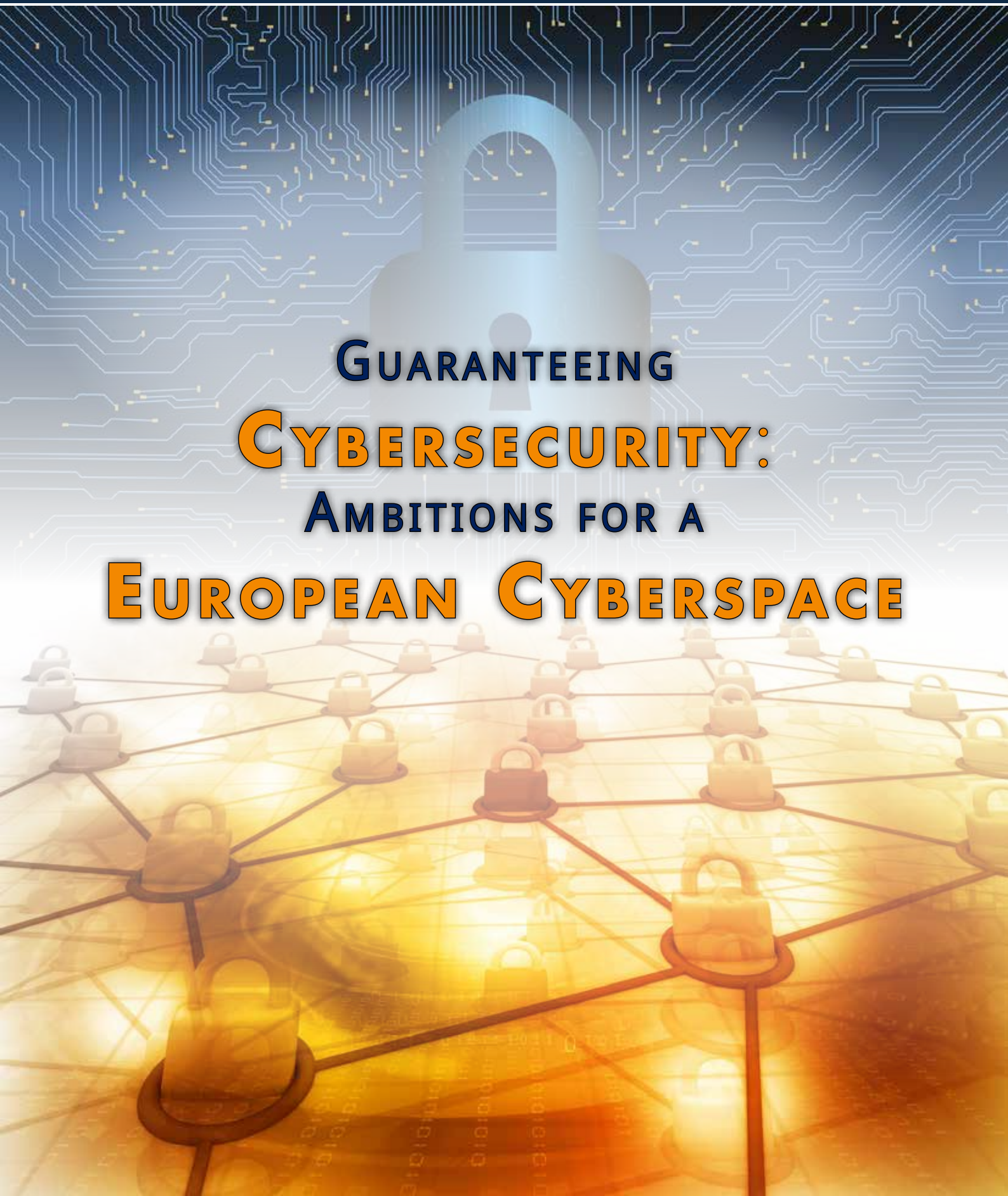
THE EUROPEAN FILES

March 2019 - n°57



Guaranteeing Cybersecurity: Ambitions for a European Cyberspace

Advanced® Track&Trace

LINKING CERTIFIED DIGITAL WORLD WITH PHYSICAL SIDE OF I.O.T.

Based on Visible Digital Seal and Seal Vector® : off-line integrity check in eIDAS/RGPD environment, physical authentication of the related item and access to the original electronic document or real-time traceability.

Seal Vector® : ATT tracer-authenticator technology

Contact : info@att-fr.com

WWW.ATT-FR.COM

EDITORIAL

Guaranteeing Cybersecurity: Ambitions for a European Cyberspace

Today, cybersecurity ranks at the top of the Commission's and Parliament's political priorities and has become a major concern for citizens, ranging from the violation of our right to privacy to the threat of terrorist attacks.

In this context, the EU must create a safer European cyberspace for all.

President Macron's 2018 Paris Peace Call for Trust & Security in Cyberspace is in line with this approach and promotes a collaborative action to better secure our political and economic environment.

With the growth of e-commerce, the development of artificial intelligence and the increasing number of connected devices it is essential to foster a culture of safety in our increasingly interconnected societies.

In September 2018, the European Commission tabled a proposal for a Regulation establishing a European Cybersecurity, Industrial, Technology and Research Competence Centre, which aims at creating an eco-system of expertise by promoting the development and deployment of cybersecurity technologies.

The European Commission has also just adopted a Regulation, called "Cybersecurity Law", to strengthen the (budgetary) capacities and competences of ENISA, and will be in charge of certifying cybersecurity in the field of ICT in order to avoid market fragmentation. It will also be responsible for coordinating the exchange of good practices within Member States and raising awareness about cybersecurity among citizens and businesses.

The creation and implementation of a binding and independent European Cybersecurity Certification Framework for products and services operating in critical sectors of our economy (transport, energy, health, banking, etc.) is paramount in order to build trust and security.

Moreover, the EU is keen to invest €1.8 billion in cybersecurity through public-private partnerships to boost competitiveness and innovation capacities in order to ensure a sustainable supply in the cybersecurity sector in Europe and strengthen our independence.

This issue of the European Files highlights the digital revolution our societies are currently experiencing, which is characterised by the speed with which we are confronted with innovation and new threats. Protecting the data of individuals and businesses by ensuring safer products and services is essential in order to build trust, and thus foster an open, interoperable, secure and reliable cyberspace.

Editor-in-Chief
LAURENT ULMANN

Management: The European Files / Les Dossiers Européens - 19 rue Lincoln, 1180 Brussels
www.europeanfiles.eu - ISSN 1636-6085 - **email:** ulmann@europeanfiles.eu
Publication Director and Editor-in-Chief: Laurent ULMANN
Layout & printing: VAN RUYS PRINTING

TABLE OF CONTENTS

Guaranteeing cybersecurity in europe: ambitions for a european cyberspace

Cyberspace Agenda: Reforms for a European framework on Cybersecurity

Guaranteeing Cybersecurity: Ambitions for a European Cyberspace

A revamped ENISA - the EU's cybersecurity agency

Mariya GABRIEL

Commissioner for Digital Economy and Society, European Commission

Europe is under attack. Not physically, of course, but virtually. Every day cyber threats are detected and cyber-attacks thwarted. Keeping European citizens safe in the connected world is a priority for the European Commission, and ENISA, the EU's cybersecurity agency, has an increasingly important and central role in this endeavour.

The European Union Agency for Network and Information Security, or ENISA for short, was originally set up in 2004 to help ensure a high level of network and information security within the EU. Based in Greece, ENISA supports the European institutions, the Member States and the business community in addressing, responding to and especially in preventing network and information security problems. Originally created as a relatively small agency with a limited budget and mandate, new EU-level cybersecurity legislation is beefing up ENISA's role and mandate significantly.

Already the 2016 Network and Information Systems (NIS) Directive gave additional tasks to the agency. That Directive created for the first time a network of the Member States' Computer Security Incident Response Teams (CSIRTs), in order to promote swift and effective operational cooperation on specific cybersecurity incidents and share information about potential risks. ENISA acts as the secretariat to the CSIRT network. Similarly, ENISA has a less proactive but equally important role to play as a member of the NIS Cooperation Group, also created by the NIS Directive and providing advice and expertise and facilitating information sharing among Member States.

The need for a truly pan-European cybersecurity agency is clear. Exposure to various cyber threats in the EU remains high. According to ENISA's own 2018 Cyber Threat Landscape report, which focuses on the 15 top cyber-threats from malware to denials of service, the number of attacks has remained relatively stable over the last few years (although the exact figures are hard to calculate because the baseline is continuously shifting as ever more attacks are automatically detected and defended against). What has changed dramatically though is the level of sophistication of many of the attacks, meaning that our responses have to become increasingly sophisticated as well.

Hence, as the number of cyber threats has risen, there was a clear political wish to enhance ENISA's remit, along with its budget and its mandate. In the Cybersecurity Act, a regulation proposed in 2017, which will come into force in spring 2019, the European Commission, put forward a number of new initiatives to further improve EU cyber resilience, deterrence and defence, including significantly expanding and strengthening the mandate and role of ENISA. This includes a permanent mandate for the agency (previously, ENISA's mandate had to be renewed every seven years) and a much greater operational budget (more than doubling from the current €11m per year), as well as handing ENISA a clear operational - and not only advisory - role in European cybersecurity.

Moreover, the Cybersecurity Act also entails the creation of a European Cybersecurity Certification Framework in which ENISA will play a key role. For businesses and consumers to be certain that their online information is safe, they need to use products, services and processes that they trust, but the lack of a single EU-wide scheme to certify this trustworthiness is a major problem. Today, products sometimes have to be certified in several different countries following different processes, which limits cross-border trade within the EU and implies big cost for the consumers. The new framework sets out the rules, requirements, standards and procedures with which EU-wide certification schemes will have to comply. It is for ENISA to organise the development of such (for the time being voluntary but this may also change with time) schemes for a wide variety of ICT products and services, from smart cards to cloud computing.

At the same time, the Cybersecurity Act maintains ENISA's advisory role; In addition to expanding on its existing remit, the agency will for example assist EU and national authorities on priority setting in research and development. It will also work closely with the proposed new European Cybersecurity Industrial, Technology and Research Competence Centre. The latter's task would be to help the EU retain and develop the cybersecurity capacities that underpin the continued development of the EU's Digital Single Market.

The challenge to keep European citizens and businesses safe and secure in today's connected world will continue to require our attention and investments for many years to come. Europe has kicked into a higher gear already, boosting its cybersecurity capabilities through legislation such as the NIS Directive or the Cybersecurity Act, and carrying out joint manoeuvres through increasing coordination and cooperation between national and EU players. The new certification framework will bolster Europe's civil defence mechanisms, reassuring users that they can continue to operate safely. Moreover, the new European Cybersecurity Competence Centre will ensure that the next generations of secure products and services but also of the engineers and programmers to create them will be available. ENISA is there with a new permanent mandate to support the EU and EU Member States in sharing vital cybersecurity information, to assist in coordinating the key players and to give the right advice. We may never be entirely free from the threat of cyber-attacks but our new comprehensive framework should provide the additional and necessary guarantees to live and work in a safer environment.

Creating a political standard for Cybersecurity in Europe

Elizabeth BIENKOWSKA

Commissioner for Internal Market, Industry, Entrepreneurship and SMEs, European Commission

Our lives are increasingly reliant on connected devices, digital networks and infrastructure. From smart phones to smart banking, we have grown so accustomed to our digital devices that we could not imagine living without them. They bring convenience, availability and opportunities, but they also come with challenges. One of these challenges is cybersecurity.

For example, the majority of EU companies have experienced at least one cybersecurity incident. The economic impact of cyber-crime is rising. They are estimated to cost the global economy €400 billion every year. That is why we have been working hard to strengthen EU cybersecurity rules – not only to tackle increasing cybersecurity threats but also to help people and businesses take full advantage of the opportunities of the digital age.

The key part of our work is our 2017 proposal for a reform of cyber security in the EU. We proposed a number of measures, for example to build a stronger EU cybersecurity agency, to introduce an EU-wide cybersecurity certification scheme and we called for implementation of the Network and Information Security Directive. The European Parliament and the Council already reached an agreement on our proposals in December 2018.

This is good news for citizens and businesses. Once in force, the EU-wide cybersecurity certification scheme for information and communications technology (ICT) products, services and processes will help reduce market fragmentation and reinforce trust in new connected products and services. As a result, it will make it easier for consumers to make more informed choices and for businesses to trade their products across Europe.

Moreover, we have been working on cybersecurity issues linked to the EU product safety legislation, ICT standardisation and cyber defence.

Cybersecurity and product safety legislation

Product safety and cyber-security are closely linked. That is why we are looking into our product safety legislation, in particular the Machinery Directive. This is the key EU legislation for robots.

Emerging digital technologies, such as artificial intelligence (AI) and Internet of Things (IoT), are increasingly being integrated into machinery. This can have a significant impact on the safety of these products and on our security. To make sure the Machinery Directive responds to these changes, we are currently planning to revise it. And we will also analyse if such a revision should include cybersecurity requirements.

Another important aspect of cybersecurity is privacy. The number of connected devices is only expected to grow. In 2020, there should be tens of billions of connected digital devices in the EU, ranging from smart fridges to smart kettles. We need to make sure that all these smart machines respect our privacy and do not pose a threat to our security.

Under the Radio Equipment Directive, the Commission can adopt measures to require that all radio equipment is fitted with features protecting our privacy and fighting against fraud. We are currently analysing whether such legal requirements would improve the security of connected products.

Cybersecurity and ICT standardisation

The connected devices we use every day should communicate safely and seamlessly, regardless of their manufacturer or country of origin. For this they need a common language: ICT standards.

