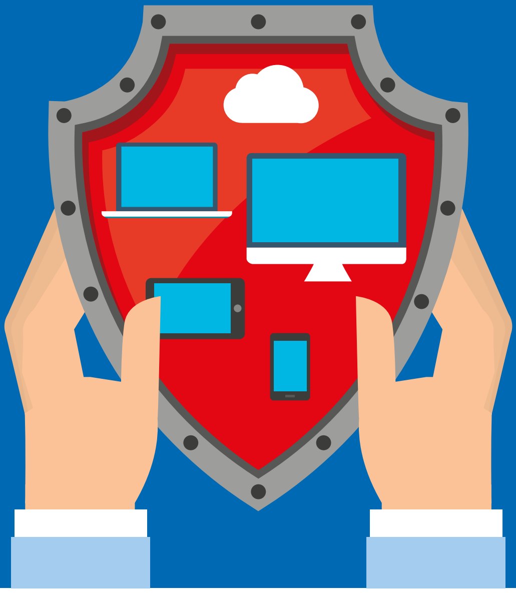
European Commission

EU cybersecurity initiatives

working towards a more secure online environment



January 2017

Since the adoption of the EU Cybersecurity Strategy in 2013, the European Commission has stepped up its efforts to better protect Europeans online. It has adopted a set of legislative proposals, in particular on network and information security, earmarked more than €600 million of EU investment for research and innovation in cybersecurity projects during the 2014-2020 period, and fostered cooperation within the EU and with partners on the global stage.

The Commission has further strengthened its approach in the past year by including cybersecurity at the heart of its political priorities: **trust and security** are at the core of the Digital Single Market Strategy presented in May 2015, while the **fight against cybercrime** is one of the three pillars of the European Agenda on Security adopted in April 2015.

In July 2016, delivering on these strategies, the Commission presented additional measures to boost the cybersecurity industry and to tackle cyber-threats.

The adoption of the **Directive on security of network and information systems (NIS Directive)** by the European Parliament in July 2016 is another important milestone towards a more secure online environment.

Why is cybersecurity so important?

Over the past years, digital technologies have become the backbone of our economy and are a critical resource all economic sectors rely on. They now underpin the complex systems which keep our economies running in, for example, finance, health, energy and transport. Many business models are built on the uninterrupted availability of the internet and the smooth functioning of information systems

Cybersecurity incidents, be they intentional or accidental, could disrupt the supply of essential services we take for granted such as water or electricity. Threats can have different origins - including criminal, terrorist or state-sponsored attacks as well as natural disasters and unintentional mistakes.

By completing the Digital Single Market, the EU could boost its economy by almost €415 billion per year and create hundreds of thousands of new jobs.

But for new connected technologies to take off - including e-payments, cloud computing or machine-to- machine communication - Europeans need trust and confidence.

The digital world should be protected from incidents, malicious activities and misuse. It is a priority for the Commission to help prevent these incidents, and in case they occur, provide the most efficient response.

Both governments and the private sector have a significant role to play - this is why the Commission works with all these actors to strengthen cybersecurity.

What are the key objectives of the Commission in the field of cybersecurity?

1. **Increasing cybersecurity capabilities and cooperation**

   The aim is to bring cybersecurity capabilities at the same level of development in all the EU Member States and ensure that exchanges of information and cooperation are efficient, including at cross-border level.

2. **Making the EU a strong player in cybersecurity**

   Europe needs to be more ambitious in nurturing its competitive advantage in the field of cybersecurity to ensure that European citizens, enterprises (including SMEs), public administrations have access to the latest digital security technology, which is interoperable, competitive, trustworthy and respects fundamental rights including the right to privacy. This should also help take advantage of the booming global cybersecurity market. To achieve this Europe needs to overcome the current cybersecurity market fragmentation and foster European cybersecurity industry.

3. **Mainstreaming cybersecurity in EU policies**

   The objective is to embed cybersecurity in the future EU policy initiatives from the start, in particular with regard to new technologies and emerging sectors such as connected cars, smart grids and the Internet of Things (loT).

What is the Commission doing to strengthen cybersecurity?

The Commission has put forward several initiatives and is contributing to a series of key measures:

1. EU STRATEGIES

EU Cybersecurity Strategy (2013)

The Commission and the European External Action Service launched the EU Cybersecurity Strategy in 2013. The strategy outlines the principles that will guide the EU action in this domain - for example on the importance of access to the internet and of the protection of fundamental rights online. It sets five priorities:

1. increasing **cyber resilience**;
2. drastically reducing **cybercrime**;
3. developing EU **cyber defence policy** and capabilities related to the Common Security and Defence Policy (CSDP);
4. developing the **industrial and technological resources** for cybersecurity;
5. establishing a **coherent international cyberspace** policy for the EU and promote core EU values

European Agenda on Security (2015)

Fighting cybercrime more effectively is one of the three priorities under the new European Agenda on Security 2015-2020 which was adopted by the Commission in April 2015. Cybercrime requires a coordinated response at European level.

