

Sehr geehrte Damen und Herren,

EK hat heute ein Packet iZm Cybersicherheit vorgestellt, das einen Aktionsplan (EK-Mitteilung) sowie eine Cybersicherheitsvereinbarung mit der Branche beinhaltet. Für weitere Informationen siehe Links und Presseausendung unten.

Beste Grüße aus Brüssel  
Ludmila Georgieva

- PA: [http://europa.eu/rapid/press-release\\_IP-16-2321\\_en.htm](http://europa.eu/rapid/press-release_IP-16-2321_en.htm)
- Communication: Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry :<https://ec.europa.eu/digital-single-market/en/news/communication-strengthening-europes-cyber-resilience-system-and-fostering-competitive-and>
- Commission Decision to establish a contractual public private partnership on cybersecurity (cPPP): <https://ec.europa.eu/digital-single-market/en/news/commission-decision-establish-contractual-public-private-partnership-cybersecurity-cppp>
- Commission Staff working document on cPPP and accompanying measures: <https://ec.europa.eu/digital-single-market/en/news/commission-staff-working-document-cppp-and-accompanying-measures>
- Commission Staff Working Document on assessment of cybersecurity in EU's 7th Framework Programme for Research and Technological Development and Competitiveness and Innovation Framework Programme (CIP): <https://ec.europa.eu/digital-single-market/en/news/commission-staff-working-document-assessment-cybersecurity-eus-7th-framework-programme-research>
- Summary report on the public consultation on the contractual PPP on cybersecurity and Staff Working Document <https://ec.europa.eu/digital-single-market/en/news/summary-report-public-consultation-contractual-ppp-cybersecurity-and-staff-working-document>

## **Commission signs agreement with industry on cybersecurity and steps up efforts to tackle cyber-threats**

Brussels, 5 July 2016

The Commission today launches a new public-private partnership on cybersecurity that is expected to trigger €1.8 billion of investment by 2020. This is part of a series of new initiatives to better equip Europe against cyber-attacks and to strengthen the competitiveness of its cybersecurity sector.

According to a [recent survey](#), at least 80% of European companies have experienced at least one cybersecurity incident over the last year and the number of security incidents across all industries worldwide rose by 38% in 2015. This damages European companies, whether they are big or small, and threatens to undermine trust in the digital economy. As part of its [Digital Single Market](#)

[strategy](#) the Commission wants to reinforce cooperation across borders, and between all actors and sectors active in cybersecurity, and to help develop innovative and secure technologies, products and services throughout the EU.

Andrus **Ansip**, Vice-President for the Digital Single Market, said: *"Without trust and security, there can be no Digital Single Market. Europe has to be ready to tackle cyber-threats that are increasingly sophisticated and do not recognise borders. Today, we are proposing concrete measures to strengthen Europe's resilience against such attacks and secure the capacity needed for building and expanding our digital economy."*

Günther H. **Oettinger**, Commissioner for the Digital Economy and Society, said: *"Europe needs high quality, affordable and interoperable cybersecurity products and services. There is a major opportunity for our cybersecurity industry to compete in a fast-growing global market. We call on Member States and all cybersecurity bodies to strengthen cooperation and pool their knowledge, information and expertise to increase Europe's cyber resilience. The milestone partnership on cybersecurity signed today with the industry is a major step ."*

Today's action plan includes the launch of the first European **public private partnership on cybersecurity**. The EU will invest €450 million in this partnership, under its research and innovation programme [Horizon 2020](#). Cybersecurity market players, represented by the European Cyber Security Organisation (ECSO), are expected to invest three times more. This partnership will also include members from national, regional and local public administrations, research centres and academia. The aim of the partnership is to foster cooperation at early stages of the research and innovation process and to build cybersecurity solutions for various sectors, such as energy, health, transport and finance. Commissioner Oettinger today signs the partnership with the ECSO in Strasbourg ([photos](#) and [videos](#) to be available at around 12.00 CET).

The Commission also sets out different measures to tackle the fragmentation of the EU cybersecurity market. Currently an ICT company might need to undergo different certification processes to sell its products and services in several Member States. The Commission will therefore look into a possible European **certification framework** for ICT security products.

A myriad of innovative European SMEs have emerged in niche markets (e.g. cryptography) and in well-established markets with new business models (e.g. antivirus software), but they are often unable to scale up their operations. The Commission wants to **ease access to finance for smaller businesses** working in the field of cybersecurity and will explore different options under the [EU investment plan](#).

The **Network and Information Security Directive**, which is expected to be adopted by the European Parliament tomorrow, already creates a network of Computer Security Incident Response Teams across the EU in order to rapidly react to cyber threats and incidents. It also establishes a 'Cooperation Group' between Member States, to support and facilitate strategic cooperation as well as the exchange of information, and to develop trust and confidence. The Commission today calls on Member States to make the most of these new mechanisms and to strengthen coordination when and where possible. The Commission will propose how to **enhance cross-border cooperation in case of a major cyber-incident**. Given the speed with which the cybersecurity landscape is evolving, the Commission will also bring forward its evaluation of the **European Union Agency for Network and Information Security (ENISA)**. This evaluation

will assess whether ENISA's mandate and capabilities remain adequate to achieve its mission of supporting EU Member States in boosting their own cyber resilience. The Commission also examines how to strengthen and streamline cybersecurity cooperation across different sectors of the economy, including in cybersecurity training and education.

## **Background**

Today's action plan finds its main roots in the 2015 [Digital Single Market strategy](#), the 2013 [EU Cybersecurity strategy](#) and the forthcoming [Network and Information Security \(NIS\) Directive](#). It builds on the recent Communications on [Delivering the European Agenda on Security](#) and [Countering Hybrid Threats](#).

---

Dr. Ludmila GEORGIEVA

Attaché

Audiovisuelles, Cyber Issues, Datenschutz, Digitale Agenda, E-Government,  
eLaw, Informationssicherheit, Vergabewesen, Statistik

STÄNDIGE VERTRETUNG ÖSTERREICHS BEI DER EU

Abt. Bundeskanzleramt

Avenue de Cortenbergh 30, B-1040 Brüssel

Mob: +32 (0) 478 330 176

Tel: + 32 (0)2 2345-226

Fax: + 32 (0)2 2356-226

E-Mail: [ludmila.georgieva@bmeia.gv.at](mailto:ludmila.georgieva@bmeia.gv.at)