Building STRONG CYBERSECURITY in the European Union

RESILIENCE. DETERRENCE. DEFENCE.

"Cyber-attacks can be more dangerous to the stability of democracies and economies than guns and tanks. [...] Cyber-attacks know no borders and no one is immune."

European Commission President Jean-Claude Juncker,
State of the Union Address, 13 September 2017

A SECURE EUROPEAN DIGITAL SINGLE MARKET

One we all trust

THE EUROPEAN CONTEXT

The digital era is creating numerous new opportunities for the economy and society. But, at the same time, it introduces new challenges.

Our adversaries want to disrupt and dismantle our common digital future. We cannot, and will not, let them.

Cyber-incidents and cyber-attacks cause the loss of billions of euros every year. Cybersecurity, trust and privacy are the foundations of a prosperous European Digital Single Market.

The EU has adopted a wide-range of measures to shield the European Digital Single Market and protect infrastructure, governments, businesses and citizens.

EUROPE'S STRENGTH LIES IN ITS DIVERSITY, SKILLS AND COMMITMENT TOWARDS STRONG CYBERSECURITY

- EU diversity and solidarity
- Cybersecurity is a top priority
- A high level of cybersecurity expertise
- A strong cybersecurity industry with innovative SMEs
- A growing Digital Single Market

A SECURE AND TRUSTED DIGITAL SINGLE MARKET

European countries occupy 18 of the top 20 places in the global National Cybersecurity Index, a ranking of countries based on their preparedness to prevent cyber threats and manage cyber incidents. (Data: NCSI Index)

€30 billion

EU cybersecurity market in 2020

+10%

Growth per year

+60,000

Cybersecurity companies in the EU

+660

Centres of cybersecurity expertise exist across the European Union

(Data: European Commission)

EU citizens are concerned about cybersecurity and privacy

(Data: Eurobarometer 2018 on attitudes towards cybersecurity)

88%

daily Internet users expressed big concerns regarding becoming the victim of cyber-attacks

77%

daily Internet users expressed big concerns about their personal information not being kept safe by websites

EU cybersecurity and digital privacy at a glance

Cooperation

- NIS Directive
- Public-Private Partnership with ECSO
- eIDAS
- Cyber diplomacy

Greater Capabilities

- NIS Directive
- EU Cybersecurity Act
- Horizon 2020 Programme
- Connecting Europe Programme

Risk Prevention

- NIS Directive
- EU Cybersecurity Act
- GDPR

In the future:

- A European Cybersecurity Competence Centre and Network

Coordinated response

- NIS Directive
- EU Blueprint cyber crisis
- Cyber diplomacy

EU Cybersecurity Certification framework

- EU Cybersecurity Act

And the EU is enhancing its cybersecurity preparedness for the future:

- A European Cybersecurity Industrial, Technology and Research Competence Centre and a Network of National Coordination Centres
- Duty of care
- Security and privacy by design
- 5G Security
- Artificial intelligence
- Liability issues for emerging technologies
- An increase in the EU investment in cybersecurity research, innovation and deployment

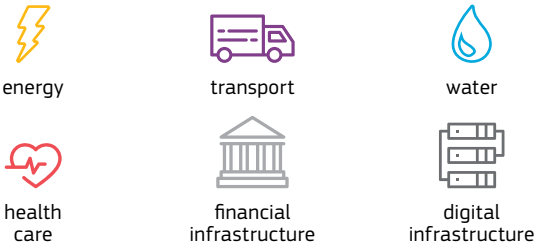
BUILDING THE CAPACITY TO PROTECT

The EU works on many fronts to strengthen cybersecurity and cyber resilience. It has an advanced cybersecurity regulatory framework in place.

