

## European Cybersecurity Competence Network and Centre

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



### Aims of this initiative

By managing the cybersecurity funds under the next multi-annual financial framework 2021-2027, the initiative will help to create an inter-connected, EU-wide cybersecurity industrial and research ecosystem. It should encourage better cooperation between relevant stakeholders, including between cybersecurity civilian and defence sectors.

This cooperation will help stakeholders to make the best use of existing cybersecurity resources and expertise across Europe. The initiative builds on the expertise that already exists in more than 660 cybersecurity expertise centres from all Member States who responded to a survey conducted by the European Commission in 2018.

The initiative should help the EU and Member States take a proactive, longer-term strategic perspective to cybersecurity industrial policy going beyond research and development. This approach should help to come up with breakthrough solutions to the cybersecurity challenges which the private and public sectors are facing and support the effective deployment of these solutions.

It will allow relevant research and industrial communities and public authorities to gain access to key capacities such as testing and experimentation facilities. These facilities are often beyond the reach of individual Member States due to insufficient financial and human resources.

The initiative will contribute to closing the skills gap and to avoiding a brain drain by ensuring access of the best talents to large-scale European cybersecurity research and innovation projects and therefore providing interesting professional challenges.

## **Network of National Coordination Centres**

Each Member State will nominate one National Coordination Centre. They will function as contact points at the national level for the Competence Community and the Competence Centre. They are the 'gatekeepers' for the cybersecurity community in their country. They support to carry out actions under this Regulation, and they can pass on financial support to national and local ecosystems.

## **The Cybersecurity Competence Community**

This Community will involve a large, open, and diverse group of actors involved in cybersecurity technology, including in particular research entities, supply/demand-side industries and the public sector. It will provide input to the activities and work plan of the Competence Centre. And, it will benefit from the community-building activities of the Competence Centre and the Network.

## **The European Cybersecurity Competence Centre**

The European Cybersecurity Competence Centre (ECCC) aims to increase Europe's cybersecurity capacities and competitiveness. It will work together with a Network of National Coordination Centres (NCCs) to build a strong cybersecurity community. Located in Bucharest, it will implement relevant parts of the Digital Europe and Horizon Europe programmes by allocating grants and carrying out procurements.

### **Tasks and objectives**

The ECCC will seek to achieve its overall mission by:

- setting up and helping to coordinate the National Coordination Centres Network and the cybersecurity competence community;
- making strategic investment decisions and pooling resources from the EU, its Member States and industry;
- implementing cybersecurity-related financial support from Horizon Europe and Digital Europe Programmes.

This will feed into the following objectives:

- contributing to the wide deployment of the latest cybersecurity technology, in particular through carrying out or supporting procurement of products and solutions;
- providing financial support and technical assistance to cybersecurity start-ups and a to connect them to potential markets and to attract investment;
- supporting research and innovation based on a comprehensive industrial and research agenda, including large-scale research and demonstration projects in next-generation cybersecurity capabilities;
- driving high cybersecurity standards not only in technology and cybersecurity systems but also in skills development;
- facilitating the cooperation between the civil and defence spheres with regard to dual use technologies and applications, and enhancing civil-defence synergies in relation to the European Defence Fund.

## **Governance structure**

The ECCC is currently being set up. Its administrative and governance structure will include:

- a Governing Board, to provide strategic orientation and oversee its activities;
- an Executive Director, to be the legal representative and to be responsible for day-to-day management;
- a Strategic Advisory Group to ensure a comprehensive, ongoing dialogue between the ECCC and the cybersecurity community.

The Governing Board will include:

- one representative from each member State, and two from the Commission, serving for a renewable four year term;
- observers, including ENISA permanently, and others on an ad-hoc basis;
- a Chairperson and deputy Chairperson, elected for three years, once renewable;
- the Executive Director, who takes part but has no voting rights.

In principle, decisions will be taken by consensus. Where this is not possible, there needs to be a majority of at least 75% of all votes. For joint actions, the vote will be proportional to the financial contributions of those involved. The EU holds 26% of voting rights for any decision affecting the EU budget .