ICT standards are key for the digitisation of European industry. And cybersecurity is also one of the five priority areas we are focusing on when it comes to ICT standardisation. By focusing on cybersecurity, we want to ensure that safety, security and privacy considerations are built-in to new standards from the outset.

The European standardisation organisations (CEN, CENELEC, and ETSI) are working on standards with specific focus on cybersecurity, in particular developing standards for data protection, information protection and security techniques.

In addition, the Network and Information Security Directive provides support for the development and uptake of ICT standards in this area.

Cyber defence

Last but not least, we are focusing on cyber defence. Cyber operations have become a new war domain, along with land, sea, air and space operations. They can pose a serious threat to our security. Cooperation in cyber defence is therefore key to protect European citizens against those threats.

In June 2018, we proposed a €13 billion European Defence Fund (EDF) to encourage cooperation among Member States in producing state-of-the-art defence technology and equipment. In February 2019, the European Parliament and the Council already reached a partial political agreement on this proposal.

The EDF will fund collaborative projects involving at least three eligible entities from at least three Member States or associated countries. Cyber defence is definitely one of the areas where the European Defence Fund could make a difference in helping Member States develop the technologies, software and equipment that they need to defend themselves.

When it comes to cybersecurity challenges, no country can face them alone. We need to continue working together so that we can tackle these challenges effectively. If we get it right, we can not only protect our citizens but also open new and exciting opportunities for all.

Strengthening Cybersecurity Capacity: A European Obligation

Horst SEEHOFER

Federal Ministry of the Interior, Building and Community, Germany

Our modern, high-tech society depends on a whole series of delicate systems: sensitive information and communications systems, high-quality infrastructure, and secure energy provision. These factors are the backbone of technological progress and economic development. In this context, the spread of digital technology increasingly influences policy and business decisions, as well as the day-to-day lives of our citizens.

The digital revolution is characterized by the breakneck speed at which we are confronted with innovation. As a society, we have less and less time to adjust to and apply technological advances. The time-to-market cycle of new apps and products is constantly shrinking, while new ventures based on innovative digital technologies crowd established enterprises out of the market.

As IT systems become more complex, all areas of the information society are increasingly interconnected. This brings with it an increased risk of disruption and attacks, from within our country and from abroad. Threats in cyberspace are hugely dynamic, with cyberattacks growing more intelligent and professional by the day. Methods of attack are evolving as rapidly as IT systems are advancing, while globalization and the interconnection of technology mean that bugs, regulatory loopholes or negligence can often have huge knock-on effects.

The greater a role digital technology plays in the actions of government, in business, and in everyday life, the more pressing the need to involve all stakeholders at national, European and international level in a joint approach to tackling the resultant cybersecurity challenges.

In the first instance, cybersecurity is a domestic task. At present, Germany is well equipped by international standards, as the report by the Federal Office for Information Security shows. However: cybersecurity must evolve constantly. The increasing reach of digital technology brings threats of an ever-changing nature and intensity.

And in an increasingly interconnected world, cybersecurity must extend beyond the national level. We must work systematically in Europe to achieve this, for example by developing joint minimum standards for the European market. Implementing the NIS Directive, passed in 2016, is therefore the top priority within the European Union. The Directive sets out measures aimed at achieving a high common level of security of network and information systems in the European Union.

To build on this, in September 2017 the European Commission put forward the Cybersecurity Package, a proposal for the new Cybersecurity Act. Preliminary political agreement was reached on the Act in late 2018. The Act will give the European Network and Information Security Agency (ENISA) a permanent mandate and allocate additional resources and capabilities to it. An EU-wide framework for basic voluntary cybersecurity certification for IT products, systems and processes will also be implemented in all sectors with the aim of creating the right incentives for secure products and system solutions. The Act is a solid basis on which we will be able to seek joint European answers to key questions on the topic of cybersecurity, both now and in the future.

In addition, in September 2018 the European Commission submitted a proposal for a regulation establishing a European Cybersecurity Industrial, Technology and Research Competence Centre. The aim of the Regulation, to stimulate the development and deployment of cybersecurity technologies, is a good one. Joint efforts at EU level are essential. It is in all of our interests for research and development on information technology and communication systems to take place within Europe. This will enable us to minimize our reliance on third countries.

We must be aware that we can only reap the full benefits of new digital technologies and the worldwide networks enabled by them if we integrate cybersecurity from the start. Security by design has to be a firm component of our strategies so that we can strengthen trust in new technologies. Because one thing is clear: If we want the digital revolution to be successful, cybersecurity is crucial.

Cybersecurity is a collective struggle

Mounir MAHJOUBI
French Minister for Digital

As I write these lines, we are under cyberattack. This is the future that we now face: digital technology has brought with it empowerment and progress, but also risk. We are increasingly vulnerable, and this in turn whets the appetite of pirates and hackers, who target the weak points in our economies and our democracies.

It is clear that this threat must be countered, but, as in the real world, the response is a complex one. Our republican values are vital for upholding our democratic freedoms; in the same way, cyber-defence is a key priority, and it is pointless to approach it in isolation.

Cybersecurity: a national priority

To ensure the safety of our fellow citizens, both French and European, as well as that of companies, cybersecurity has become one of France's strategic priorities, and it is my hope that we can remain at the forefront of the fight. Thanks to the work of the National Information System Security Agency (ANSSI) France has tightened our security standards. We alert citizens and companies to the cyber-threats they face, and provide a government website, cybermalveillance.gouv.fr, for victims to report cybercrimes. Concurrently, we are structuring our cybersecurity network to help ensure a successful digital transition and foster trust. The issue of national digital sovereignty also cannot be ignored. This is why France has decided to customise its use of cloud computing, and has created a hybrid cloud that features different levels of security depending on the importance and sensitivity of the data to be protected.

All of these forward-looking cyber-defence measures are in full complementary with the European ecosystem.

A trusted cyberspace is only possible on a European scale

Cyberattacks do not stop at national borders, and neither should the regulations and resources needed to build a secure digital space. To better protect themselves, the EU and its Member States must draw inspiration from and challenge each other.

Given the threat that the American CLOUD Act represents for our sovereignty, France supports a European initiative to negotiate an agreement between the EU and the US on cross-border access to electronic evidence, as well as the European Commission's proposed E-evidence Regulation. In a similar vein, the General Data Protection Regulation (GDPR) and the NIS Directive (Security of Network and Information Systems) have inspired and galvanised us to create a normative framework specifically designed to keep digital infrastructures and stakeholders secure. Lastly, we support European efforts to build a secure cyberspace via the Cybersecurity Act, which will introduce a permanent mandate for the EU's cybersecurity agency ENISA and a framework for European Cybersecurity Certificates. We also support the other provisions in the Commission's 2017 roadmap, including the establishment of a European Cybersecurity Industrial, Technology and Research Competence Centre and a Network of National Coordination Centres.

The convergence of national and European structures is the foundation of a genuine network of trust, which is inspiring at global level. But our public and institutional response is only the beginning.

Cybersecurity is a cultural issue

Although the power to punish cyber-criminals remains the purview of governments – France is in favour of banning hack-backs – private-sector stakeholders must proactively protect themselves against cybersecurity threats. This is the reasoning behind the Paris Call for trust and security in cyberspace, backed by 64 governments, 328 companies and 129 civil society organisations. Every day, I strive to foster dialogue and cooperation amongst governments, the private sector and civil society, because our security depends on a virtuous cycle of collaboration. Everyone, at every level, is concerned.

In the face of digital technology, we are, in the end, only human. No matter how sophisticated our technical structures and legislation are, the vast majority of breaches are the fault of human error. We rely on every digital action, each new behaviour we must adopt, such as having a unique password for each service, or setting up two-factor identification, which is critical to warding off cyberattacks. Cyber hygiene must be as universal as digital uses, and we must raise our level of cyber culture.

We have reached a turning-point. When we type on a keyboard or activate a touch screen, we all have an enormous responsibility to imagine an Internet in which we can collectively place our trust. The resilience of our digital society will be measured by our digital skills.

Guaranteeing Cybersecurity in Europe: Ambitions for a European Cyberspace

Boštjan POKLUKAR
Minister of Interior, Slovenia

In the age of digitalisation the internet is becoming increasingly what is called the internet of things. The European Commission estimates that by 2020 the number of devices connected to the internet will reach several tens of billions. Parallel to this is an increase in the number of cyber threats, which in the assessment of the European Commission grew fivefold in the years from 2013 to 2017, and up to 2019 another four times, with a trend of growth supposedly each year. There is no doubt that exposure to cyber threats is one of the most significant security risks in the modern world, and controlling this is extremely important both for ensuring national security and for the security of the European Union as a whole.

Europol estimates that cybercrime costs the European Union around EUR 265 billion annually, and in some EU countries cybercrime already represents around half of all crime. Poor digital hygiene, risky digital practices and inadequate protection would in the period of one year supposedly give rise to the disclosure of as much as two billion records of European Union citizens. Advanced countries are therefore already placing the digital space, in terms of importance, alongside the "classical" dimensions of space, i.e. land, air and water.

Despite measures adopted in recent years in the area of cybersecurity, the level of preparedness of EU Member States for cyber threats can still to a large extent be assessed as inadequate. The reasons for this can be divided into three categories:

1. Legal reasons, which limit Member States, and especially their police forces, and slow them down in obtaining data on cybercrime and threats. Such malevolent activities are indeed not just limited to the territory of an individual country or community of countries, so national police forces face difficulties especially when they need to obtain data from third countries, or where the perpetrators are non-state global actors (for instance global terrorist organisations or criminal associations). In order to achieve their aims, these actors make use principally of what is called the dark web, and the important things in effective investigation of crime arising from the dark web are adequate national legislation, which can make investigating such activities easier and more effective for the police, and international cooperation.

2. Insufficient financial resources allocated to the area of cyber security, in connection with the difficulties for state authorities to compete with commercial companies for adequately qualified human resources.

3. Strategic reasons, since what are called the western partners in the Euro-Atlantic integrations do not have a common strategy for responding to cyber attacks, where these are assessed as acts of war. It is hard to formulate a common strategy, especially since cyber attacks are very difficult to ascribe to a single organisation or country. Moreover, owing to the credibility risk and their diminished standing, countries are reluctant to share information about successful cyber attacks.

We should in no way stop at merely determining the legal frameworks for the fight against cyber threats, and we will need to take steps forward. Steps in the right direction are: increasing funding and human resources for cybersecurity, linking up with technology companies that are developing protection against cyber threats, and also tightening sanctions for the perpetrators of such acts.

We are all well aware that cyber threats actively impact the lives and security of individual people. For this reason it is all the more important for key actors to link together and cooperate in the area of cyber and information security (both in the international and national contexts) in seeking the best responses to the challenges of the modern digital world.

Cyberspace and the fight against terrorism: New challenges, new tools

Gilles DE KERCHOVE

European Counter-Terrorism Coordinator, European Council

The cyber dimension of the terrorist threat is evolving rapidly

Digital tools are already widely used by terrorist groups for strategic and tactical purposes. The digital space enhances their ability to inspire and recruit; to organise logistics and raise funds; and, of course, to prepare attacks (command and control of operatives, sharing attack methodology and designating targets).

Apart from basic 'jihackist' techniques, we are yet to see a shift into the world of terrorist groups actively using cyber as the primary vector for an attack. Hitherto, cyberspace has only played a supporting role, but the future may be different. Major future threats could lie in development of capacity to strike critical infrastructure through a cyber-attack. Terrorists may not be able to develop this capability alone, but it is possible that in the near term they could seek to procure it on the digital black market.

Given the shift to 'crime as a service' in the dark web, it feels highly probable that a terrorist group will seek to acquire the capacity to launch a cyberattack that will pose a threat to life or at least create widespread panic.

The accelerated digitisation and interconnection of the economy and the public sphere stimulate wealth creation and huge opportunities. They also have a darker flip side and provide new opportunities to terrorists. We must therefore harness the potential of new digital capacities in the security sphere to outpace our adversaries.

Five main challenges to tackle

Fighting online radicalisation. The rise of social media was a game changer in radicalisation. Da'esh outpaced us all and started a sea change in propaganda capability. To counter that, the EU created the Internet Referral Unit (IRU) within Europol and launched a partnership with the big companies. Working together to identify and remove content has achieved significant success and an advance in detection technology to cope with the problem. But there is more to do.

Primarily we need to act quicker and ensure that the successes of the big companies cascade down to the small companies. Swift adoption by the European Parliament of the Terrorist Content Online proposal making it possible to remove illicit content within one hour would be a decisive step forward. We also need to tackle the abuse of social media for terrorist finance purposes and uphold our own values in supporting alternative narrative online.

Improving access to digital information. Cross-border access to e-evidence is a key element of the fight against terrorism, but it faces legal and practical obstacles. Frankly, it is not fast or smooth enough. Adopting the legislative proposals regarding access to e-evidence would give authorities access to information held by all service providers operating in the EU. An agreement with the United States in this field is vital.

Encryption is a great advance in protecting individual data and must remain. But it is widely used by terrorists to retain anonymity. Here, the EU needs to strike a balance between protecting data and privacy and retaining access to critical, potentially lifesaving, information. There also concerns on the usage by Internet service providers of Carrier Grade Network Address Translation (CGN) technology, which allows a single IP address to be assigned to thousands of users. Whilst the EU can pride itself on leading in the protection of privacy, a balanced approach must be found to limit disproportionate effects on public safety or the development of artificial intelligence, for example.