The Network and Information Security Directive (NIS)

The NIS legislation 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:

- Creates a culture of security across vital sectors of our economy and society:



- Increases national cybersecurity capabilities by requiring EU Member States to have:
  - A National Cybersecurity strategy
  - National Computer Emergency Response Teams (CSIRTs)
  - NIS national competent authorities
  - A Single Point of Contact (SPOC)
- Enhances EU-level cooperation and sharing of information by establishing:
  - The CSIRTs Network – a network composed of EU Member States' appointed CSIRTs and CERT-EU
  - The NIS Cooperation Group - composed of representatives of the EU Member States, the European Commission and the ENISA

EU Cybersecurity Act

The EU's Cybersecurity Act sets:

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

The European Cybersecurity Certification Framework

- A common European approach to cybersecurity certification as a vital element of Europe's Digital Single Market.
- Modern, dynamic and risk-based cybersecurity certification schemes.
- Open, inclusive and transparent governance framework with multiple opportunities for stakeholder contributions.
- Market oriented with a strong emphasis on the use of globally relevant international standards.

Formed in 2004, the **European Union Agency for Network and Information Security** (ENISA) in Athens, Greece, is Europe's foremost centre for cybersecurity expertise, working closely with EU countries and the private sector, to advise on and resolve critical problems of the day.

Coordinated Response to Large-Scale Cyber Incident – the Blueprint

- Cross-border response procedures
- European training and exercises
- Cyber incident taxonomy
- Swift and effective cooperation
- EU-wide cybersecurity exercises

NEW EFFORTS TO STEP UP CYBERSECURITY IN THE EUROPEAN UNION

Establishing a Network of Cybersecurity National Centres with a new European Cybersecurity Industrial, Technology and Research Competence Centre at its heart, in order to:

- Pool, share and ensure access to existing expertise
- Help deploy EU cybersecurity products and solutions
- Ensure long-term strategic cooperation between industries, research communication and governments
- Co-invest and share costly infrastructure

The European Cybersecurity Industrial, Technology and Research Competence Centre

Centre's Role:

- Network coordination and support
- Research programming and implementation
- Procurement
- Ensuring synergies between civilian and defence spheres

A Network of National Cybersecurity Centres

Each EU 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 priorities in the EU countries.

INVESTMENT IN CYBERSECURITY RESEARCH, INNOVATION & DEPLOYMENT

The European Union has been investing in cybersecurity and privacy research and innovation since the early '90s.

1,352 organisations involved in **132** EU cybersecurity and privacy R&I projects across Europe.

(Data: Cyberwatching.eu)

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
- Crack challenges
- Supports a cross-border and transgovernmental collaboration
- Promotes the sharing of knowledge
- Provides input to shape the future EU policies

European Union and cybersecurity industry public-private partnership

The contractual public-private partnership of the European Union with the European Cyber Security Organisation (ECSO) will have triggered € 1.8 billion of investment in cybersecurity by 2020.

CYBERSECURITY ENHANCES DIGITAL PRIVACY

Europeans have set high standards for digital privacy. These standards help deliver better cybersecurity.

ePrivacy Directive – Shielding confidentiality of our online communications

The ePrivacy Directive ensures the confidentiality of communications and defines the rules regarding online tracking and monitoring. It is now being updated to cover the new means of online communications, such web emails and messenger services (ePrivacy Regulation).

General Data Protection Regulation (GDPR) – A European success story complied with worldwide

The GDPR, introduced in May 2018, provides new rules to give citizens more control over their personal data, and a competitive edge to compliant businesses.

eIDAS Regulation

The electronic identification, authentication and trust services (eIDAS) system came into force in October 2018, introducing safe ways for individuals and companies to perform transactions online. It includes:

- A cross-border digital signature system
- GDPR-compliant digital profiling
- Compliance with the “once-only principle”, where citizens and companies only have to provide standard information to authorities once.

CYBER DIPLOMACY

The European Union and its Member States strongly promote an open, free, 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 outreach and capacity building to promote responsible state behaviour and advance global cyber resilience.
- commit to prevent conflicts and advance cyber stability through the use of law-enforcement, legal and economic and diplomatic instruments, including if necessary sanctions.

Building STRONG CYBERSECURITY in the European Union

RESILIENCE. DETERRENCE. DEFENCE.

The European Union and the EU Member States are building the necessary cybersecurity culture and capabilities to resist and counteract the very real and ever-changing cyber threats and cyber-attacks.

The European Union stands ready to take up the challenges of tomorrow.

Cyberwatching.eu has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 740129.