European Commission

#DSM

Digital Single Market

Resilience, Deterrence and Defence: Building strong cybersecurity in Europe

To equip Europe with the right tools to deal with cyber-attacks, the Commission proposed **on 13 September 2017** a wide-ranging set of measures to build strong cybersecurity in the EU.

Ransomware attacks have **increased by 300%** since 2015.

x5

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.

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**.

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.

+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.**

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

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

European citizens and businesses rely on digital services and technologies:

Europeans believe that digital technologies have a positive impact on:

75% our economy

64% our society

67% our quality of life

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

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** is already a reality. There will be **6 billion** devices connected in the EU by 2020.

EU RESILIENCE TO CYBER-ATTACKS

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

A European Union Cybersecurity Agency to **assist Member States in dealing with cyber-attacks**.

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

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 to **help develop and roll out the tools and technology needed to keep up with an ever-changing threat**.

A new Directive to **combat fraud and counterfeiting of non-cash means of payment**.

Measures to **strengthen international cooperation on cybersecurity, including deepening of the cooperation between the EU and NATO**.

STEPPING UP EFFORTS TO TACKLE ILLEGAL CONTENT ONLINE

With the surge of illegal content online, including online terrorist propaganda, xenophobic and racist speech inciting violence, and terrorism, the social responsibility of online platforms is growing. The Commission has put forward **guidance on how online platforms should step up prevention, detection and removal of illegal content**.