Making more use of new technologies. Artificial intelligence and big data analytics have huge potential for the security sector. Such innovation can improve analysis, detect weak signals or identify suspects at the borders. Quantum computing cryptography will provide stronger capacities in decryption. European JHA agencies such as Europol, Frontex and Cepol must become centres of technological excellence to support Member States and pool resources. We can only succeed in this if we do it together.

EU regulation must find a way to prevent malicious use of cyberspace and to allow law enforcement to respond to ever more sophisticated threats. The strategic autonomy of Europe in this field is also critical in a dangerous world. Supporting European industry through developing cyber clusters gathering research, funding, business and academia is essential. A dedicated fund to support European start-ups in this field, in addition to stricter control of foreign investment and market position must be a priority for the new Commission.

Overcome the institutional and technological complexity

Cybersecurity requires the effective combination of a wider variety of services, with sometimes competing interests, in order to respond to advanced cyber threats which know no borders. Working as a network based on trust, exploring a mechanism to share vulnerabilities, creating truly joint analysis and providing united operational response capability would add significant value to the fight against terrorism and to Security Union in general.

Preventing and combating cyberterrorism. In order to outpace terrorist attempts to develop offensive cyber capabilities, all European agencies active in cyberspace, the CERT-EU, the Member States, their private sector partners and civil society will need to mobilise together to develop an effective capability, not just to understand the threats, but to develop an ability for attribution of threats and attacks and to build a credible layer of options for operational response.

Objectives for a secure future in digital services for Europe

Anne BERNER

Minister of Transport and Communications, Finland

Advances in technology enable us to innovate as never before. In the last couple of years, we have seen this development accelerating with advancements made in such fields as artificial intelligence, the internet of things and smart vehicles. Growth today, and increasingly so in the future, is built on data. The EU data economy, estimated to represent around two per cent of the entire European Union's GDP in 2016, could double to four per cent by 2020.

Meeting the challenges of the digital revolution requires a holistic digitalisation strategy that centres on digital businesses and the commercialisation of digital opportunities. Discussions surrounding the requirements of a more balanced data economy must be taken to a new level in terms of competitive markets, functionality of economies, equality and ethics. A successful data economy calls for new types of operating models that are based on data access and shared data, while not forgetting the need for new approaches to privacy and information security in order to create an environment that promotes innovation.

Trust in the reliability of data processing is a prerequisite for a digital society. Questions of privacy are increasingly relevant; data protection and information security are significant concerns to the public and private sectors and citizens alike. Utilisation of the vast economic and societal prospects of digitalisation will not be possible without the users' trust in both the internet and digital practices.

The main threat is that cybercrime, data breaches or large-scale privacy infringements will erode the trust of users in the internet and digital practices. The public's concerns relating to connected cars provide just one example of the problem of a lack of trust in data protection and information security. In a survey conducted by FIA (Fédération Internationale de l'Automobile), 85 % of Europeans indicated they were concerned that someone could hack their vehicle and interfere with their driving. This kind of lack of trust risks delaying the development of technology which could in fact drastically improve the safety of road users. According to studies, around 90 per cent of road accidents are in fact caused by human error, and driverless technology is expected to significantly reduce, if not eliminate, this factor.

Building the trust of users in digital services is not impossible. The banking sector offers a good example. All of us have trusted our money to digital accounts. We have also managed to develop a trust-based market of electronic identification. If we can trust our money and transactions into the hands of digital services, we should be able to do the same when it comes to transport, health care and all other sectors.

Notwithstanding the acknowledged benefits, digitalisation makes us more vulnerable to digital threats. We need to actively seek new innovative ways of countering these threats. In order to maintain the trust of citizens, it is necessary to ensure that the use of digital services, algorithms and artificial intelligence benefits the citizens and never acts against them. Governments and industry should face this challenge, and together figure out how to provide more trusted and secure digital services to the whole of society. When algorithms and artificial intelligence control everyday services, such as transport and health care, it is crucial to protect these services from unauthorised or harmful use.

Citizens and business users will inevitably demand more secure ICT's. Further actions should be taken to increase the availability of trusted and secure digital products and services globally. A prerequisite for intelligent solutions in fields such as trade, industry and transport is that the underlying systems and legislation are in order. It is essential that new technologies, such as the internet of things, artificial intelligence, automated transport and digital devices and services, are safe and secure by design. Privacy and security need to be integrated into algorithms and artificial intelligence. Cyber security certification, standardisation and encryption are key to making this happen.

Cooperation between different actors is crucial for achieving both a secure and encouraging environment where digital services can thrive. Information security and privacy are global issues, and we need to ensure, that the internet and the use of data does not become divided into regional blocks. National cooperation between companies and officials is important, but so is international cooperation. Active work towards developing a global approach, for example to cybersecurity, is needed. Within the EU, important steps for increasing EU-wide cybersecurity have already been taken, for example through the adoption of the Directive on security of network and information systems (the NIS Directive) and the pending adoption of the Cybersecurity Act. These legislative instruments increase cooperation between Member States within cybersecurity and endeavour to align some national practices in order to achieve improved cybersecurity within the union.

Digitalisation has much to offer in tackling the huge societal challenges of our time. A prerequisite is, however, that we simultaneously ensure the openness and sharing of data with trust, digital rights and cybersecurity. To achieve this end, the public sector, companies and individuals all need to collaborate, both nationally and internationally. Through this collaboration, a thriving and secure future for our digital services is within our grasp.

Secured European cyberspace: Stimulating the Ecosystem through financing

Ambroise FAYOLLE

Vice President of the European Investment Bank

Alexander STUBB

Vice President of the European Investment Bank

The EU is facing an increasingly complex and volatile range of security threats both beyond its borders and at home. On top of tensions in the Middle East and terror attacks on civilians in the EU, there is a strong increase in cyberattacks ranging from targeted malware incidents to the more subversive dissemination of fake news or the use of internet based communications for the preparation of terror attacks. However, the cybersecurity landscape in the EU is still fragmented and spending is spread across several national bodies.

The need to further address EU Cyber resilience at a European level has recently driven a number of initiatives launched. The European Commission and the European Cyber Security Organisation (ECSO) launched a contractual Public Private Partnership as part of the EU cybersecurity strategy. In order to increase access to financing, the European Council encouraged the EIB to examine further steps with a view to supporting investments in defence research and development activities. As a response, the EIB put in place the European Security Initiative - Protect, Secure, Defend, with the aim of strengthening its support for RDI for dual-use technologies, cybersecurity and civilian security infrastructure. The initiative aims to provide financing of EUR 6bn until 2021 in the domain of European security and defence.

Europe has so far not been at the forefront of adopting cutting-edge cybersecurity technologies. The technology leaders in this domain are mainly companies based in the US, Israel and China. We see thus as crucial the need to support on one hand the deployment of cyber security solutions in the public and the private sector and on the other hand, the development of new solutions and technologies- in the EU.

The EIB's focus will be on increased support to investments in Research, Development and Innovation for dual-use applications including in the field of cybersecurity. The EIB aims to step up support in particular for projects that address issues of cybersecurity for both the public and private sector as well as for those to protect civilian infrastructures.

Build trust to capitalize on the potential of the digital transformation

The rapid transformation to digital of our economies generates an increasing need for trust and security. Lack of existing cybersecurity infrastructure and technologies risks being the Achilles' heel of digitalisation in Europe. The demonstration of successful cyberattacks across a wide range of geographies and sectors demonstrates the vulnerability of digital assets and undoubtedly justifies the trend for more investment in cybersecurity.

The EIB is a key player when it comes to supporting the emergence of and building capacity in a new sector for Europe. Given the risks and the emergence of new threats across all areas of the economy, it is the EIB's mission to provide financing for innovative solutions to tackle cybersecurity challenges.

Develop a strategic European ecosystem with access to growth capital

The EIB actively supports investments in RDI by start-ups to large enterprises with facilities ranging from venture debt to senior debt. Cybersecurity is a sector with a substantial potential for the EIB. For instance, the EIB recently signed a EUR 20m finance contract with the CS Communication & Systèmes (CS) Group in France to support the implementation of its research and development programme. This type of financing has most often been made possible by a guarantee provided by the European Commission as part of the Juncker Plan, of which one of the priority actions is to promote innovation.

Likewise, the EIB's subsidiary EIF makes investments in Venture Capital and Private Equity funds that are active in the technology sector, which in turn invest in equity in start-ups. The EIF has committed funds to hundreds of ICT funds so far, focussing on digital technologies and cybersecurity.

Building a European ecosystem requires alignment and cooperation among European institutions. The EIB and the European Defence Agency (EDA), within their respective remits, teamed up to support EU policy objectives, in particular as regards the Common Security and Defence Policy (CSDP). The cooperation between the two entities materialises as major European initiatives supporting the EU level of ambition in the area of security and defence are launched, including a European Defence Fund. The EDA will support the EIB in the identification and assessment of projects.

Encourage adoption through access to financing

The EIB Finances security investments, mainly consisting in components of large digitalisation projects and programmes to strengthen the resilience of critical infrastructures and IT systems against cyber-attacks as well as other sectors making increasing use of digital such as the manufacturing, financial, healthcare or others.

The transition to digital economies requires investments in Cybersecurity as a vital response to increased threats of illegal access and malign use of data for the EU and global economies. New technologies such as the Internet of Things (IoT) and the increase in connected devices are likely to magnify the potential of threats.

Despite the increased awareness of both private and public players, several major inhibitors are still hindering an effective implementation of cybersecurity strategies, including: lack of top management buy-in, budget and resource constraints, skills shortages and limited access to talent pool. In addition, it is crucial to speed up investment in the secure functioning of the electronic infrastructure on which most of economic transactions will be based directly or indirectly. Successfully addressing these issues - skills and infrastructure and access to finance - while leveraging on Europe strong knowledge and industrial basis would allow Europe to navigate its way through the 2nd wave of digital/technological revolution.

The government's role in collaborative risk management

François THILL

Director, Cybersecurity, Ministry of the Economy Luxembourg

In the connected world, ICT is at the core of every system. Companies, administrations, citizen depend on a proficient and secure infrastructure.

Many actors are involved in information security management. These include regulators, like the data protection authority, the telecom and energy regulator, the regulator of the financial sector and the regulator in the area of critical infrastructures or in the context of the Network and Information Security (NIS) directive. It also involves Internet service providers, specialised ICT companies, as well as many administrations or companies, down to the individual citizen who uses new technologies in everyday life.

Technological and human failures increasingly confirm how much managers, experts and users are still unaware of ICT risks. The challenge for the growth of a connected economy is: How well do we know how to tackle this situation? What do we undertake to improve existing managing methods, share and coordinate the knowledge and expertise among security key players? It lies at hand, but most economies still fail to realise that what traditionally represents the 'shield' of ICT, i.e. the 'management of information security' must become more accessible, transparent, and coordinated to be successful at national level.

Information security is generally measured in terms of data confidentiality, integrity and availability. It is addressed by the existing legislation and the current EU guidelines in an extremely broad way by defining 'obligations of means', by making reference to the 'principle of proportionality and necessity' and by proposing risk categories, respectively minimum requirements or best practices. Thus, when dealing with information security management, one is often faced to oneself, because the standards are extremely complex and the application of a proper methodology rather expensive.

In our opinion, one of the ways to improve national information security consists therefore in establishing 'risk management' as the **major risk assessment and risk treatment tool for all players involved**. This undertaking represents important challenges, as a greater harmonisation of methods and results are required nationally at several levels. However, by taking into account the remarkable ISO/IEC 27005 methodology, and with the support of the already existing Luxembourgish information security structure, as well as its market players, it is a leap worth taking. The economic and societal benefits lie at hand: a state of the art security management at an individual level strengthens the overall national level of information security and conversely: performant national governance in terms of risk management reassures and inspires individual structures, thus increasing the user confidence - and use - of ICT systems.

The responsibility to grant a culture of security in a highly interconnected society that thrives notably on electronic commerce lies rather at government level, than with the individual. We strongly believe that it is the States' task to play a unifying role in risk management. It can take this role by democratizing the use of risk management and by putting in place an overall system of governance for information security.

The challenges everybody faces, mostly alone, when implementing risk management lies in making the right choices. Decisions should be based upon facts. Risk management decisions should be repeatable and comparable, at regulatory level but also on the level of companies dealing with subcontractors. Unfortunately, for the time being, most of us face the blank page when starting a risk assessment. There is only little exchange between experts, leading to subjective risk management, based on rare known facts.

A collaborative approach is needed. Based upon a commonly agreed taxonomy as well as a common understanding of scopes and of most important scenarios (a threat exploiting a vulnerability and causing an impact) would help to make risk management decisions more objective.

The ground knowledge, i.e. what kind of scenarios are likely to lead to incidents, lies within specialised security companies, Computer Incident Response Teams and regulators. The aim of the Luxembourg government is to generate, on the basis of this proficiency, a regularly updated situational awareness, helping companies to identify how to define the scope and what kind of risk scenarios should be taken into account. This would largely contribute to the creation of comparable risk assessments and improve governance efficiency in cyber security. Companies for themselves or at group level, companies dealing with their subcontractors, but also regulators should be able to rely on objective risk assessments and treatments.

Creating an evolving basis for risk management is only the very first step. The Luxembourg government is equally keen to distil information already available in a very technical form in MISP[1] into metrics in order to further detect threat probabilities and ease of exploitation of vulnerabilities, as well as analyse the effectiveness of risk treatments.

The government intends to create, in the spirit of the open MISP platform, a collaborative platform for the exchange of risk information. This platform would make available information about scopes and risk scenarios, and would also foster collaboration with partners to identify specific sectorial risk scenarios.

Cybersecurity is a process that nobody can address alone; close collaboration is requested in order to exchange valuable information in a trustworthy interdependent ecosystem.

