European Commission

Digital Single Market

Building strong cybersecurity in Europe

#DSM

#Cybersecurity

December 2018

'Cyber-attacks know no borders, but our response capacity differs very much from one country to the other, creating loopholes where vulnerabilities attract even more the attacks. The EU needs more robust and effective structures to ensure strong cyber resilience and respond to cyber-attacks. We do not want to be the weakest links in this global threat.'

Jean-Claude Juncker, Tallinn Digital Summit, 29 September 2017

To equip Europe with the right tools to deal with an ever-changing cyber threat, in 2017 the European Commission and the High Representative proposed a wide-ranging set of measures to build strong cybersecurity in the EU. On 10 December 2018 the European Parliament, the Council of the EU and the Commission agreed on the Cybersecurity Act which reinforces the mandate of the EU Agency for Cybersecurity, (European Union Agency for Network and Information and Security, ENISA) so as to better support Member States with tackling cybersecurity threats and attacks. The Act also establishes an EU framework for cybersecurity certification, boosting the cybersecurity of online services and consumer devices.

Today's cyber threats

+4,000 ransomware attacks per day in 2016

80% of European companies experienced at least one cybersecurity incident last year

Security incidents across all industries **rose by 38%** – the biggest increase in the past 12 years

In some Member States **50% of all crimes committed** are cybercrimes

+150 countries and +230,000 systems across sectors and countries were affected by Wannycry attack in May 2017 with a substantial impact on essential services connected to the internet, including hospitals and ambulance services.

Strengthening resilience to cyber-attacks

The Commission is already supporting the reinforcement of the EU's deterrence of, and resilience and response to, cyber-attacks, including by:

Supporting effective implementation of the first EU cybersecurity law (Directive on Security of Network and Information Systems), with:

The EU institutions agreed on:

GREATER CAPABILITIES

Member States have to improve their cybersecurity capabilities

COOPERATION

Increased EU-level cooperation

RISKS PREVENTION

Players in key sectors (such as energy, transport, health) are obliged to put in place measures to prevent risks and handle cyber incidents

EU CYBERSECURITY AGENCY

Strengthening the European Union Agency for cybersecurity to better assist Member States

EU CERTIFICATION FRAMEWORK

An EU-wide certification framework to ensure that products and services are cyber-secure

COORDINATED RESPONSE

Ensuring fast and coordinated responses to large scale cyber-attacks

The European Union Agency for Network and Information Security assists Member States' cybersecurity authorities in better protecting the EU against cyber-attacks.

- A strong mandate
- A permanent status
- Adequate resources

ENISA RESOURCES	Now	Future
Staff	84 people	125 people
Budget	€11 million	€23 million
	gradual increase: starting with +5 million 1st year and fully achieved 4 years after entry into force	

Pooling resources and expertise in cybersecurity technology

Beyond the EU cybersecurity initiatives which have been agreed so far, the Commission also proposed to create a Network of Competence Centres and a European Cybersecurity Industrial, Technology and Research Competence Centre to develop and roll out the tools and technology needed to keep up with an ever-changing threat.

The European Centre will be in charge of coordinating the funds foreseen for cybersecurity in the next long-term EU budget together with the Member States in the most targeted way. This will help to create new European cyber capabilities.

A wealth of expertise already exists in Europe - there are more than **660 cybersecurity competence centres** spread across the EU. To draw on and use their expertise effectively, a new mechanism will now:

Pool, share and ensure access to existing expertise

Help deploy EU cybersecurity products and solutions

Ensure long-term strategic cooperation between industries, research communities and governments

Co-invest and share costly infrastructure

European Competence Centre:

Will coordinate the use of the funds foreseen for cybersecurity under the next long-term EU budget for years 2021-2027 under the Digital Europe and Horizon Europe programmes. The centre will support the Network and Community to drive the **cybersecurity** research and innovation. It will also organise **joint investments** by the EU, Member States, and industry. For example, under the Digital Europe programme **€2 billion** will be invested in safeguarding the EU's digital economy, society and democracies by boosting the EU's cybersecurity industry and financing state-of-the-art cybersecurity equipment and infrastructure.

Network of National Coordination Centres:

Each Member State will nominate one national coordination centre to lead the network, which will engage in the development of new cybersecurity capabilities and broader competence building. The network will help to identify and support the most relevant cybersecurity projects in the Member States.

Competence Community:

A large, open and diverse group of cybersecurity stakeholders from research and the private and public sectors, including both civilian and defence authorities.

What will improve?

- better coordination of work;
- access to expertise;
- access to testing and experimental facilities;
- assessment of product cybersecurity;
- access to innovative cybersecurity products and solutions;
- support for market deployment of products and services;
- increased visibility towards potential investors and business partners;
- cost-saving by co-investment with other Member States;
- EU capacity to autonomously secure its economy and democracy;
- EU becoming a global leader in cybersecurity.

Who will benefit?