
# Building STRONG CYBERSECURITY in the European Union

*"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.

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 TO STRONG CYBERSECURITY

Our assets:

- Cybersecurity as a top EU priority
- High-level cybersecurity expertise
- Strong cybersecurity industry with our innovative SMEs
- A growing Digital Single Market
- EU solidarity

# 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)

**+€130 billion**
EU cybersecurity market

**+17%**
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

- Security of Network & Information Systems Directive (NIS)
- Cybersecurity public-private partnership
- Electronic Identification Regulation (eIDAS)
- Cyber diplomacy
- EU Cybersecurity Act Regulation

## Risk Prevention

- Security of Network & Information Systems Directive (NIS)
- EU Cybersecurity Act Regulation
- General Data Protection Regulation (GDPR)

## Greater Capabilities

- Security of Network & Information Systems Directive (NIS)
- EU Cybersecurity Act Regulation
- Horizon 2020 EU research programme
- Connecting Europe funding programme

**In the future:**

- A European Cybersecurity Competence Centre and Network

## Coordinated response

- NIS Directive
- EU cyber-crisis blueprint
- Cyber diplomacy

## EU Cybersecurity Certification framework

- EU Cybersecurity Act Regulation

## 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

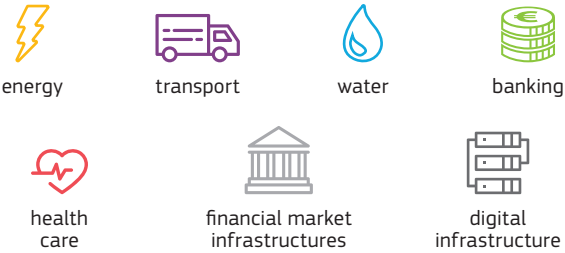
# BUILDING THE CAPACITY TO PROTECT

**THE EU WORKS ON MANY FRONTS TO STRENGTHEN CYBERSECURITY AND CYBER RESILIENCE. IT HAS AN ADVANCED CYBERSECURITY REGULATORY FRAMEWORK IN PLACE.**

## THE DIRECTIVE ON SECURITY OF NETWORK AND INFORMATION SYSTEMS (NIS)

The NIS Directive 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
- 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 EU Agency for Cybersecurity (ENISA)

## EU CYBERSECURITY ACT

The EU's Cybersecurity Act sets:

- A permanent mandate and stronger role for the European Union Agency for Cybersecurity (ENISA)
- 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 Cybersecurity** (ENISA) in Athens, Greece is working closely with EU Member States and the private sector to advise on and resolve critical problems of the day.

## EU Blueprint for COORDINATED RESPONSE TO LARGE-SCALE CYBER INCIDENTS

- Cross-border response procedures
- Cyber incident taxonomy
- Swift and effective cooperation
- Preparedness

# 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 community 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

## A NETWORK OF NATIONAL CYBERSECURITY CENTRES

Each Member State will put in place one national coordination centre to work in the network to develop new European cybersecurity capabilities. The network will identify and support the key cyber research and development priorities in the EU.

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

## EUROPEAN COMMISSION AND CYBERSECURITY INDUSTRY PUBLIC-PRIVATE PARTNERSHIP

The contractual public-private partnership of the European Commission with the European Cyber Security Organisation (ECSO) will have triggered more than € 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 – EU-WIDE ELECTRONIC IDENTIFICATION AND AUTHENTICATION SYSTEM

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.