1 Malware Information Sharing Platform

Cybersecurity as an enabler of Digital Innovation

Raul RIKK

National Cyber Security Policy Director, Ministry of Economic Affairs and Communications, Estonia

Cybersecurity is not a brake, but it is the enabler, which makes rapid digital innovation possible. Estonia has been developing its information society since the 1990s and has hitherto become highly dependent on its ICT infrastructure. 99 per cent of Estonian public services are online 24/7 and accessible worldwide. We could not have done it without an appropriate cyber security ecosystem.

One of the significant innovations in Estonia is the i-Voting system, where security is particularly important. In February this year during the Estonian parliament elections, approximately 40 per cent of votes were given electronically over the Internet. It is a new record for Estonia and the entire world. In 2005, when the i-Voting solution was introduced, 1.9 per cent of all votes were digital. Over the 15 years, i-Voting has become more and more popular due to its reliability and simplicity. It can be used securely around the world as long as a computer and internet connectivity are available.

Digital penetration is prevailing in Estonia. The Estonian Government sessions are organised and held online without paper since the year 2000. Annual tax declarations are prepared electronically and it takes about 5 min to confirm it. 98 per cent of the declarations are submitted online. Moreover, the same percentage of companies are established online, because the electronic process takes couple of hours instead of 5 days. Our whole public service system functions as a cyber-organism.

The smart and comprehensive cyber security ecosystem has been up and running without significant security incidents for 20 years. Even though the system was put under a test during the 2007 cyber-attacks against Estonia. The cornerstones of the cyber ecosystem are unified digital identity and secure data exchange layer for the Internet. Through these cornerstones and many other aspects, we have made unsecure Internet environment secure. Moreover, the government provided universal security system is available for all citizens, businesses and government entities.

The official digital identity (e-ID) is like a passport to the national cyberspace, where all e-services are accessible. It allows a secure authentication and usage of legally valid digital signature. By issuing e-ID cards (also mobile ID-s and Smart-ID-s), the government gives state of art encryption devices to the hands of the users. The digital ID makes an encrypted communication possible over the unsecure Internet.

Secure data exchange layer for the Internet is the Estonian "protected territory" in cyberspace. It means that electronic service providers can use information in different databases in the public and private sector over the Internet. In Estonia, data has a clear owner and is organised in different registers. If a certain information is available in some database, there is no need to collect it again. The e-service provider can use existing data as a national resource to develop e-services. All exchanged data is digitally signed, encrypted, authenticated and logged.

Thank to the outlined cybersecurity ecosystem we can avoid many common cyber threats. Our approach is to prevent incidents from happening in lieu of only managing them well. Cybersecurity is a part of the e-services development process, not a disparate system. We believe the key to success is the "security by design" approach, prevention of cyber incidents and resilience f the basic cyber infrastructure.

In recent years, EU has implemented several regulations and directives in the field of cyber security and data protection in order to establish the secure basis for single digital market. The eIDAS Regulation sets grounds for mutual recognition of national digital identities and electronic signatures. The NIS Directive provides minimum requirements for national cyber security arrangements and cooperation within the Union. Finally, the General Data Protection Regulation gives a legal basis for modern data protection.

In the coming years, it is important to implement these regulations and directives fully in the member states and take the secure digital compatibility to the next level. The smart European cyber ecosystem will boost EU-wide digital innovation the same way as it has proven its success in Estonia.

Developing an ecosystem in cybersecurity: Increasing capacity to support and protect a digital economy in the European Union

Roberto VIOLA

Director General, DG CONNECT, European Commission

The European Union has made creating a digital single market one of its top priorities. We in Europe firmly believe that the socio-economic model of the future is a digital one. But as in any other society, citizens and businesses need to feel safe in the digital society, and this is why the EU is working to build up its cybersecurity capacities.

In fact, we already have considerable expertise and experience in cybersecurity in the EU. A recent mapping of cybersecurity centres of expertise conducted by the European Commission recorded more than 660 organisations from across the EU. And the EU and its Member States have an important role to play - not to mention a strong reputation - in the global cybersecurity ecosystem, as the latest report from standard organisation ETSI clearly shows.

And yet for all this expertise and experience, the efforts of the cybersecurity research and industrial communities in the EU remain fragmented, lacking alignment and a common mission: each Member State has its own approach, its own goals, which often overlap with those in other Member States but can equally as often be entirely different. This lack of a common approach hinders not only the EU's competitiveness in this domain but also - and perhaps more importantly - its ability to secure its own digital assets.

The Commission's mapping exercise also showed key cybersecurity sectors such as energy, space, defence or transport currently lacking sufficient support. And where there are potential synergies - for example between the civilian and defence cybersecurity sectors - these are not being fully exploited in Europe either.

But the Commission's mapping also pointed out the potential in the EU: if we unite and invest in the development of our European cybersecurity ecosystem, then this ecosystem can deliver innovation and new, 'made in EU', cybersecurity products and solutions. Our European cybersecurity ecosystem could cover the whole cybersecurity value-chain and secure EU's Digital Single Market.

We have already indeed begun to work on putting the necessary structures in place. The creation in 2016 of the cybersecurity Public-Private Partnership ('cPPP') was a solid first step. 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. The EU will invest €450 million in this partnership up to 2020 but cybersecurity market players are expected to invest three times more, with up to €1.8 billion in cybersecurity investment expected to have been made by 2020.

Successful as these investments have been in helping to bring some structure and coordination to the cybersecurity sector in Europe, there is still much more than can be done. What we need is investment on a much larger scale and an approach based on building lasting capacities, pooling efforts and competences and stimulating the development of innovative solutions.

This is why in 2017 we proposed the creation of a European Cybersecurity Competence Network and Centre to help the EU retain and develop the cybersecurity technological and industrial capacities necessary to secure its Digital Single Market. Using the €2 billion in cybersecurity funds we expect to be available under the new Digital Europe funding programme for 2021-2027, as well as ongoing support for cybersecurity research under the new Horizon Europe programme, the aim is to create an inter-connected, Europe-wide cybersecurity industrial and research ecosystem.

We want to see each Member State setting up a national coordination centre that will act not only as that country's gateway to a wider cybersecurity competence community across the EU but also as the main interlocutor of the new EU competence centre. The centre will in turn coordinate the work of the network of national centres and nurture the cybersecurity competence community, drive the cybersecurity technological agenda and facilitate access to the expertise of national centres.

And we have already set out a number of concrete ideas to guide the work of this new ecosystem. For example, in the domain of cybersecurity research, development and standardisation we propose focusing on topics such as quantum-resistant cryptography, AI for automated threat detection and response or security and data protection for machine learning. The centre will also look at how to better support SMEs in the cybersecurity sector and encourage the wider take-up of cybersecurity tools.

As Europe and the rest of the world becomes increasingly digital, the intensity and sophistication of cyberthreats is likely to grow. We have to be able to respond rapidly and effectively to this ever-evolving threat, and this is why the EU's cybersecurity ecosystem needs to be reinforced, pooling and boosting EU resources and supporting innovation in this vital field.

Cybersecurity: Four steps in the cyber space

Michal BONI

MEP (EPP Group), Member of the LIBE Committee

It is time of the digital revolution.

There are digital challenges, digital issues and digital solutions. They are creating the digital game changer. The paramount impact of this game changer is seen in every area and every aspect of our life. What is the most important for the future, if we want to keep the human centric digital development of the world? The TRUST!

Trust is based on our needs and the desirable feeling of security, privacy protection, full respect of all technological inventions to the fundamental rights, ethical values, and the principle of transparency. Cybersecurity framework (institutional, legislative) is needed as a fundament to build the trust. What is the additionally important - is clear explainability of all rules significant for the cybersecurity addressed to all users, to all of us.

This is the FIRST STEP.

But, trust can be build and developed due to the sharing responsibility for the cybersecurity.

It means, that we have to start with individuals' responsibilities. Some kind of the cyber hygiene is crucial - our everyday customs, behaviors should be trained. We have to educate people, to give them some tools for the cybersecurity literacy. It is basic.

And the capability of all companies and institutions to make the risk analysis, clear assessment of the risks and to find proper responses - is crucial. It should be clear that we are not talking only about the critical infrastructure. Everything should be treated as critical, if we want to implement the strong, real solutions for the cybersecurity in the modern, digitally advanced world.

It also means that in every country we need to implement common European solutions - done in the NIS directive and the Cybersecurity Act, and to have properly, precisely described duties of the state institutions. For many activities, the national level is crucial.

At the end - it is the European responsibility with the new role and mandate of the ENISA agency, and some new institutions, key for the cybersecurity growth and the European certification model development. It requires the proper and desirable level of European harmonisation. In addition, it is important to build the European solutions in the course of the global undertakings and key-lines. The cybersecurity issues are global, because the threats are global.

It is the SECOND STEP.

Day by day, it is more and more understandable, that we live in the data economy paradigm.

If we want to protect our security at the cyber space - we want to keep the data secure and safety. Everything is about data: our participation in all kinds of digital services, the usage of all devices and logins and passwords to them, the new opportunities of the encryption and encrypted interactions, the information about formats of the hacking schemes, all our personal data from general information to the more sensitive, related to our state of health. The data are flowing, the exchange of data is crucial for the digital game changer. Therefore, we have to protect not only the data, the information, but also the transfers of data. In addition, when the data are under attack, it is meaningful to share all those information, incidents - for analysis: how it was done! We need to recognise the schemes of attacks - it is for investigation and future protection.

Additionally, it is time to use algorithms and Artificial Intelligence powers to support at the big scale the work of all analytical groups: from the ENISA team, Europol, national CERTs to all institutions responsible for the security. It is the challenge of speeding up the results of analytical efforts, more precise recognition of some patterns, and - predictions of the future schemes of attacks. The battle against cybercrime organisations is the never-ending story - it should be continued in every case and it should be oriented at some new forms of attacks. Making those attacks much more predictable is one of the key goals of the cybersecurity policies.

It will be the THIRD STEP.

Finally, we need to come back to the problem of certification schemes and instruments. It is essential for the cybersecurity. If we will have devices, systems, networks, any kind of walls etc. better and deeper harmonised and in the predictable future - unified due to the proper, European certifications, we will live in the much more secure environment.

It is the work, which should be done. But we need the agenda and the timetable to achieve this objective. The Cybersecurity Act established the framework for this purpose. Nevertheless, we should feel obliged to fulfil it completely with involvement of all partners at the European and probably the global level to make it real.

It is important for the cybersecurity, and for the cybersecurity industry development. It will create the new jobs, it will support the new investments based on the research achievements. There are many advantages of the process of making all cybersecurity certifications - European in a short-term perspective.

Moreover, it will be the FOURTH STEP.

There are the steps, which can lead us to the cybersecurity as European guarantee. It is possible to achieve this purpose, but - it requires the adequate and strong leadership.

ENISA Leads the Way for a better Cybersecurity in Europe

Udo HELMBRECHT
Executive Director, ENISA

The European Union Agency for Network and Information Security (ENISA) came into existence following the adoption of Regulation (EC) No 460/2004 on 10 March 2004. Within those last 15 years, ENISA has established itself as a centre for cybersecurity expertise in Europe, developing collaborations that are key to the Digital Single Market.

The Agency has successfully collaborated with European bodies and the EU Member States in preparing to respond to cyber challenges and threats. The past 15 years have been about working together both in policy and on an operational level, thereby creating a safer European cyberspace for everyone. ENISA strongly advocates that cybersecurity is a shared responsibility that can range from the cyber hygiene practiced by all to the introduction of connected cars.

In the last few years, the European Union made tremendous efforts to improve its preparations against rising cyber threats by developing new regulation (Network Information Security Directive, Cybersecurity Act) and making targeted proposals for cooperation (Cyber Competence Centre & Network, Public-Private Partnership on Cybersecurity, the Information Sharing and Analysis Centres). ENISA has made a major contribution to these efforts, and the agency's anniversary is an opportunity to reflect on its successful work. In creating lighthouse projects such as the Cyber Exercises, the Annual Data Protection Forum and the Cyber Threat Landscape, ENISA hugely drives increasing cybersecurity in Europe.

Despite the success and the achievements to date, this year will be special for ENISA and marks an important milestone. On the one hand, there will be changes in the ENISA leadership team, as I will leave the agency later this year concluding my tenth year as Executive Director. I wish my successor the very best in continuing the development of the agency's role in a time when stakeholders will increasingly look to ENISA for support. The change of the ENISA Executive Director and the European Institutional leadership indicates that a new era in EU cybersecurity is coming. In addition to those upcoming changes, ENISA is expected to receive a new permanent mandate and will henceforth be known as 'the EU Agency for Cybersecurity'. According to the proposed Cybersecurity Act (CSA), the agency will play a more important role, especially regarding the development and implementation of the cybersecurity policy in the EU. Moreover, the Cybersecurity Certification Framework will offer a new opportunity to prepare certification schemes.

Thanks to this new mandate and the opportunity to exert more influence, the Agency will grow in 2019. As a result, ENISA is currently hiring experts from a wide range of fields as cybersecurity is not a purely technical challenge but involves far more parameters such as societal and economic challenges. The Internet of Things (IoT), one of the most discussed and important technologies in the age of an increasingly ongoing digitisation, is a prime example for the aforementioned interconnection of different disciplines. Nowadays, IoT basically touches upon every aspect of human live. Therefore, it is essential to find ways to secure the European information society in such a way that the citizens feel safe using their devices as well as services while protecting their data.

