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.

© Image by Traitov - iStock Getty Images

Page Contents
Cybersecurity Strategy


The Strategy covers the security of essential services such as hospitals, energy grids and railways. It also covers the security of the ever-increasing number of connected objects in our homes, offices and
factories.

The Strategy focuses on building collective capabilities to respond to major cyberattacks and working with partners around the world to ensure international security and stability in cyberspace. It outlines how a Joint Cyber Unit can ensure the most effective response to cyber threats using the collective resources and expertise available to the EU and Member States.

**Legislation and certification**

**Directive on measures for a high common level of cybersecurity across the Union (NIS2 Directive)**

Cybersecurity threats are almost always cross-border, and a cyberattack on the critical facilities of one country can affect the EU as a whole. EU countries need to have strong government bodies that supervise cybersecurity in their country and that work together with their counterparts in other Member States by sharing information. This is particularly important for sectors that are critical for our societies.

The Directive on security of network and information systems (NIS Directive) (https://digital-strategy.ec.europa.eu/en/policies/nis-directive), which all countries have now implemented, ensures the creation and cooperation of such government bodies. This Directive was reviewed at the end of 2020.

As a result of the review process, the proposal for a Directive on measures for a high common level of cybersecurity across the Union (NIS2 Directive (https://digital-strategy.ec.europa.eu/en/library/proposal-directive-measures-high-common-level-cybersecurity-across-union)) was presented by the Commission on 16 December 2020.

The Directive (https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32022L2555) was published in the Official Journal of the European Union in December 2022 and entered into force on 16 January 2023. Member states will have 21 months from the entry into force of the directive in which to incorporate the provisions into their national law (actual date: 18 October 2024).

**ENISA - the EU cybersecurity agency**

ENISA (European Union Agency for Cybersecurity (https://www.enisa.europa.eu/)) is the EU agency that deals with cybersecurity. It provide support to Member States, EU institutions and businesses in key areas, including the implementation of the NIS Directive.

**The Cyber Resilience Act**


**Cybersecurity Act**

The Cybersecurity Act (https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act) strengthens the role of ENISA. The agency now has a permanent mandate, and is empowered to contribute to stepping up both operational cooperation and crisis management across the EU. It also has more financial and human resources than before. On 18 April 2023, the Commission proposed a targeted amendment to the EU Cybersecurity Act
Cyber Solidarity Act

On the 18 April 2023, the European Commission proposed the EU Cyber Solidarity Act, to improve the response to cyber threats across the EU. The proposal will include a European Cybersecurity Shield and a comprehensive Cyber Emergency Mechanism to create a better cyber defence method.

Certification

Our digital lives can only work well if there is general public trust in the cybersecurity of IT products and services. It is important that we can see that a product has been checked and certified to conform to high cybersecurity standards. There are currently various security certification schemes for IT products around the EU. Having a single common scheme for certification would be easier and clearer for everyone.

The Commission is therefore working on an EU-wide certification framework, with ENISA at its heart. The Cybersecurity Act outlines the process for achieving this framework.

Investment

Recovery Plan

Cybersecurity is one of the Commission’s priorities in its response to the coronavirus crisis, as there were increased cyberattacks during the lockdown. The Recovery Plan for Europe includes additional investments in cybersecurity.

Support for research and innovation: Horizon 2020 and cPPP; Horizon Europe

Research into digital security is essential to building innovative solutions that can protect us against the latest, most advanced cyber threats. That is why cybersecurity is an important part Horizon 2020 and its successor Horizon Europe.

In Horizon Europe, for the period 2021-2027, cybersecurity is part of the ‘Civil Security for Society’ cluster.

As part of Horizon 2020, the Commission co-funded research and innovation into topics such as cybersecurity preparedness through cyber ranges and simulation, cybersecurity for small and medium-sized enterprises, cybersecurity in the electrical power and energy system, and cybersecurity and data protection in critical sectors. These topics fall under the cluster ‘Secure societies — Protecting the freedom and security of Europe and its citizens.’

In 2016, the Horizon 2020 contractual public-private partnership (cPPP) on cybersecurity was established between the European Commission and the European Cyber Security Organisation.
Support for cyber capacities and deployment

Our physical and digital infrastructures are very closely intertwined. Therefore, the Commission has also invested in cybersecurity as part of its infrastructure investment funding programme, the Connecting Europe Facility (CEF), for the period 2014-2020.