The Governing Board is assisted by an Industrial and Scientific Advisory Board to ensure regular dialogue with the private sector, consumers' organisations and other relevant stakeholders.

## **Financial resources**

The European Commission proposes that the Competence Centre is funded jointly through financial contributions from the European Union and the participating Member States.

The European Commission has placed cybersecurity high on the agenda for the next long-term EU budget for years 2021-2027. Under the new Digital Europe programme the European Commission proposed in 2018 to invest €2 billion into safeguarding the EU's digital economy, society and democracies through polling expertise, boosting EU's cybersecurity industry, financing state-of-the-art cybersecurity equipment and infrastructure. Cybersecurity research and innovation will additionally be supported under the Horizon Europe programme.

The ECCC and Network will also seek to achieve synergies with other relevant EU programmes where appropriate.

The participating Member States should match the EU's financial contribution with investments of the same amount in line with their priorities and with co-financing of the running costs of the Centre and the Network.

The concrete funding priorities will be established as part of the Competence Centres annual Work Plan, which will be adopted by the Governing Board after having received input from the Industrial and Scientific Advisory Group.

It is envisioned that the bulk of the funding will be allocated through open calls for proposals and calls for tender. Stakeholders know this system from the past Research and Innovation Framework Programmes. In these cases, the Competence Centre will manage and eventually disburse financial support to recipients, which would typically be academic and research entities, industrial companies,

or public authorities.

The ECCC will also seek to promote joint procurement of strategic cybersecurity infrastructures and tools together with one or several other entities – typically public authorities.

Some funding will be made available directly to National Coordination Centres for them to carry out tasks under this Regulation.

National Coordination Centres will also be able to financially support their respective national ecosystems through the use of so-called cascading grants.

Website of the European Cybersecurity Competence Centre and Network

The four pilot projects

Instagram: Cybersecurity Competence Centre

Follow the latest progress and learn more about getting involved.





Follow the Cybersecurity Competence Centre on Twitter @Cybersec\_ECCC

## Latest

PRESS RELEASE | 30 September 2021

Trade and Technology Council: Inaugural meeting  
agrees on important deliverables and outlines  
areas for future EU-US cooperation

At the first meeting of the Trade and Technology  
Council (TTC) in Pittsburgh, the EU and the US  
agreed on concrete deliverables and outlined the

future scope of work. Notably, the EU and the US committed to cooperating closely on shared priorities such as export controls, foreign investment screening, critical and emerging technology standards including Artificial Intelligence, and secure supply chains including on semiconductors. They also agreed to work together on important global trade issues, such as the challenges posed by non-market economies and trade-related climate and environment

PRESS RELEASE | 30 September 2021

The European Cybersecurity Month is kicking off:  
'Think Before U Click'

The ninth edition of the European Cybersecurity Month has kicked off and will run for the entire month of October under the motto 'Think Before U Click'. This is an annual awareness campaign organised by the Commission, the European Union Agency for Cybersecurity (ENISA) and over 300 partners in the Member States, including local authorities, governments, universities, think tanks, NGOs and professional associations.

PRESS RELEASE | 28 June 2021

The European Cybersecurity Competence Centre and Network is now ready to take off

The regulation establishing a new Cybersecurity Competence Centre and a Network of National Coordination Centres has entered into force this week. The Cybersecurity Competence Centre, which will be located in Bucharest, will contribute to strengthening European cybersecurity capacities and to boosting research excellence and the competitiveness of the Union's industry in the cybersecurity field.

PRESS RELEASE | 23 June 2021

EU Cybersecurity: Commission proposes a Joint Cyber Unit to step up response to large-scale security incidents

The Commission has laid out a vision to build a new Joint Cyber Unit to tackle the rising number of serious cyber incidents impacting public services, as well as the life of businesses and citizens across the European Union. Advanced and coordinated responses in the field of cybersecurity have become increasingly necessary, as cyberattacks grow in number, scale and consequences, impacting heavily our security. All relevant actors in the EU need to be prepared to respond collectively and exchange relevant information on a 'need to share', rather than only 'need to know', basis.

[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

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 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.

---

**Source URL:** <https://digital-strategy.ec.europa.eu/policies/cybersecurity-competence-centre>