Therefore, the European Agenda on Security sets out the following actions:

- giving renewed emphasis to **implementation of existing policies on cybersecurity, attacks against information systems, and combating child sexual exploitation**;
- reviewing and possibly extending legislation on **combatting fraud and counterfeiting of non-cash means of payments** to take account of newer forms of crime and counterfeiting in financial instruments, with proposals in 2016;
- reviewing obstacles to **criminal investigations on cybercrime**, notably on issues of competent jurisdiction and rules on access to evidence and information;
- enhancing **cyber capacity building action** under external assistance instruments.

Digital Single Market Strategy (2015)

Trust and security are essential to reap the benefits of the digital economy. This is why the Digital Single Market Strategy presented in May 2015 includes a public-private partnership (PPP) on cybersecurity.

The partnership was signed on 5 July 2016 by the Commission and the European Cyber Security Organization (ECSO) - an industry-led association, which includes a wide variety of stakeholders such as large companies, SMEs and start-ups, research centers, universities, end-users, operators, clusters and association as well as public authorities.

The goal of this partnership is to stimulate European competitiveness and help overcome cybersecurity market fragmentation through innovation, building trust between Member States and industrial actors as well as helping align the demand and supply sectors for cybersecurity products and solutions.

This partnership will be instrumental in structuring and coordinating digital security industrial resources in Europe. It includes a wide range of actors, from innovative SMEs to producers of components and equipment, critical infrastructure operators and research institutes. The initiative will leverage EU, national, regional and private efforts and resources - including research and innovation funds - to increase investments in cybersecurity.

Ultimately, the partnership helps to:

- gather industrial and public resources to deliver innovation against a **jointly-agreed strategic research and innovation roadmap**;
- **focus on targeted technical priorities** defined jointly with industry;
- **maximize the impact of available funds**;
- provide visibility to **European research and innovation excellence** in cybersecurity.

The partnership is supported by EU funds coming from the Horizon 2020 Research and Innovation Framework Programme (H2020) with a total investment of up to **€450 million** until 2020. The Commission aims at launching the first H2020 calls for proposals under the cybersecurity PPP in the first quarter of 2017.

Communication on Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry (2016)

Delivering on the EU Cybersecurity Strategy and the Digital Single Market Strategy, the Commission adopted the Communication Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry on 5 July 2016.

It includes a set of measures aiming at:

- **Stepping up cooperation across Europe**: the Commission encourages Member States to make the most of the cooperation mechanisms under the NIS Directive and to improve the way in which they work together to prepare for a large-scale cyber incident. This includes more work on education, training and cybersecurity exercises.
- **Supporting the emerging single market for cybersecurity products and services in the EU**: for example, the Commission will explore the possibility of creating a framework for certification of relevant ICT products and services, complemented by a voluntary and light weight labelling scheme for the security of ICT products; the Commission suggests also possible measures to scale up cybersecurity investment in Europe and to support SMEs active in the market.
- **Establishing a contractual public-private partnership (PPP) with industry**, to nurture cybersecurity industrial capabilities and innovation in the EU (cf. above).

2. EU LEGISLATION

Directive on Network and Information Security

In 2013 the Commission proposed the Directive on security of network and information systems (NIS Directive) aiming at ensuring a high common level of cybersecurity in the EU. Negotiators of the European Parliament, the Council and the Commission found an agreement on the text on 7 December 2015.

Following the political agreement reached on 7 December 2015, the text of the NIS Directive was adopted by the European Parliament on 6 July 2016 and entered into force in August 2016. Member States will have 21 months to transpose the Directive into their national laws and 6 months more to identify operators of essential services.

The Directive builds on three main pillars:

- ensuring **Member States preparedness** by requiring them to be appropriately equipped, e.g. via a Computer *Security Incident* Response Team (CSIRT) and a competent national *NIS authority*;
- ensuring **cooperation** among all the Member States, by setting up a 'Cooperation Group', in order to support and facilitate strategic cooperation and the exchange of information among Member States, and a 'CSIRT Network', in order to promote swift and effective operational cooperation on specific cybersecurity incidents and sharing information about risks;
- ensuring a **culture of security** across sectors which are vital for our economy and society and moreover rely heavily on information and communications technologies (ICT). Businesses with an important role for society and economy that are identified by the Member States as operators of essential services under the NIS Directive will have to take appropriate security measures and to notify serious incidents to the relevant national authority. These sectors include **energy**, **transport**, **water**, **banking**, **financial market infrastructures**, **healthcare** and **digital infrastructure**. Also key digital service providers (search engines, cloud computing services and online marketplaces) will have to comply with the security and notification requirements under the new Directive. Similar requirements already apply to telecom operators and internet service providers through the EU telecoms regulatory framework.

