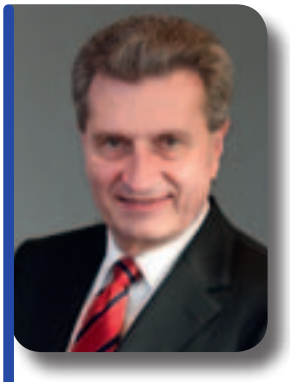
Partnerships to step up cybersecurity in Europe



Günther H. OETTINGER
European Commissioner for Digital Economy and Society

In today's digitalised world, cybersecurity incidents – intentional or accidental – can have a huge negative impact on our ultra-connected societies. Whatever their origin – criminal, terrorist or state-sponsored attacks as well as natural disasters and unintentional mistakes – they can disrupt the complex finance, health, energy and transport systems which keep our world turning, and encroach our education, cultural, sporting, social and family lives which rely more and more on digital technologies.

Some incidents hit the headlines as was the case in April 2015 when the French broadcaster TV5 Monde was the victim of an unacceptable attack against the freedom of press and expression. Or in early December 2015 when it became public that hackers had obtained the names, passwords, homes addresses and birthdays of 5 million adults and 200,000 children from VTech, a Chinese toy manufacturer whose toy tablets, phones, and baby monitors may be in your homes or were waiting under the Christmas tree. Threat is always present, and cybersecurity needs constant attention. Cybercrime is global by its very nature, and therefore I strongly encourage European Union Member States to cooperate on cybersecurity issues.

People will not use what they do not trust. Greater confidence and security are absolutely fundamental for a more widespread use of digital technologies, including e-payments, cloud computing and machine-to-machine communications which are at the heart of our digital economy and society. However, currently only 22% of Europeans have full trust in search engines, social networking sites and e-mail services and only 38% of Europeans feel confident about online purchases from another EU country.

That is why cybersecurity is one of my top political priorities. We laid the foundations in 2013 with the adoption of the EU Cybersecurity Strategy, and the Commission has since stepped up its efforts to better protect Europeans online. We outlined our plans in the Digital Single Market strategy that I presented in May 2015 with my colleague Andrus Ansip, Vice-president of the Commission in charge of the Digital Single Market. The fight against cybercrime is also at the core of the European Agenda on Security presented in April last year.

This challenge is real and major improvements are needed, but it is well worth the effort. By completing the Digital Single Market, the EU could boost its economy by €415 billion per year and create hundreds of thousands of new jobs.

We achieved a major step with the very recent political agreement (7 December 2015) between the European Parliament and Member States on a Commission's proposal for a Directive aiming at reaching a high common level of network and information security (NIS) in the EU.

In practice, the new directive acts on three levels. Firstly, it aims at improving cybersecurity

in EU countries. Each Member State will be obliged to have a national strategy, to identify who will enforce this and to set up a "Computer Security Incident Response Team" to handle incidents and risks. Secondly, and because the internet and cyber-attacks don't stop at national borders, the rules will help Member States and their response teams to cooperate on cybersecurity issues and to share information about risks. Finally, the operators of essential services – power companies, financial institutions, transport providers, healthcare and digital infrastructure, etc. – and others such as search engines and cloud computing services will have to take appropriate security measures and inform the authorities when they have a cyber- incident.

Everybody will gain from those new rules: consumers will have more confidence in the technologies and services and systems they rely on day-to-day, while governments and businesses can be confident that digital networks and critical infrastructure like the electricity, gas and transport sectors can securely provide their services at home and across borders.

To act, the EU has its own tools. Since 2004, the European Union Agency for Network and Information Security (ENISA) has helped the Commission, the Member States and the business community to address, respond and especially to prevent network and security problems. In particular ENISA helps collect and analyse data on security incidents in Europe and emerging risks. It also promotes risk assessment and risk management methods to enhance capability to deal with information security threats. Our permanent Computer Emergency Response Team (CERT-EU) is also great instrument to protect the EU institutions, agencies and bodies from cyberattacks.

Given the fact that ENISA's current mandate expires in 2020, the Commission will conduct review of its activities by 2018. Then, it will be time to re-examine the role attributed to the agency in the context of the NIS Directive implementation, amongst others.

Last, but not least, cybersecurity presents a huge economic and industrial opportunity for European companies. We must seize this chance so that European industry can play a key role in the global cybersecurity market, expected to be worth around $100 billion by 2018. As part of our Digital Single Market strategy, during the course of 2016, we will establish a contractual public-private partnership on cybersecurity.

To set the ball rolling a few weeks ago, the Commission launched a public consultation to help prepare this and other possible measures to strengthen EU cybersecurity capacities. This partnership will involve the whole EU cybersecurity community, from innovative SMEs and national security agencies to producers of components and equipment, critical infrastructure operators and research institutes. It will leverage EU, national, regional and private efforts and resources – including research and innovation funds – to increase investments in cybersecurity. It will be supported by EU funds coming from the Horizon 2020 Framework Programme. The Commission has earmarked up to €500 million alone for research and innovation in this area during the period 2014-2020

This initiative should be instrumental in structuring research and innovation for digital security in Europe and will boost the industry to ensure the sustained supply of innovative cybersecurity products and services needed to increase online security.

All in all, I want European citizens and businesses to have access to the latest digital security technology developments, secure infrastructures and best practices, which are stworthy and based on European rules and values including the right to privacy.