To offer the needed trust and security, ENISA continuously develops processes and means of promoting security and was the first to introduce baseline IoT security recommendations. Earlier this year, the Agency released an online tool for IoT and Smart Infrastructures Security, which helps to identify threats and prioritise certain security areas. It ensures that companies can stay ahead of new deployments and have practical tools that cover cybersecurity requirements regarding all elements of the IoT ecosystem throughout its lifetime. While ENISA continues to provide tools and reports that offer concrete technical advice, it is also becoming a thought leader for IoT cybersecurity by, for example, implementing new formats to raise awareness for this topic.

In January 2019, ENISA held its first 'Transport Cybersecurity' conference, gathering a wide range of stakeholders from the aviation, maritime, road, rail and other public transportation sectors to discuss the security of our homes, cities and the entire infrastructures, which are becoming smarter and smarter. ENISA already highlighted the security concerns regarding IoT environments in the ENISA 2018 Cyber Threat Landscape but despite the Agency's efforts and recommendations, low-end IoT devices and services still often lack some important protection mechanisms. In the past few years, there have been numerous instances where IoT enabled children's toys had to be banned from sale as they provided poor security.

This is one example where ENISA's expertise comes into play. The agency offers support in analysing and advising where IoT needs to be more secure, and helps to prevent potential future problems instead of trying to solve them in the aftermath. Therefore, ENISA will continue to raise awareness for challenges surrounding cybersecurity of information technology while also providing practical and economically viable solutions for all stakeholders to lead the EU member states into a safer future. The next few years should be seen as an opportunity to build on ENISA's existing achievements and to continue fostering cooperation and increased stakeholder engagement, thereby shaping the future European cybersecurity landscape.

Guaranteeing a safe European cyberspace: a shared responsibility

Guillaume POUPARD

Director General of ANSSI, the National Cybersecurity Agency of France

With the European parliamentary elections around the corner, and the growing level of cyber threats, stakes are high for the European Union and its Member States regarding cybersecurity.

From the NIS directive that entered into force in 2018, the Cybersecurity Act, that will be adopted in the coming weeks, to the current discussions on the cybersecurity competence center, the EU has made important efforts to address cybersecurity challenges and managed to create what we have pleaded for: building an EU cyber community.

The upcoming renewal of the Commission and the start of a new legislative period gives us an opportunity to take stock of the progress made and of the challenges lying ahead.

Cybersecurity to defend European core values

With cyberattacks becoming more and more sophisticated, at a time where multilateralism is under threat, France firmly believes in European cooperation to defend Europe's core values but also its freedom to choose its own path.

Cybersecurity is no longer about protecting strictly delimited networks, belonging to States or critical infrastructures; it is about protecting the very functioning of the whole economy and society as well as the trust in the democratic process.

While under threat, some wrongly think that the answers are in the easiest solutions, such as weakening encryption or allowing private retaliation to cyberattacks in the form of "hacking back". However, beyond the disregard of EU's core values of freedom, peace and democracy, those solutions are also detrimental to the overall stability of cyberspace. In fact, by weakening the basic principles upon which cyberspace stability is resting, they pave the way to the emergence of a highly deregulated and chaotic digital Far West.

The Paris Call for Trust and Security in Cyberspace, launched by President Macron on the 12th of November, has been a new and innovative step to unite the international community, from States, the civil society, to the private sector, around core principles that we believe are necessary to preserve a peaceful, open and stable cyberspace. The support of this call by all EU Member states has shown that a shared vision is within reach on how to protect the digital economy and society against cyber threats.

Cybersecurity: a shared responsibility

The multistakeholder approach of the Paris Call is also a clear reminder that States will not be able to deal with such tremendous challenges alone. The private sector has sparked a great number of initiatives to step up efforts in this respect, demonstrating that this is no longer an area of concerns only for the States. Protecting the digital economy and society has indeed become a shared responsibility between the States, the private sector and the citizens.

With this new reality in mind, the European Commission and the Member States have strived to establish the foundation of an EU cybersecurity, gathering all relevant actors - from the NIS-inspired national authorities, the certification community, the digital industry to the research community. Thanks to these efforts, all those actors are now working together to address common challenges at the EU scale.

The EU's way forward

A lot still needs to be done to promote the EU's own approach to the security of cyberspace.

Firstly, it requires the strengthening of EU's strategic autonomy, through technological, capacity building and regulatory efforts. Secondly, it demands the reinforcement of the responsibility of private actors in the security of digital services and products, throughout their lifecyle and supply chain. Thirdly, it requires the EU to promote its unique approach on cybersecurity on the international stage, in particular through diplomatic efforts.

During the next European legislative period, France will be an avid supporter of cooperation at EU level in order to reach these ambitious common goals.

A new certification framework for Europe: building trust in digital technologies with the new Cybersecurity Act

Peter KOUROUMBASHEV

MEP (S&D), ITRE-Committee and Shadow-Rapporteur on the Cybersecurity Act

The European Commission's proposal for a regulation on ENISA and on Information and Communication Technology cybersecurity certification, also known as "the Cybersecurity Act", has been a major step towards better prepared and more cyber resilient European Union. ENISA, the European Cybersecurity Agency, will now have a permanent mandate and its budget will be doubled. Nevertheless, this new budget will still be less than an average European bank's. Hopefully it could be doubled again in 7 years' time and every 7 years after that.

ENISA will now have reinforced competences for assisting the Member States (MS): it will be empowered to promote security-by-design and privacy-by-design for IT services, products and processes. It will also be able to deploy technical capabilities in response to cyberattacks at the request of a MS. My idea was to propose the Agency to have technical capabilities to analyse threat information data at large scale, the ability to conduct forensic analysis on terminal equipment and the ability to analyse malware, among others. This detailed list of capabilities, however, appears in the text in a summed up version: "necessary resources, including technical and human capabilities and skills". Nonetheless, the new capabilities, even if not expressly mentioned, will pave the way for ENISA to one day play a central role in organizing an EU-coordinated response in cases of cyberattacks, in accordance with the procedures set in the Blueprint for rapid emergency response, adopted in the 2017 Cybersecurity package. This is not the case yet as my wish for the Agency to have its own "EU CERT" was not realized. Another area where ENISA could play a leading role in the future is by creating a certification scheme for 5G equipment, in accordance with the new cybersecurity certification framework rules discussed below.

Among the new tasks of ENISA is to promote a high level of cybersecurity awareness, including cyber hygiene and cyber literacy among the European citizens and businesses. The Agency will be supporting the MS by enabling closer coordination and facilitating exchange of best practices. The aim is to achieve a certain level of cybersecurity risks-related knowledge at all levels: from the young children at school or university students, to experienced professionals or, most importantly, various businesses where the topic is still not properly addressed. This will also have a crucial role in developing the cybersecurity industry in the EU, in particular SMEs and start-ups. Also, in order to keep SMEs and start-ups in the game, part of the new European cybersecurity certification scheme will be a conformity self-assessment, which can be carried out by a manufacturer or provider of low complexity ICT products and services with low risk for the public interest. This will allow for SMEs and start-ups to keep their position on the market by adhering to the new certification rules set at EU level.

An important task related to capacity building is that ENISA is going to assist Member States by organising regular and at least biennial cybersecurity exercises at the Union level. This is highly insufficient: these exercises need to be organized at least twice a year in order to keep the pace with the fast evolving cyber threats landscape. The main goal is to achieve better cooperation and partnership between the MS, which will be achieved only partially because of the agreed frequency of exercises. Nonetheless, ENISA will now have the opportunity to draft policy recommendations based on the evaluation process of the exercises outcome and the lessons learned from the gathered experience.

Another significant point regarding ENISA is that in order to achieve its objectives, it may cooperate with the competent authorities of third countries or with international organisations, in particular NATO and Europol. Essentially, ENISA will have the freedom to establish working arrangements with the aforementioned organisations. In addition, it will also provide advice and support to the Commission on matters concerning agreements for mutual recognition of cybersecurity certificates with third countries. The idea behind this it to have our EU standards having worldwide applicability rather than only EU-wide, which for instance could be the case with a successful ENISA-developed 5G certification scheme. This leads us to the next section of the Cybersecurity Act, the EU cybersecurity certification framework.

An important achievement with this new piece of legislation is that the certification framework is more future proof: there will be no maximum validity of the scheme, which means no additional cost for the companies forced to reissue certificates after a certain time. From now on, ENISA's task will be to review the schemes every five years. I agree with the negotiation team's final position that a mandatory certification at this stage would not have been a step in the right direction. In this way, this new certification framework will not be used as advantageous by the big names in the field.

When issuing certificates and EU statements of conformity, national cybersecurity certification authorities will be subject to peer review. It will cover these authorities' activities related to the issuance of certificates and whether it adheres to a strict separation of roles and responsibilities. It will also cover the procedures for monitoring and enforcing the obligations of manufacturers and providers of ICT products or services, among other things. The peer review will be performed by minimum 2 authorities coming from other MS and the Commission and will be carried out at least once every 5 years. ENISA can also take part in these reviews. The added value of the peer review is that more tech-savvy MS could help less cybersecurity-prepared countries which will help avoiding fragmentation of the market.

At the final trialogue in December 2018 it was agreed that European Cybersecurity Certification Group (ECCG) will be established. The ECCG, composed of representatives of the abovementioned national cybersecurity certification authorities, will advise and assist the Commission on the consistent implementation of the Union rolling work programme, a strategic but not legally binding document to serve stakeholders when preparing for future cybersecurity certification schemes. The ECCG or the Commission could, in duly justified cases, request ENISA to prepare candidate schemes. This brings the necessary balance between the Group and the Commission.

Last but not least, we managed to convince our colleagues from the other EU institutions of the significance of the establishment of a Stakeholder Certification Group (SCG), which will advise the Commission on strategic issues and assist with the preparation of the Union rolling work programme. ENISA and the Commission will both have a say in the selection process of the members. Our objective was to reinforce the presence of stakeholders in the process of elaborating the new certificates. Academia, industry and consumer associations are going to be able to provide advice also to ENISA. Moreover, in cases of urgency, the SCG will have the power to advise the Commission and the ECCG on establishing new certification schemes not included in the work programme. Furthermore, ad-hoc working groups that will include relevant stakeholders with expertise on the concrete subject will be set to advise ENISA throughout the development phase of the schemes.

What has not been accepted in the final text of the Cybersecurity Act and will perhaps be included in another EU cybersecurity-related legislation, is the establishment of a cybersecurity adviser to the President of the Commission. In the future, this role could be in the hands of ENISA's Executive Director or a separate individual. Such an expert will provide invaluable input to the President on ENISA's activities, on the national CSIRTs and any cybersecurity strategies.

Enhanced cyber-security is vital for europe's energy infrastructure

Dominique RISTORI

Director-General for Energy, European Commission

The energy infrastructure is one of the most critical assets of a modern society. Its effective operation is a pre-condition for securing energy supply for a wide range of economic and social activities. Without energy, we cannot fuel our cars, withdraw money, run our industries or our hospitals or access the internet.

Due to the urgent need to address climate change and to put in place the necessary transition to a low-carbon economy, the energy sector is undergoing a profound transformation in terms of infrastructure and market functioning. In addition, citizens are more and more actively participating in the energy market as consumers and decentralised producers of energy.

Traditional energy technologies are also becoming ever more connected to modern, digital technologies and networks. This increasing digitalisation makes the energy system smarter and enables consumers to benefit better from innovative energy services. At the same time, digitalisation creates risks by an increased exposure to cyber-attacks and cybersecurity incidents, potentially jeopardizing the security of energy supply or the privacy of consumer data.

Today, cybersecurity is very high on the political agenda and the European Commission has been very active in tackling cybersecurity challenges. In September 2017, it adopted the Cybersecurity Package[1], which includes the Cybersecurity Act[2]. This package follows up on the EU Cyber Security Strategy of 2013[3] and the Directive on Security of Network and Information Systems[4] of 2016.

However, what might work for the internet will not be necessarily adequate for other sectors. In this context, it is indispensable to have a closer look at the energy sector in terms of cybersecurity and to identify and address its particularities. Indeed, the focus should first be put in priority on energy infrastructure and grids. They are among the most complex and most critical infrastructure serving as the backbone of our economic activities and security.

First, there are real-time requirements. Some energy systems need to react so fast that standard security measures such as authentication of a command or verification of a digital signature can simply not be introduced due to the delay these measures impose.

Second, the energy system can produce cascading effects. Electricity grids and gas pipelines are strongly interconnected across Europe and well beyond the EU. An outage in one country might trigger black-outs or shortages of supply in other areas and countries.

Finally, the energy system is the combination of legacy systems with new technologies. Many elements of the energy system were designed and built well before cybersecurity considerations came into play. This legacy now needs to interact with the most recent state-of-the-art equipment for automation and control, such as smart meters or connected appliances, and devices from the Internet of Things without being exposed to cyber-threats.

The European Commission is therefore addressing these specificities of the energy sector in several ways. In the short run, it is developing sector-specific guidance to implement horizontal cybersecurity rules. This guidance is planned to be adopted together with the Report on the State of the Energy Union in spring 2019 and aims to increase preparedness in the energy sector.

As cooperation and trust among stakeholders as well as among Member States is key when it comes to cybersecurity due to the potential cascading and cross-border effects, the Commission is also working to raise awareness about cybersecurity and to promote broad discussions among different stakeholders from the energy sector. For this purpose, the Commission organised an event on Cybersecurity in the Energy sector in Rome in March 2017 on the occasion of the 60th anniversary of the Treaty of Rome as well as a high-level event in October 2018 in Brussels and participated to the last two editions of the International Forum on Cybersecurity in Lille.