Legislative actions to fight cybercrime

Several EU legislative actions contribute to the fight against cybercrime. These include

- 2013 – A Directive on attacks against information systems, which aims to tackle large-scale cyber- attacks by requiring Member States to **strengthen national cybercrime laws and introduce tougher criminal sanctions**. This Directive had to be implemented by Member States by September 2015 and the Commission is currently checking implementation. Five infringement procedures for partial or noncommunication have been launched in December 2015. An implementation report will be published in 2017.
- 2011 – A Directive on combating the **sexual exploitation of children online and child pornography**, which better addresses new developments in the online environment, such as grooming (offenders posing as children to lure minors for the purpose of sexual abuse). This legislation had to be transposed by 2013, and the Commission is currently verifying implementation. Two reports on implementation were issued at the end of 2016.
- 2001 – Framework Decision on **combating fraud and counterfeiting of non-cash means of payment**, which defines the fraudulent behaviours that EU States need to consider as punishable criminal offences. The Commission is assessing the need to revise this Framework Decision to cover new forms of money transmissions like virtual currencies and other aspects, with a plan to come forward with any new initiative for the first quarter of 2017.

3. NETWORKS / ORGANISATIONS

The European Union Agency for Network and Information Security

The European Union Agency for Network and Information Security (ENISA) was set up in 2004 to contribute to the overall goal of ensuring a high level of network and information security within the EU.

ENISA helps the Commission, the Member States and the business community to address, respond and especially to prevent NIS problems. The main activities run by ENISA include:

- collecting and analysing data on security incidents in Europe and emerging risks;
- promoting risk assessment and risk management methods to enhance capability to deal with information security threats;
- running of pan-European cyber exercises;
- supporting Computer Emergency Response Teams (CERTs) cooperation in the Member States;
- • awareness-raising and cooperation between different actors in the information security field.

In order to boost the overall level of online security in Europe, the agency organises each October the Cybersecurity Month awareness campaign, with the support of NIS contact points in all Member States.

ENISA's current mandate expires in 2020; taking also into account the reinforced role the NIS Directive attributes now to the Agency and the developments in the threat landscape, the Commission has advanced its evaluation and included the revision of the Regulation currently setting ENISA's mandate and tasks in the Commission Work Programme for 2017. A public consultation on ENISA's evaluation and review is open for contribution from interested stakeholders until 12 April 2017.

The EU Computer Emergency Response Team

The EU Computer Emergency Response Team (CERT-EU) was set up in 2012 with the aim to provide effective and efficient response to information security incidents and cyber threats for the EU institutions, agencies and bodies. The European Commission has some of its security experts in the core team of CERT-EU, together with experts from the General Secretariat of the Council, the European Parliament, the Committee of the Regions and the Economic and Social Committee. CERT-EU also cooperates with other CERTs in the Member States and beyond as well as with specialised IT security companies.

The Europol's Cybercrime Centre

The Europol's Cybercrime Centre (EC3) was set up in 2013 as integral part of Europol and has become a focal point in combatting and preventing cross-border cybercrime by:

- serving as the central hub for criminal information and intelligence;
- supporting Member States' operations and investigations by means of operational analysis, coordination and expertise;
- providing strategic analysis products;
- reaching out to cybercrime related law enforcement services, private sector, academia and other non-law enforcement partners (such as internet security companies, the financial sector, computer emergency response teams) to enhance cooperation amongst them;
- supporting training and capacity building in the Member States;
- providing highly specialised technical and digital forensic support capabilities to investigations and operations;
- representing the EU law enforcement community in areas of common interest (R&D requirements, internet governance, policy development).

4. EU FUNDING

Research and Innovation

During the 2007-2013 period, the EU invested **€334 million** in cybersecurity and online privacy projects. Topics such as trustworthy network and service infrastructures, cryptology and advanced biometrics were addressed under the 7th Framework Programme (FP7) and the Competitiveness and Innovation Programme (CIP). During the same period, the Security Research theme of FP7 invested **€50 million** in cybercrime projects addressing topics like the economy of cybercrime, risk analysis for infrastructure protection, money laundering and dedicated road mapping actions.

For the period 2014-2016, the EU has so far invested **€160 million** under the Horizon 2020 Research and Innovation Framework Programme (H2020) in cybersecurity research and innovation projects. The EU will also invest up to **€450 million** of H2020 funding to pursue cybersecurity research and innovation under the contractual public-private partnership on cybersecurity for the period 2017-2020.