CEF support has gone to computer security incident response teams, operators of essential services (OES), digital service providers (DSPs), single points of contact (SPOC) and national competent authorities (NCAs). This enhances the cybersecurity capabilities and the cross-border collaboration within the EU, supporting the implementation of the EU Cybersecurity strategy.

The Digital Europe Programme, for the period 2021-2027, is an ambitious programme that plans to invest €1.9 billion into cybersecurity capacity and the wide deployment of cybersecurity infrastructures and tools across the EU for public administrations, businesses and individuals.

Cybersecurity is also a part of InvestEU. InvestEU is a general programme that brings together many financial instruments and uses public investment to secure further investment from the private sector. Its strategic investment facility will support key value chains in cybersecurity. It is an important part of the recovery package in response to the coronavirus crisis.

Cybersecurity Competence Centre and Network; Atlas

The European cybersecurity industrial, technology and research competence centre will pool expertise and align European development and deployment of cybersecurity technology. It will work with industry, the academic community and others to build a common agenda for investments into cybersecurity, and decide on funding priorities for research, development and roll-out of cybersecurity solutions through the Horizon Europe and Digital Europe Programmes.

Currently, four pilot projects are running to lay the groundwork for the Competence Centre and Network. They involve more than 170 partners.

For a better overview of cybersecurity expertise and capacity across the EU, the Commission has developed a comprehensive platform called the Cybersecurity Atlas.

Policy guidance

Blueprint for coordinated response to major cyber-attacks

The Commission's blueprint for rapid emergency response provides a plan in case of a large-scale cross-border
cyber incident or crisis. It sets out the objectives and modes of cooperation between the Member States and EU Institutions in responding to such incidents and crises. It explains how existing Crisis Management mechanisms can make full use of existing cybersecurity entities at EU level.

**Joint Cyber Unit**

As a follow-up, Commission President Ursula von der Leyen announced a proposal for an EU-wide Joint Cyber Unit. The Recommendation on the creation of the Joint Cyber Unit announced by the Commission on 23 June 2021 is an important step towards completing the European cybersecurity crisis management framework. It is a concrete deliverable of the [EU Cybersecurity Strategy](https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2391) and the [EU Security Union Strategy](https://ec.europa.eu/commission/presscorner/detail/en/ip_20_1379), contributing to a safe digital economy and society.

The Joint Cyber Unit ([https://digital-strategy.ec.europa.eu/en/policies/joint-cyber-unit](https://digital-strategy.ec.europa.eu/en/policies/joint-cyber-unit)) will act as a platform to ensure an **EU coordinated response** to large-scale cyber incidents and crises, as well as to offer **assistance** in recovering from these attacks.

**Secure 5G deployment in the EU**

5G networks are planned to be rolled out across the EU. They will offer huge benefits, but also have more potential entry points for attackers due to the less centralised nature of their architecture, greater number of antennas and increased dependency on software. The EU Toolbox on 5G ([https://digital-strategy.ec.europa.eu/en/library/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures](https://digital-strategy.ec.europa.eu/en/library/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures)) sets out measures to strengthen security requirements for 5G networks, apply relevant restrictions for suppliers considered high-risk, and ensure the diversification of vendors.

**Securing the electoral process**

Our European democracies have become increasingly digital: political campaigns take place online and elections themselves happen through electronic voting in many countries.


**Skills and awareness**

**Skills**

We can only ensure digital security if we have experts with the right knowledge and skills, and there are currently not enough. That is why the Commission is taking action to stimulate the development of cybersecurity skills.

The Commission prepared a call for coherent framework for teaching cybersecurity skills in university and professional education. The four pilot projects that prepare the cybersecurity competence centre and network by ECSO are currently working on this. There are also recurring initiatives meant directly for students, such as the yearly European cybersecurity challenge ([http://europeancybersecuritychallenge.eu/](http://europeancybersecuritychallenge.eu/)).
Cybersecurity skills fall under the Commission’s general agenda on digital skills (https://digital-strategy.ec.europa.eu/en/policies/digital-skills-and-jobs). They are also a part of the funding efforts under Horizon 2020, Horizon Europe and the Digital Europe Programme. One example is the funding for ‘cyber ranges’, which are live simulation environments of cyber threats for training.