The Commission also plans to strengthen the role of the European Energy–Information Sharing Analysis Centre (EE-ISAC) which helps utilities improve the cyber security and resilience of their grid by enabling trust-based data and information sharing.

Delivering on the Energy Union goals requires a fundamental transformation of Europe's energy system while maintaining a high level of security. By the end of 2018, the EU concluded the negotiations on the Clean Energy for All Europeans package which puts forward the most advanced regulatory framework to lead the clean energy transition. It creates an optimal environment for taking advantage of the digital transformation in the energy sector while reinforcing cybersecurity.

The new regulation on electricity risk preparedness will mandate Member States to develop national risk preparedness plans and coordinate their preparation at regional level, including measures to cope with cyber-attacks. Furthermore, the recast of the Electricity Regulation proposes to develop a network code on cyber security, to increase the resilience of the energy sector and protect the energy systems.

But as cybersecurity is a continued effort, the work of the European Commission will not stop here: it will continue in order to protect and enhance our energy infrastructure to guarantee energy is delivered securely and safely to European citizens.

1 JOIN(2017) 450

2 COM/2017/0477

3 JOIN(2013) 1

4 Directive (EU) 2016/1148

Keep the "Trojan" horse out: energy transition requires enhanced security for grids and data

Kristian RUBY
Secretary General of Eurelectric

As Europe proceeds with the implementation of the Paris Agreement, the role of clean electricity will continue to grow. By mid-century, electricity will need to cover at least half of all energy demand. In order to decarbonise, our buildings, transport systems and energy-intensive industries will gradually need to be electrified. And with electricity assuming an even more central role serving society's energy needs, ensuring a stable, secure supply of electricity will become increasingly critical.

As we decarbonise, the electricity system will change. And so will the crucial parameters for security of supply. As often stated, decarbonisation goes hand in hand with a radical decentralisation of the power system as well as a profound digitalisation required to control a much more complex power system. The implications of digitalisation and decentralisation will be absolutely paramount when constructing a new, climate-compatible paradigm for security of supply.

Decentralisation of the system will mean that distribution system operators (DSOs) will play a key role. Just eleven years from now, their core functions and responsibilities will have fundamentally evolved, pushed by the booming development of decentralised generation from renewables, together with the need to connect some 40 million electric vehicles that will drive on our roads. Adding to this, important uptakes of connected electric heat pumps, rapid developments on batteries and other grid edge technologies will also add to the need for top-tuned distribution operators.

DSOs 2.0 must be agile. Hence, they must update their current capabilities and invest massively in new ones that enable the sophistication of assets management, integrate digital solutions and build new skillsets.

With increased digitalisation, smart grids foster a two-way communication between utilities and networks. This enables them to monitor and automate their operations, and thus substantially contribute to the improvement of system reliability, resilience and efficiency.

Gradually, DSOs will become platforms that enable customer empowerment, leverage flexibility resources and facilitate non-discriminatory access to the energy system.

Traditional energy systems were composed of control systems tailored to operate physical networks. Today however, they are going through a substantial digitalisation process. On the one hand, the system becomes smarter and enables customers to actively participate in the market. On the other hand, it increases exposure to cyber-attacks with a potential to jeopardise security of supply and breach data privacy.

Protecting networks and data becomes critical, as during the past decade over 400 serious attacks on infrastructure happened annually.

Electricity grids are strongly interconnected across Europe, with over 4 million network nodes allowing for reliable monitoring of grids and the control of operations. At the same time, this opens the door to potential cyber-attacks. The complexity of this situation increases as systems cannot be turned on and off easily, and therefore a system outage triggers cascading effects into other sectors and regions.

When it comes to network operations, the cornerstone of cyber security is represented by robust intrusion detection systems and processes that allow for a swift system recovery. In light of increasingly sophisticated and frequent cyber threats, Europe needs to step up and increase awareness, vigilance and create a forward-looking regulatory framework.

From plant to plug, and across platforms, digitalisation heralds numerous benefits for all players in the power ecosystem. To reach the full potential of these benefits, several regulatory frameworks must be developed conjunctively.

First, the current infrastructure was designed at a time of very limited cybersecurity considerations. DSOs must now be equipped with adequate "fit for the future" capabilities, which allow for a suitable mix between conventional and IT based operational technologies. This includes substantial investments in early warning systems, breach detection and response capability.

Secondly, DSOs require long-term and stable regulations that facilitate efficient and resilient market exchanges. Increased interoperability, transparency and standardisation of both communications and data protocols are essential enablers of cooperation. For instance, standardised, smart and public charging infrastructure is paramount to provide electric fuels to 95% of the vehicles that will cross the European roads by 2045.

Last but not least, Europe must strive to build a cybersecurity culture. One step forward was made with last year's political agreements on the Cybersecurity Act providing support to Member States in tackling cyber threats and boosting security of online services and customer devices. Another step forward will be taken with the creation of the DSO Entity that should be brought to develop sector specific cybersecurity codes.

Process-based Security Certifications Are the Right Fit for The Digital Economy

Tim MCKNIGHT
Chief Security Officer, SAP SE

Meet a new certification model that complements existing security practices while increasing confidence and breaking rigid borders in digital environments.

Across the digital economy, the potent mixture of speed, openness, and connectivity is stressing standard security practices. Companies are connecting to customers, suppliers, partners, employees, and assets, and the threat landscape gets larger with every connection. Bit by bit, organizations become easy prey for malicious actors looking to compromise systems, steal data, and hold organizations for ransom. Nation-state threats are no longer philosophical discussions; they are a real concern.

The scale and cross-border nature of cyberthreats calls for stronger and more structured dialogue and a harmonized approach among standards bodies, governments, businesses, security technology providers, users, and in particular companies offering secure products and services. Ultimately, these parties must work collaboratively to remove digital barriers that slow economic growth and market development. A united effort is the best prospect for successfully identifying digital processes that suit the digital economy and secure global connectivity.

There's a real and obvious need for consolidation of national certification schemes and the development of new ones to address challenges triggered by emerging technologies and new business models. Within a new security framework, we can build greater transparency and trust in our digital-centric world.

Borderless cyber threats need a global solution

For decades governments and security bodies have crafted security regulations and individual product or system certifications to protect our critical infrastructures in energy, banking, healthcare, and transport. Cyberattacks are a significant cause for worry in these high-profile industries, and operators have worked diligently to ensure that appropriate network and information security measures are in place. The general benchmark of "zero trust and validate all" has led to the current product- and system-centric certifications, which have served nations well and protected our infrastructures. In these environments where components have a long lifetime, the existing certifications are a much-needed requirement, but digital environments have a completely different playbook.

Digital environments have unique, diverse landscapes. Let's look at the characteristics of these environments and their impact on the certification process.

Global in scope. Globalization is a major factor in today's market. Rarely do industries remain within a single border. A cybersecurity certification strategy for international efforts requires a global effort, as it is a global challenge. Our world's hyperconnectivity crosses borders and security must be defined on an international level.

Agile in response to changes. While agile may be an overused term, it is undeniably a hallmark of current software development. Under agile software development practices, updates are constantly refining the software and user experiences. These rapid development cycles are fueled by speed and flexibility and can lead to daily updates and new releases to mobile and enterprise apps. New security regulations must accommodate the fast pace of these updates. Product- and system-centric certificates cannot match the speed of software cycles.

Scalable for large and complex systems. Considering the scope and complexity of digital projects, a scalable security process is a necessity for successful go-to-market deployments. In a typical industrial IoT system, such as a connected car, a real-time supply chain, or a predictive maintenance application for industrial machinery, the scope is sizeable. These systems are composed of devices, edge components, communication links, platforms, and applications and services providing the actual business functionality, which can run on edge devices, platforms, or stand-alone. The components are provided, owned, and operated by multiple entities and can be exchanged on the fly. A security model must accommodate the diverse and interchangeable nature of the environment.

Adaptable for heterogeneous technologies. Connected cars, manufacturing on demand, and automated remote asset monitoring are early examples of complex digital environments that have heterogeneous technologies.

These environments thrive on openness and easy accessibility, creating a delicate balance that supports security controls without preventing access. Cloud-based services, for example, are standard within digital businesses in a public, private, or mixed architecture, and their technologies are typically from a heterogeneous set of third party-providers. End-to-end platforms and systems are not the norm so a security framework must work within this multi-player, multi-component, open environment.

Economically viable. The certification process must be of global scale, spanning nations, verticals, and organizations. Nations and organizations should include mutual recognition agreements. At all costs, they should avoid the need to repeat certificates for multiple nations or bodies. The additional expense of multiple certificates for the same assessment places too much stress on global operators. Under the same argument, the certificates should cover product portfolios rather than individual products.

Collectively, these attributes of a digital landscape point to a need for a security framework that is unlike the current ones. Rather than replace current frameworks, an up-to-date process-based certification should complement present-day certifications. The core concepts for a digital-friendly framework are: process oriented, risk based, and harmonized across all regions and verticals. The certification would be based on international standards and address the effectiveness for the processes applied to the development, deployment, and operation of the software.

Under process certification, solution and software providers would provide the security best practices applied to their development activities and acknowledge the protection needs and risk exposures for each release. The process would extend to all lifecycle phases, including deployment and operation.

Security under the European Cybersecurity Act

With its move towards the establishment of a European cybersecurity certification framework, the European Commission would be in an ideal position to promote process certification as an alternative for providing transparency of security assurance in an agile, digital environment.

The final Cybersecurity Act includes process certification alongside product and service certification. Therefore, the European Union Agency for Network and Information Security (ENISA) should consider a process-based certification a priority under its extended mandate defined in the Cybersecurity Act. The entire industry would realize significant progress by elaborating on a similar certification for mainstream commercial software systems and cloud services and working with industry stakeholders and security labs.

Moving forward, greater collaboration between EU Member States to harmonise security measures and reporting requirements is crucial to continued growth in the digital economy. What's needed now is a risk-based, harmonised and international approach that gives the private sector the flexibility to adapt to rapid changes. In these environments, process-based certifications are a much-needed solution.

Securing global efforts together with process-based certificates

Process certification is a promising alternative since it can assure that best practices have been employed for the design, development, and operation of a complex system. With process certification, security best practices will be applied in the development activities of each product. As the technology evolves, process-oriented schemes will not require re-evaluation when new product versions embody the latest technology controlled by best-practice methodologies. Innovation can continue.

As global cybersecurity threats loom larger, our hope is that European institutions cooperate more closely with trade associations, international forums, and industry experts. Security is a joint effort, and we look forward to working more closely with everyone in the ecosystem to build global secure digital environments.

Cybersecurity Act: New Momentum for Europe

Angelika NIEBLER

MEP (EPP Group), Member of the ITRE Committee

A couple of days before Christmas, the European Parliament and the Member States reached an agreement on the Cybersecurity Act. At the end of the year, when people all over the world celebrate Christmas, the birth of Jesus Christ, when families come together, kids are very excited, looking for their Christmas gifts. They often find the latest electronic devices underneath the Christmas tree. Kids love them, start playing with them, but are all these smart devices cyber secured? Do they guarantee the user safety and privacy?

Actually, as the responsible rapporteur for the Cybersecurity Act in the European Parliament, this reflection was my starting point. My mission was to make sure that all users of internet of things-devices could place trust in the safety and security of their products. With more and more devices and services connected to the internet, users are increasingly put at risk of cyber-attacks. Europe is becoming more digital with every passing day. Over 80% of the EU's population have internet connections and by 2020 the vast majority of our digital interactions will be machine to machine with tens of billions of internet of things-devices. At the same time, Europe is facing an increasing amount of cyber-attacks like "WannaCry" or "NotPetya" threatening Europe's prosperity and society. But, the EU is reacting to this threat! By establishing an EU framework for cybersecurity certification, we want to ensure a harmonized approach within the EU to handle these attacks in the most efficient way.

As we all know, humans are often the biggest security risk. We do not change our passwords regularly, we do not efficiently protect our home routers, we are often not smart in handling our smart home applications and most importantly, we are not patching often enough. But it is not only the user who is in charge of increasing the security of smarts devices, we, the European legislators, have to provide a framework which creates more trust in the security of these devices. Therefore, the Cybersecurity Act aims at increasing the acceptance of digital technologies in our daily lives. The European Parliament insisted that product information for users for smart devices must be provided, so that users are given guidance and are provided with recommendations on secure configurations and maintenance of their devices, availability and duration of updates and known vulnerabilities. Following the recommendations, will provide for more cyber security for smart devices.

The Cybersecurity Act however not only increases users' trust in internet of things-devices, but also strengthens the stakeholder involvement in the certification process. Neither governments nor the industry can face the challenge of ensuring a higher level of cybersecurity in the EU alone. By allowing stakeholders to contribute to the development of cybersecurity certification schemes, we allow for the maximum use of the available expertise in Europe. A transparent work programme outlining all upcoming cybersecurity certification schemes will also contribute to an inclusive process. By showing what certification schemes are planned by the European Commission and drafted by ENISA, the European Cybersecurity Agency, the industry can prepare and better plan. The voluntary certification schemes will later be assessed by the European Commission who can then decide whether a certain scheme shall be made mandatory. This is an important step towards more security, especially for our critical infrastructures. The agreed Cybersecurity Act furthermore strengthens the role of ENISA by increasing its budget, staff, providing it with a permanent mandate and expanding its tasks.

These new provisions are urgently needed as studies have shown that last year, 80% of European companies fell victim to at least one cybersecurity incident. In some Member States, half of all crimes committed are cybercrimes! This development is very worrisome and has made the issue of cybersecurity one of the top priorities of the EU. The EU needs to react and it does! It is not too late but if Europe wants to be one of the leaders worldwide in this area we have to be quick and develop a comprehensive European strategy to ensure that there is an environment for start-ups and innovative ideas to grow, for research in this area to increase and for companies to be competitive on the global level. Cybersecurity not only is a top risk for European companies but also a top business case. The existing expertise in cybersecurity needs to be used more effectively to create a competitive advantage for the European Union.

