential Services (OES), National Cybersecurity Certification Authorities (NCCAs) and National Competent Authorities (NCAs) for cybersecurity are among the selected applicants that will receive €11 million in funding by the Connecting Europe Facility cybersecurity...

European Cybersecurity Competence Network and Centre

The mission of the European Cybersecurity Network and a Competence Centre is to help the EU retain and develop the cybersecurity technological and industrial capacities necessary. This goes hand-in-hand with the key objective to increase the competitiveness of the EU's...

Stakeholder Cybersecurity Certification Group

The Stakeholder Cybersecurity Certification Group was established to provide advice on strategic issues regarding cybersecurity certification.

The EU Cybersecurity Act

The Cybersecurity Act strengthens the EU Agency for cybersecurity (ENISA) and establishes a cybersecurity certification framework for products and services.

The EU cybersecurity certification framework

The EU cybersecurity certification framework for ICT products enables the creation of tailored and risk-based EU certification schemes.

NIS Cooperation Group

The Network and Information Systems Cooperation Group was established by the NIS Directive to ensure cooperation and information exchange among Member States.

NIS Directive

The NIS Directive is the first piece of EU-wide legislation on cybersecurity. It provides legal measures to boost the overall level of cybersecurity in the EU.