**Awareness**

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 (http://www.enisa.europa.eu/topics/cybersecurity-education/european-cyber-security-month) together with ENISA.

**The EU Cybersecurity Skills Academy**

The EU Cybersecurity Skills Academy (https://digital-skills-jobs.europa.eu/en/cybersecurity-skills-academy), launched as part of the European Year of Skills, will pool together private and public initiatives at European and national levels to address the gap in the cybersecurity workforce. The initiative will be hosted online on the Commission's jobs and skills platform and will feature funding opportunities, training, and certifications from across the EU, for those interested in a career in cybersecurity.


**Cyber community**

**ENISA - the EU cybersecurity agency**

ENISA is the EU’s agency that deals with cybersecurity. It provide support to Member States, EU institutions and businesses in key areas, including the implementation of the NIS Directive.

**ISACs**

Information Sharing and Analysis Centres (ISACs) foster collaboration between the cybersecurity community in different sectors of the economy. Further developing ISACs at both EU and national level is a priority for the Commission. In collaboration with ENISA, the Commission also promotes the establishment of new ISACs in sectors that are not covered. The “empowering EU ISACs consortium”, supervised by the Commission, provides legal, technical and organisational support for ISACs.

**JRC**

The Joint Research Center (JRC) of the Commission is actively contributing to Cybersecurity in the EU. For example, the JRC has developed a Cybersecurity Taxonomy (https://publications.jrc.ec.europa.eu/repository/handle/JRC125533). This aligns the terminology used in cybersecurity so that we can have a clearer overview of cybersecurity capabilities in the EU.

The JRC also recently published a report that provides insights into the current EU cybersecurity

CSIRTs/CERTs

Under the NIS Directive, EU Member States are required to ensure that they have well-functioning Computer Security Incident Response Teams ('CSIRTs'), also known as Computer Emergency Response Teams ('CERTs'). These teams provide deal with cybersecurity incidents and risks in practice. They cooperate with each other at EU level, and also work together with the private sector. All types of operators of essential services and digital service providers have to be covered by designated CSIRTs.

The main tasks of CSIRTs are:

- monitoring incidents at a national level;
- providing early warning, alerts, announcements and other information about risks and incidents to relevant stakeholders;
- responding to incidents;
- providing dynamic risk and incident analysis and situational awareness;
- participating in the CSIRTs network.

ECSO

The European Cybersecurity Organisation (ECSO) was created in 2016 in order to act as the Commission’s counterpart in a contractual public-private partnership covering Horizon 2020 in the years 2016 to 2020. The majority of ECSO’s 250 members belong either to the cybersecurity industry or to research and academic institutions in the field. To a lesser degree, ECSO’s members also comprise public sector actors and demand-side industries.

Besides making recommendations on Horizon 2020, ECSO carries out various activities aiming at community building and industrial development at European level.

Women4Cyber

It is important to highlight the role of women in the cybersecurity community, who are underrepresented. That is why the Commission has set up the Women4Cyber Registry (http://ec.europa.eu/futurium/en/Women4Cyber), in cooperation with ECSO’s Women4Cyber initiative. It makes it easier for the media, event organisers and others to find the many talented women working in cybersecurity, so these women become more visible and prominent in the cyber community and the public debate.

Other cyber policy areas

Cybercrime

Cyber diplomacy

The EU is making efforts to protect itself against cyber threats from outside its borders. As a part of this, the Commission works together with the European External Action Service and Member States on the implementation of a joint diplomatic response to malicious cyber activities (http://data.consilium.europa.eu/doc/document/ST-13007-2017-INIT/en/pdf) (the ‘cyber diplomacy toolbox’). This response includes diplomatic cooperation and dialogue, preventative measures against cyberattacks, and sanctions against those involved in cyberattacks (http://www.consilium.europa.eu/en/press/press-releases/2020/05/14/cyber-security-council-extends-sanctions-regime-until-18-may-2021/) threatening the EU.

The Commission assists in decision-making on responding to external cyber threats wherever needed. It also directly funds the ongoing EU Cyber Diplomacy Support Initiative (https://eucyberdirect.eu/).

Cyber Defence

On 10 November 2022, the Commission and the High Representative put forward a Joint Communication on an EU Cyber Defence Policy (https://www.eea.europa.eu/sites/default/files/documents/Comm_cyber%20defence.pdf) to address the deteriorating security environment following Russia’s aggression against Ukraine and to boost the EU’s capacity to protect its citizens and infrastructure.