The Cybersecurity Act also needs to be seen in the context of the wider strategy of the Digital Single Market. Next to the NIS Directive, the Directive on Security of Network and Information System, whose objective is to improve national cyber-readiness and capabilities, the two other policy initiatives are the Cybersecurity Act and the proposal on the Cybersecurity Competence Centres. By implementing this proposal, a cybersecurity competence network with a European Cybersecurity Research and Competence Centre at its heart shall be created. We need to keep up with technology developments and increase cyber-readiness and resilience. With this holistic strategy, progress is made. After all, Europe needs a cyberspace that is safe and secure in order for the European Union to compete internationally. Let us fight for a safer Europe together!

Driving security in uncertain times The Charter of Trust for a secure digital world

Eva SCHULZ-KAMM

Global Head of Government Affairs at Siemens AG

Digitalization is the biggest and most radical transformation in the history of industry. The real and virtual worlds are merging – digital twins, robotics, big data, and artificial intelligence are revolutionizing the world of manufacturing. And as the number of devices and machines connected to the Internet of Things grows, the risks are rising: In 2017 alone, cyber attacks caused damage amounting to €500 billion worldwide.

What if attacks on critical infrastructure were successful? What if the IT systems connecting and controlling our homes, hospitals, airports, factories and power grids failed? How can we protect our economy and our society, and ultimately the more than seven billion people on this planet against such attacks? Well, first, by recognizing that the threats in the digital world are real and that they put the real world at risk. And, second, by understanding that we can only meet these threats together – by joining forces and making a strong collective effort.

That's why Siemens, together with the Munich Security Conference and a number of other companies, initiated the Charter of Trust. It outlines principles and concrete actions based on our expertise and more than 30 years of experience in the field of cybersecurity. The goals of the Charter are clearly defined: first, to protect the data of individuals and companies; second, to prevent damage to people, companies, and infrastructure; and third, to create a foundation for trust in the digital world. We're already taking action to achieve these goals.

An area of early and intense focus has been security of global supply chains. Third party risks in global supply chains, are becoming a more prevalent issue and are the source of 60 percent of cyberattacks. The Charter of Trust member companies have worked out baseline requirements and propose their implementation for making cybersecurity an absolute necessity throughout all their digital supply chains. These requirements address all aspects of cybersecurity – including people, process and technology. Examples of these requirements include:

- Data shall be protected from unauthorized access throughout the data lifecycle.
- Appropriate level of identity and access control and monitoring, including third parties, shall be in place and enforced.
- A process shall be in place to ensure that products and services are authentic and identifiable.
- An appropriated level of security education and training for employees shall be regularly deployed.

Together we are establishing a risk-based methodology for implementing these requirements in our own supply chains, involving supply chain partners in the process. In addition we're exploring how to improve awareness and knowledge of cybersecurity issues through training and education.

And that's just one side of the coin. With our round tables worldwide, we enabled an in-depth exchange between policy makers and the Charter partners. Governments and industry are aligning at the global, regional and national levels in the pursuit of common security goals. The "Paris Peace Call for Trust & Security in Cyberspace" presented in November 2018 by French President Emmanuel Macron for example is a clear commitment to form and achieve stability in cyberspace and confirms the willingness to work together to define and implement international cybersecurity principles. Content wise, the Paris Peace Call shares key tenets with the Charter of Trust principles and the partners look forward to seeing them reinforced further at the forthcoming G7 summit. Also, the new EU Cybersecurity Act was an important step towards strengthening cyber institutions and providing more security in uncertain times.

But that's not all. For 2019 we have set ourselves ambitious goals. Besides deepening and expanding the policy dialog, we plan to advance the topic "Security by default". This means that security is already preconfigured during the development of products.

Since 2018, the Charter of Trust has grown to 16 members. In addition to Siemens and the Munich Security Conference, the signatories include AES, Airbus, Allianz, Atos, Cisco, Daimler, Dell Technologies, Deutsche Telekom, Enel, IBM, NXP, SGS, Total and TÜV Süd. In addition, the German Federal Office for Information Security, the CCN National Cryptologic Center of Spain and the Graz University of Technology in Austria have joined the charter as associate members. On February 19, 2019, Mitsubishi Heavy Industries (MHI) signed a letter of intent to join the Charter of Trust for cybersecurity in Tokyo, expanding the Charter's reach into Asia. The company's membership is expected to be finalized by the end of September 2019. MHI will be the first Asian company to join the global cybersecurity initiative.

That clearly demonstrates: no company and no country is big enough or powerful enough to meet the cybersecurity challenge alone. That's why all of us should work together to establish binding global rules and standards. The Charter of Trust shows that even in times of imminent trade conflicts and growing mistrust, global collaboration is possible for the good of all.

www.charter-of-trust.com

Cybersecurity in AI and Robotics: The importance of a protective EU framework

Mady DELVAUX-STEHRES

MEP (S&D Group), Chair of Working Group on Robotics, European Parliament

With the development of artificial intelligence and the IoT cybersecurity became a major concern for citizens, ranging from the infringement of our right to privacy to the threat of major terrorist attacks.

Cyberattacks clearly can have considerable consequences for our society and are the prototype of international cross-border activities, it is thus clear that the EU has to act and create a protective European framework.

There are plenty of examples showing that the development of our technologies and the improvement of cybersecurity have to go hand in hand. For instance, how could we trust autonomous cars that rely on a vulnerable infrastructure / network?

All the experts I have discussed this matter with clearly agreed on one thing: When it comes to the hacking of a product or a service, the question is not "will it be possible to hack this product?" but "How long will it take to hack it?"

To meet this challenge, an increased EU-level cooperation is needed both for citizens and for industries.

For four years, I have been calling on the Commission to act on AI and robotics for the EU to catch up with China and the US. If we are deemed late on this issue, the EU strength could still be to foster the development of a safe and ethical AI.

From the Communication of the Commission in 2016 to the adoption of the Cybersecurity act by the Parliament in the plenary March I, many steps go in the right direction for the development of a trustworthy framework.

I believe the creation of an EU cybersecurity certification framework for ICT products and services is a very good first step. These harmonised requirements provide more legal certainty for companies, guarantee safer products and services and boost the trust of consumers. The creation of compulsory certification for products and processes that operate in critical sectors of our economy (transport, energy, health, banking system etc) is a plus. However, I consider that a general standardisation carried out by the CEN-CENELEC would have been more efficient than a voluntary basis or a sectorial approach.

The new mandate of the ENISA as a permanent and stronger Cybersecurity agency is definitely a plus to assist Member States and ensure a good cooperation. The involvement of the different stakeholders such as industries, consumers, SMES and other relevant actors in the cybersecurity sphere to provide to the Commission and the Agency with external expertise and know-how is a good initiative.

The recommendation for a coordinated EU response to cyber-attacks, the so-called Blueprint, is an essential mechanism to answer to the increasing number of cyber-attacks.

Diplomacy is also a strong mean to ensure the countries selling their products in Europe respect at least the same standards of protection as the ones applied in the EU. Given the global nature of the challenge, building and maintaining robust alliances and partnerships with third countries is fundamental to prevent and limit cyber-attacks – which are increasingly central to international stability and security.

Beyond the challenge of security, I think we should carefully look at the ethical and educational aspects.

The Ethics guidelines proposed by the High Level Expert Group in the beginning of April should pave the way for an ethical development of AI respecting our European values such as the right to privacy. But here again, I am afraid of the voluntary basis parameter. We should seize the opportunity to make ethical principles compulsory. Our EU values are the core of our identity, it should not be something you choose to take part in or not.

The transparency and accountability of algorithms requested in the guidelines could be useful to understand how AI works and thus improve their resilience to cyberattacks.

This additional information is however useless for the consumer if it is not put in place along with a proper/ an efficient educational system.

Users should be aware of the functioning of AI, its advantages and risks and should know the best practices to take the most benefit from the use of these products and services.

It is our role to provide consumers, businesses and researchers with the best framework to ensure safe, cyber-secure and trustworthy products in the EU.

Education as a tool against cybercrime

Miriam DALLI

MEP (S&D Group), Coordinator in the ENVI Committee

The Internet: a powerful tool that we use for different purposes including communication, work, education and entertainment amongst others. It is the place where access to online information is so fast that it makes it unprecedented. Information, news - whether true or false - can spread so quickly and easily that it makes it the perfect target for manipulation.

The internet is a world of opportunities as much as it can be harmful, not in of itself but in how it is utilised.

Cyber bullying, cyber-attacks, cyber-crime, and cyber threats: these are all the downfall of a digital world that we believe should be used to improve citizens' lives and help businesses expand their reach.

In 2016, over 4,000 ransomware attacks were registered daily. Last year, 80% of European companies experienced at least one cyber-security incident. More statistics show that security incidents across all industries rose by 38%, marking the biggest percentage increase in the past 12 years.

Even though we should not undermine the positive elements that the Internet brings with it, we must not ignore those 'dark forces' that are ready to use this tool as a weapon. Suffice to say that in some Member States, 50% of all crimes committed are cybercrimes. In 2017, over 150 countries and more than 230,000 systems across sectors and countries were affected by the WannaCry attack with a substantial impact on essential services connected to the internet, including hospitals and ambulance services.

A point of criticism against the European Union is that it didn't act quickly enough against the threat of cybercrime. Whilst it has dealt with cybercrime by passing laws against those who commit cybercrime, not enough was done to pre-empt such attacks. Therefore, it is most welcoming that the European institutions have agreed on supporting an effective implementation of the EU cybersecurity law. It adopts a six-way approach through Member States improving their cybersecurity capabilities, increasing EU-level cooperation, risk prevention, strengthening the European Union Agency for cybersecurity to better assist Member States, developing an EU-wide certification framework to ensure that products and services are cyber-secure and, finally, ensuring fast and coordinated responses to large scale cyber-attacks.

The European Commission has also proposed to create a Network of Competence Centres and a European Cybersecurity Industrial, Technology and Research Competence Centre to develop and roll out the tools and technology needed to keep up with an ever-changing threat. With over 660 cybersecurity competence centres across the EU, a wealth of expertise already exists in Europe. It is imperative that this expertise is used effectively.

Whilst this legislative model is being adopted, it is imperative that education takes centre stage. This should not be only done in the context of developing digital literacy and training youths on how to use internet wisely and safely. It is of course important that young people are able to manage their own security as well as being able to evaluate the sources as well as to know when it isn't safe to share information and how to manage data in a secure way. Youths themselves can be role models to others in discouraging negative behaviour as cyberbullying.

But young people should also be empowered with knowledge on how to respond effectively to cyber attacks. Generally speaking, internet users should know that common passwords for multiple accounts should be avoided. It is important that devices are updated with the latest cybersecurity measures.

Education is also important when it comes to informing users how to avoid being tricked into divulging personal financial information. For example, phishing remains an extremely popular method of identity theft. Divulging such information to cybercriminals may result in money theft or fraud. The fact that cyber-attacks are becoming increasingly sophisticated and more difficult to spot is another challenge.

Indeed, cybercriminals can be very creative in what information they can attain in order to access an individual's or an organisation's data. Sometimes, all that is required is a convincing phone call. Once inside the system, hackers will waste no time in finding and stealing confidential information. This means that, even businesses, should not limit themselves to just implementing new software or other IT solutions to strengthen their system. They should train their employees on the different types of attacks that exist and how to spot them.

To enhance Europe's cybersecurity also means increasing the trust of citizens and businesses given the level of concern that exists among both. We should also not forget that Eurobarometer figures show that 61% of Europeans worry that elections can be manipulated through cyberattacks.

With the recently approved Cybersecurity Act, the EU is sending the message that it is stepping up the fight to strengthen the bloc's cybersecurity efforts. Now it is imperative that this fight yields results and that our citizens and businesses across the EU are truly protected.

Cybersecurity standards are a priority!

Andreas SCHWAB

MEP (EPP Group), Member of the IMCO Committee

In 2019, the financial loss through ransomware worldwide will be more than 11.5 billion USD. Additionally, by 2022, more than 6 billion people will be potential targets of cyberattacks. At the same time, the number of job vacancies in the cybersecurity sector will triple. These numbers show the urgency with which the European Union and its Member States need to strengthen their cybersecurity capacities.

The adoption of the directive on security of network and information systems (NIS directive) in 2016 was a first step in the right direction and a turning point for the EU's efforts to step up its cybersecurity capacities. Before adoption of the NIS Directive, that I was rapporteur for in the European Parliament, cybersecurity was seen as an issue of Member State's competence. The NIS Directive is the first piece of EU-wide legislation on cybersecurity and it is the first time that Member States agree to address cybersecurity as a European issue.

As network and information systems are increasingly interlinked across borders, a cyberattack on one of these network and information systems can easily have European-wide consequences. The NIS directive therefore establishes for the first time, that a response to the threat of cyberattacks has to be a European response. The NIS directive lays down that essential services in sectors such as energy, transport, water, banking, financial market infrastructures, healthcare and digital infrastructure will have to take appropriate security measures and notify serious incidents to the relevant national authority.

This also concerns SMEs in essential sectors. For SMEs this can be a big financial burden. However excluding them from these responsibilities would present a loophole in the European cybersecurity infrastructure. The Connecting Europe Facility (CEF) programme is providing €38 million in funding until 2020 to support NIS directive stakeholders, such as the operators of essential services and digital service providers. This funding can help especially SMEs with their responsibilities.