Cybersecurity and privacy are part of two streams of the **Horizon 2020 programme**:

- Under the Societal Challenge **"Secure societies – Protecting freedom and security of Europe and its citizens"**.

  The **Digital Security** sstrand focuses on increasing the security of current applications, services and infrastructures by integrating state-of-the-art security solutions or processes, supporting the creation of lead markets and market incentives in Europe. Security is also a so-called "digital focus area" under other challenges (privacy and security in ehealth; energy; transport; innovative security solutions for public administrations). The aim is to ensure digital security integration in the application domains.

  The **Fighting Crime and Terrorism** strand focuses on increasing the knowledge of the cybercrime phenomenon - its specificities, its economy (including its unlawful markets and its use of virtual currencies) and the means for law enforcement authorities to fight it more efficiently and to prosecute offenders with more solid evidence from specialised forensic activities.

- Under **Leadership in enabling and industrial technologies** Projects on dedicated technology- driven digital security building blocks are funded (such as the 2014 calls on Cryptography and Security- by-Design). Security is also integrated as a functional requirement in specific technologies, such as the Internet of Things, 5G, Cloud, etc.

Infrastructures

For the 2014-2020 period, the European Structural and Investment (ESI) Funds foresee a contribution of up to **€400 million** for investments in trust and cybersecurity. The ESI funds can finance security and data protection investments to enhance interoperability and interconnection of digital infrastructures, electronic identification, privacy and trust services.

Cybersecurity is one of the areas supported under the Digital Service Infrastructures (DSIs) stream within the Connecting Europe Facility (CEF). The funded projects deploy trans-European digital services based on solutions such as e-identification and interoperable health services. One of the aims is to achieve cross-border cooperation in cybersecurity, enhancing the security and thus the trust in cross-border electronic communication, contributing to the creation of the Digital Single Market. In 2014-2016, the EU invested about €20 million in such projects; an additional investment of €12 million is earmarked for a call for proposals to open in May 2017.

Projects against cybercrime

The Commission supports the fight against cybercrime by financing Europol's Cybercrime Centre EC3 (staff and operational costs) and by funding cybercrime projects such as:

- the **Prevention and Fight against Crime** Programme (ISEC 2007-2013) which has contributed around €15 million to the fight against cybercrime since 2007.
- the Internal Security Fund (ISF) as the successor to ISEC for the period 2014-2020, with a total budget slightly over €1 billion available for funding actions under the ISF Police instrument, including the fight against cybercrime. Concrete actions to be funded through this instrument can include a wide range of initiatives, such as setting up and running IT systems, acquisition of operational equipment, promoting and developing training schemes and ensuring administrative and operational coordination and cooperation.

Capacity Building in third countries

Recognising the strong link between increased cyber resilience and sustainable development, the Commission has launched capacity building engagements in third countries. The objectives are to increase third countries' technical capabilities, preparedness, and establish effective legal frameworks to address cybercrime and cybersecurity problems; and at the same time enhance their capacity for effective international cooperation in these areas. The Commission has partnered with the Council of Europe and EU Member States for the implementation of these actions.

At a global and trans-regional level these initiatives are financed by the **Instrument contributing to Stability and Peace** (IcSP) where cybersecurity and combatting cybercrime have been identified as areas of priority since 2013 with an allocation of **€4.5 million** for 2013, and an indicative allocation of **€21.5 million** over the period 2014-2017.

In specific regions, the Commission has also used other instruments, including the **European Neighbourhood Instrument** (ENI), to help countries of the Eastern Partnership (Armenia, Azerbaijan, Belarus, Georgia, Moldova, Ukraine) to define strategic priorities related to the fight against cybercrime. The **Instrument of Pre-accession** (IPA) finances a new action of **€5 million** to help countries in South-Eastern Europe and Turkey to cooperate on cybercrime. The roll-out of more actions in these areas is foreseen in the next years, also through other financing instruments.

5. INTERNATIONAL ACTIVITIES

The European External Action Service (EEAS) and the Commission ensure, together with the Member States, coordinated international action in the field of cybersecurity. In doing so, the EEAS seeks to uphold EU core values and promote a peaceful, open and transparent use of cyber technologies. The EEAS, the Commission and the Member States engage in policy dialogue with international partners and with international organisations such as the **Council of Europe**, the **Organisation for Economic Co-operation and Development** (OECD), the **Organization for Security and Co-operation in Europe** (OSCE), the **North Atlantic Treaty Organization** (NATO) and the **United Nations** (UN).

The EEAS and the Commission, in close cooperation with the Member States, also establish links and dialogues on international cyber policy and security of information and communication technologies with key strategic partners such as **Brazil**, **China**, **India**, **Japan**, the **Republic of Korea** and the **United States**.

The Commission also supports capacity building in third countries (cf. above).