European
Commission

STATE OF THE UNION 2017

CYBERSECURITY

> *"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. This is why, today, the Commission is proposing new tools, including a European Cybersecurity Agency, to help defend us against such attacks."*
>
> European Commission President Jean-Claude Juncker, State of the Union Address, 13 September 2017

Resilience, Deterrence and Defence: Building strong cybersecurity in Europe

The European Commission and the High Representative have proposed a wide range of concrete measures that will further strengthen the EU's cybersecurity structures and capabilities with more cooperation between the Member States and the different EU structures concerned. These measures will ensure that the EU is better prepared to face the ever-increasing cybersecurity challenges.

European citizens and businesses rely on digital services and technologies:

Europeans believe that digital technologies have a positive[1] impact on:

75%	64%	67%
our economy	our society	our quality of life

86% of Europeans believe that the risk of becoming a victim of cybercrime is increasing.[2]

Sectors like **transport**, **energy**, **health** and **finance** have become increasingly dependent on network and information systems to run their core businesses.

The **Internet of Things (IoT)** is already a reality. There will be **tens of billions** of connected digital devices in the EU by 2020.[3]

Cyber incidents and attacks are on the rise:

+4,000 ransomware attacks per day in 2016.

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

+38% Security incidents across all industries rose by **38%** in 2015 – the biggest increase in the past 12 years.

80% of European companies experienced at least one cybersecurity incident last year.[4]

+150 countries and **+230,000** systems across sectors and countries were affected with a substantial impact on essential services connected to the internet, including **hospitals and ambulance services.**

The scale of the problem makes it necessary to act at the European level. Recent figures show that digital threats are evolving fast: ransomware attacks have increased by 300% since 2015. According to several studies, the economic impact of cybercrime rose fivefold from 2013 to 2017, and could further rise by a factor of four by 2019.[5] Evidence suggests that people from around the world identify cyber-attacks from other countries among the leading threats to national security.

Furthermore, in the aftermath of the “Wannacry” and “(Non)Petya attacks”, a recent report has estimated that a serious cyber-attack could cost the global economy more than €100 billion.

Awareness and knowledge

Despite the growing threat, awareness and knowledge of cybersecurity issues is still insufficient.

69% of companies have no or basic understanding of their exposure to cyber risks

60% of companies have never estimated the potential financial losses from a major cyber-attack[6]

51% of European citizens feel not at all or not well informed about cyber threats[7]

EU RESILIENCE TO CYBER-ATTACKS

The EU needs more robust and effective structures to ensure strong cyber resilience, promote cybersecurity and to respond to cyber-attacks aimed at the Member States and at the EU’s own institutions, agencies and bodies. It also needs strong cybersecurity for its Single Market, major advances in the EU’s technological capability and a broader understanding of everybody’s role in countering cyber threats. In response, the Joint Communication suggests new initiatives to further improve EU cyber resilience and response in three key areas:

- **Building EU resilience** to cyber-attacks and stepping up the EU’s cybersecurity capacity
- Creating an **effective criminal law response**
- Strengthening global stability through **international cooperation**

The Commission and the High Representative are therefore proposing to reinforce the EU’s resilience, deterrence and response to cyber-attacks by:

- Establishing a stronger **European Union Cybersecurity Agency** built on the Agency for Network and Information Security (ENISA), to assist Member States in dealing with cyber-attacks.
- Creating an **EU-wide cybersecurity certification scheme** that will increase the cybersecurity of products and services in the digital world.
- A **Blueprint for how to respond** quickly, operationally and in unison when a large scale cyber-attack strikes.
- A **network** of competence centres in the Member States and a **European Cybersecurity Research and Competence Centre** that will help develop and roll out the tools and technology needed to keep up with an ever-changing threat and make sure our defence is as strong as possible.
- A new **Directive on the combatting of fraud and counterfeiting of non-cash means of payment** to provide for a more efficient criminal law response to cyber crime.
- A Framework for a **Joint EU Diplomatic Response to Malicious Cyber Activities** and measures to **strengthen international cooperation** on cybersecurity, including deepening of the cooperation between the EU and NATO.
- The EU aims at driving **high-end skills development** for civilian and military professionals through providing solutions for national efforts and the set-up of a **cyber defence training and education platform**.

[1] *Attitudes towards the impact of digitisation and automation on daily life*, Eurobarometer, 2017.

[2] Eurobarometer on Cybersecurity (EBS 464).

[3] *Definition of a Research and Innovation Policy Leveraging Cloud Computing and IoT Combination*, IDC and TXT, study carried out for the European Commission, 2014.

[4] PWC, Global State of Information Security Survey, 2016 and http://news.sap.com/pwc-study-biggest-increase-in-cyberattacks-in-over-10-years/.

[5] *How to protect your networks from ransomware*, CCIPS, 2016 https://www.justice.gov/criminal-ccips/file/872771/download.

[6] *Continental European Cyber Risk Survey* 2016 Report.