The EU Policy on Cyber Defence (https://ec.europa.eu/commission/presscorner/detail/en/ip_22_6642) is built around four pillars that cover a wide range of initiatives that will help the EU and Member States to be better able to detect, deter and defend against cyber-attacks:

1. Act together for a stronger EU cyber defence
2. Secure the defence ecosystem
3. Invest in cyber defence capabilities
4. Partner to address common challenges

The new policy calls for investments in full-spectrum cyber defence capabilities and will strengthen coordination and cooperation between the EU military and civilian cyber communities. It will enhance cooperation with private sector and efficient cyber crisis management within the Union. The new policy will also help reduce our strategic dependencies in critical cyber technologies, and strengthen the European Defence Technological Industrial Base (EDTIB). It will stimulate training, attracting and retaining cyber talents.


Cyber capacity building in third countries

The EU cooperates with other countries to help build up their capacity to defend against cybersecurity threats. The Commission supports various cybersecurity programmes in the Western Balkans and
the six eastern partnership countries in the EU’s immediate neighbourhood, as well as in other countries worldwide through its International Cooperation and Development department.

Follow the latest progress and learn more about getting involved.

- Follow the Commission's work on cybersecurity @CyberSec_EU (https://twitter.com/cybersec_eu?lang=en)

**Latest News**

PRESS RELEASE | 05 December 2023
The Commission has approved, under EU State aid rules, an Important Project of Common European Interest ('IPCEI') to support research, development and first industrial deployment of advanced cloud and edge computing technologies across multiple providers in Europe.

PRESS RELEASE | 01 December 2023
Commission welcomes political agreement on Cyber Resilience Act

The Commission welcomes the political agreement reached last night between the European Parliament and the Council on the Cyber Resilience Act, proposed by the Commission in September 2022.

PRESS RELEASE | 24 November 2023
EU and Canada launch Digital Partnership to strengthen strategic cooperation

Today, the EU and Canada strengthened their relationship as strategic and like-minded partners in the digital field.

PRESS RELEASE | 21 November 2023
EU cybersecurity exercise to foster cooperation and promote free and fair EU elections

To evaluate and strengthen current working methods ahead of the 2024 elections, EU institutions have organised a cybersecurity exercise. National and EU partners tested their crisis plans and possible responses to potential cybersecurity incidents affecting the European elections.

Browse Cybersecurity
Library

- 01-12-2023  
  Cyber Resilience Act - Factsheet  

- 10-11-2023  
  Kick-off event with EU Cybersecurity Skills Academy Pledgers  

- 16-10-2023  
  Japan-US-EU Industrial Control Systems Cybersecurity Week for the Indo-Pacific Region  
Events

- 06-05-2023  
  #DigitalEU at the European Open Day on Saturday, 6 May  

- 15-06-2023 - 16-06-2023  
  Digital Assembly 2023: A Digital, Open and Secure Europe  

- 27-01-2023  
  Transatlantic Tech and Security: A Conversation with EU Commissioner Thierry Breton  
Consultation

- 16-03-2022 - 25-05-2022
- 12-05-2021 - 02-09-2021
  Public consultation on a set of European Digital Principles
- 07-07-2020 - 02-10-2020
  Public consultation on the Directive on security of network and information systems (NIS Directive)
The EU has outlined a cybersecurity strategy to boost Europe’s ability to fight and recover from cyberattacks.
On the 18 April 2023, the European Commission proposed the EU Cyber Solidarity Act, to improve the preparedness, detection and response to cybersecurity incidents across the EU.

New EU cybersecurity rules ensure safer hardware and software.

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...

The European Cybersecurity Network and Cybersecurity Competence Centre help the EU retain and develop cybersecurity technological and industrial capacities.

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

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 for ICT products enables the creation of tailored and risk-based EU certification schemes.
The NIS2 Directive is the EU-wide legislation on cybersecurity. It provides legal measures to boost the overall level of cybersecurity in the EU.

**See Also**


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

**Related Content**


The Digital Europe Programme will help the EU achieve a high common level of cybersecurity.

---

**Source URL:** [https://digital-strategy.ec.europa.eu/policies/cybersecurity-policies](https://digital-strategy.ec.europa.eu/policies/cybersecurity-policies)