In the long run, we have to ensure a rethinking however. Cybersecurity is not yet appreciated as a fundamental core value in the new digital economy. Digital innovation and cybersecurity seem to be at odds with each other, preventing the scale up of SMEs on the European market. However, digital innovation and cybersecurity can unlock more value when integrated. We should keep this in mind and make sure that SMEs receive the necessary support to thrive in the European market while ensuring a high level of cybersecurity for their services, not only in the essential sectors under the NIS directive, but in all sectors.

At international level, we have to note, that Europe is already behind. While the European Union wants to invest 1.8 billion € in cybersecurity by 2020 through public-private partnerships, the United States invest 18 billion € per year, 10-times as much. Also, 364 of the biggest 500 cybersecurity firms are nowadays situated in the US. We have to catch up and invest more, especially for SMEs that have a key role in Europe.

For a more secure environment for information transmission and consumers

Giovanni BUTTARELLI
European Data Processing Supervisor (CEPD)

With the increase in processing of personal data, we have seen too many massive violations of the fundamental rights to privacy and personal data. Many of these violations were the consequence of security failures. Since the full applicability of the General Data Protection Regulation (GDPR) with a comprehensive obligation to notify personal data breaches, the number of notifications has surged in some areas. As of February 2019, a total of 64 684 complaints have been initiated on the basis of a data breach notification, about a third of all cases reported by supervisory authorities.[1]. The numbers reported for the different EU member states may depend more on the reporting discipline in a country than on the actual state of information security. In fact, as the lack of information security may mean that breaches are not detected, low numbers of reported breaches may be reason for concern rather than for satisfaction. In any case, the number of notified breaches demonstrates that security violations for personal data are a problem of high significance, possibly causing significant harm for millions of individuals.

Public awareness of this problem does not directly prevent breaches, however, it enables us to monitor the developments. It will help the competent regulators, i.e. the data protection authorities, to invest their resources in order to address the most relevant problems and encourage controllers to implement effective solutions. For controllers, an effective breach notification system is an important element of their accountability measures. On the one hand, the need to admit failures publicly is an incentive to take efforts to avoid them; on the other hand, an effective internal policy to detect breaches provides a means to measure the effectiveness of an accountability system. For the citizens whose data has been compromised, the information about the breach may enable them to take mitigating measures as soon as possible, like changing passwords and PIN codes, blocking credit cards etc.

The obligation to notify data breaches is one building block in the GDPR system to ensure that controllers take full responsibility and implement adequate security. From a legal perspective, not only does an actual data breach constitute a violation of data protection principles, the failure to perform an appropriate risk assessment and implement the necessary safeguards and measures is in itself an infringement.

For decades, security experts have demanded "Security by Design", ever since the inherent weaknesses of many IT products were exposed by the first global security incidents, famous viruses and malware. They argued that all actors, from product designers and developers up to users, take their responsibility within the chain, especially because most modern technology is built as a stack of products relying on each other, and overall security is limited by the weakest link.

The EU legal framework embraces this approach. Security obligations are part of the GDPR (see Article 32), Directive 2016/680 and the new EUI Data Protection Regulation 2017/1725 as well as the specific instruments for police and judicial cooperation and the EU's large-scale information systems. The EDPS has explicit obligations to audit IT security in regular intervals.

An important aspect of information security and confidential communications is adequate and comprehensive protection of communications. As a rule, communications should only be readable by the intended recipient and verifiably convey the information the sender transmitted. The communications devices, protocols and networks must protect confidentiality, authenticity and integrity of communications. The data protection framework, as well as that of communications services have developed considerably in recent years, so that is high time to adapt the link between these two frameworks and adopt the ePrivacy Regulation. The current pending situation not only creates legal uncertainty for providers of communications services, but may also increase security risks for communications and data flows.

The importance of adjusting and completing the frameworks is underlined by the significant efforts that the EU has invested in the improvement of its instruments for information security and the growing cyber security acquis.

Another risk for information security and communications confidentiality comes from active attempts at undermining the security of systems for the purpose of covert surveillance. While some countries' administrations pursue such attempts, the resulting weaknesses in products and services affect everybody. Use of loopholes and backdoors is not limited to state services, but also serves fraudsters and other criminals. Illegal business opportunities abound: there are markets trading in knowledge about exploitable vulnerabilities in computer systems. The EDPS has warned the EU against permitting the creation and export of intrusive surveillance tools that build on such vulnerabilities[2].

Bold initiative is necessary to reshape this exploit economy, to direct the efforts of security researchers towards fixing the vulnerabilities instead of leaving them open for exploitation. To this end, we should oppose all demands for the creation of backdoors or limits to encryption strength, and stop government agencies from contributing to proliferating vulnerabilities by buying such exploits or the tools that abuse them. Instead, we should provide incentives for responsibly disclosing discovered security issues and protect whistleblowers who report them.

1 European Data Protection Board (EDPB): First overview on the implementation of the GDPR and the roles and means of the national supervisory authorities, report to the European Parliament LIBE Committee, 26 February 2019 at http://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/LIBE/DV/2019/02-25/9_EDPB_report_EN.pdf

2 EDPS Opinion 8/2015 on Dissemination and use of intrusive surveillance technologies

Big problem, little action Why cybersecurity is a top consumer issue

Ursula PACHL
Deputy Director General, BEUC

It has been said many times. Technology is changing the way we live. It changes our markets, our societies and how we interact with each other.

It is also changing the products we buy and the way we use them. Cars, baby monitors, fridges, toys, washing machines are now computers 'connected to the internet'. The nature of consumer products is changing: they are becoming a mix of hardware, software, data and services. And products are evolving all the time. Remote software updates can add new functionalities and result in a product becoming different from the one purchased.

Connected products can bring huge potential benefits. In terms of convenience for instance, consumers can now switch on the washing machine remotely to take advantage of cheaper energy tariffs. A smart thermostat can optimise your heating and allow you to save energy.–

But this is only one side of the equation. The 'Internet of Things' inevitably leads to an increase in risks and challenges. A connected product may invade a person's privacy. Unsecure products can be hacked and lead to theft of one's personal data, thus making people vulnerable to worries like credit card fraud. And there's the risk that people get physically harmed when safety is compromised by cyberattacks.

Our member organisations are constantly carrying out tests in order to give guidance to consumers when they want to choose a connected device. The results of their tests show that the market is swamped with products which pose big risks.

Test Achats/Test Aankoop from Belgium installed 19 popular smart devices, like alarm systems, a smart lock and a robot vacuum cleaner, in one apartment. It didn't take the two hackers they hired very long to find security flaws which, in some cases, even allowed them to enter the apartment.[1]

Unfortunately, children's products are among those most at risk. Consumer group Forbrukerrådet from Norway showed that strangers can seize control of smart watches and use them to track and eavesdrop on children[2]. UK consumer association Which? revealed that it was very easy to connect to a 'smart' toy to send a child a message.[3]

Consumers are usually not aware that a connected fridge or smart lock may lack basic cyber-security features and be prone to hacks. Worse, consumers would often not even know when a product has been hacked and is posing a – privacy, security or safety – risk for their owners

Laws not up-to-date

EU laws aren't fit to address these challenges. The lack of EU rules stipulating that products must be cyber-secure is a glaring gap to protect consumers. There is need for a horizontal cybersecurity legislation to ensure that all connected products being placed on the EU market are cybersecure.

Another major flaw is that the concept of 'safety', as enshrined in the EU's product safety legislation, is too narrow to adequately protect consumers from new problems which come along with internet-connected objects. This is because product safety is understood in the traditional sense only regarding their potential harm to consumers' health and their physical safety such as through exposure to harmful chemicals and injuries. What it does not capture are risks to our privacy or the digital security of our environment and devices – for instance a smart lock that can be easily hacked makes houses vulnerable to burglaries and intrusions.

In addition to the fact that the EU's legislation is not fit for purpose, authorities are not in a position and/or not motivated to perform effective market checks to keep dangerous unsecure connected products off the shelves. The lack of a state-of-the-art definition of 'safe' products means checks by authorities are not weeding out products that pose risk to consumers due to security flaws. Consumer groups' testing clearly shows digital products fly under the radar of market supervision.

Makes you WannaCry

This negligence and lack of action on making connected products more secure is baffling. The risks stemming from insecure connected products are not just problematic for consumers but also for society at large.

1 https://www.test-aankoop.be/hightech/internet/nieuws/slimme-woning

2 https://www.beuc.eu/publications/new-research-reveals-alarming-security-flaws-smartwatches-children/html

3 https://www.which.co.uk/reviews/toys/article/smart-toys-should-you-buy-them

The WannaCry ransom attack from May 2017 crippled hospitals in the UK and led to damages exceeding billions of dollars. Irrespective of the origins and way of dissemination of WannaCry, what the attack clearly showed was that it's too easy to play with our cybersecurity. Keeping millions of consumer products unsafe and prone to attack is a disservice to our society and our economy.

And the Cybersecurity Act?

In light of the risks it is disappointing that the recently adopted Cybersecurity Act falls short of making consumer products safer. It does introduce a cybersecurity certification scheme. However, companies are not required to get a certificate for their product – it is a non-binding scheme. The result is that unsafe toys, smart watches and routers can still end up on the market.

Policy-makers should adopt binding rules which require all manufacturers of connected consumer products to adhere to a minimum set of cybersecurity measures *before* placing their products on the market. These binding rules should at least include strong authentication mechanisms (for instance passwords), data encryption and making security updates available.

The Cybersecurity act has been adopted, what else can be done? Our member organisations will continue to test products, inform consumers and alert authorities when they discover grave security flaws. Other legislative tools – such as actions under the EU's Radio Equipment Directive – can help fixing some of the legal loopholes.

There is also movement at national level. The UK Government recently released a promising Code of Practice for Consumer IoT Security which sets out 13 practical guidelines for manufacturers and industry stakeholders to improve the security of their connected devices. Initiatives like this code are a welcome development. The European Union Agency for Network and Information Security (ENISA) can also play a leading role her in terms of providing guidance or a model code but more is definitely needed. Voluntary measures are not enough. There is a strong need for a binding legal instrument that makes sure that unsafe connected products are kept off the market.

Security in the digital age: can Europe hack it?

Cecilia BONEFELD-DAHL
Director-General of DIGITALEUROPE.

Security is like a chain and humans are always the weakest link. If Europe wants to be safe, it cannot tackle cybersecurity as a purely technological challenge. People should be the focus to improve awareness and skills.

As all things *cyber* are currently gaining traction amongst world leaders, they need to see the bigger picture and provide adequate incentives to create an enabling and trustworthy environment.

Cyber-attacks feature at the fifth place amongst the top ten risks to lookout for in 2019. In 2015, 19% of internet users were discouraged from online purchases because of security concerns. By 2025, fewer than 10% of internet users should be deterred from online purchases due to safety concerns. If Europe wishes to patch its vulnerabilities, deeper cooperation and coordination is needed.

"Europe's leaders should take the responsibility to build trust"

DIGITALEUROPE released its **Call to Action for A Stronger Digital Europe 2025** to envision Europe's next-generation challenges in the digital age.

Trust is fundamentally important as it is the glue that holds relationships together and features as a basic pre-requisite for a well-functioning and engaging democracy. Together, leaders from the EU, governments and industry can strengthen our common cybersecurity through information-sharing, best practices and a common approach.

Industry plays a vital role in harbouring cybersecurity and a secure infrastructure, and agile partnerships are key to fend off malicious cyber activities across borders.

By 2025, all large European enterprises should have a clear cybersecurity strategy. Efforts need to be made for SMEs to implement cybersecurity strategies by an additional 20%. In 2015, only 31.6% had formally defined their ICT security policy. On this matter there is a great variance with 72.1% of large enterprises having done so against only 27.1% of small ones.

"It is time to fill in the gap of cybersecurity professionals"

Everyone has a role to play, from private citizens, micro-enterprises to larger organisations. Cyber hygiene and awareness are critical to ensure an acceptable level of protection against cyber threats, both at home and at work.

To that end, education and skills form an integral part of the response. By 2025, Member States, universities and businesses should be training specialists for the most in-demand jobs, including cybersecurity. Additionally, Europe should strive to invert the increasing gap of cybersecurity professionals that it requires. As of now, the gap is expected to rise to 350,000.

Moreover, there needs to be far more inclusion to diversify the talent pool in the sector. Cyber threats do not discriminate against their targets and Europe should be able to benefit from the brightest minds to defend itself.

Ideas and initiatives need to be nurtured in a spirit of collaboration through the support of cyber competence centres across the continent. These valuable networks can federate research and align understandings on future solutions.

Europe should continue to adopt a multi-stakeholder and consensus-based approach to addressing security issues. As such, a growing number of stakeholders are adhering to the Paris Call for Trust and Security in Cyberspace.

Dialogue is a first yet vital step to promote responsible norms of State behaviour in cyberspace.

Europe has achieved many milestones in integrating cyber issues into its policy-making. Ever since the adopting of its first cybersecurity strategy, Europe has increasingly adopted ambitious measures to improve Europe's security.

It is now time for Member States to promptly capitalise on these initiatives and fully implement the NIS Directive.

"Europe must prepare for unified and coordinated responses to cyber incidents"

Relevant labelling schemes and standards on a given product, service or solution could provide basic guidance to users concerning acceptable levels of protection. Europe's cybersecurity agency ENISA currently has a solid mandate to ensure harmonised practices and facilitate cooperation with industry.

Businesses across various sectors need clear Code of Conducts to establish an agreeable baseline and complement the reach and scope of GDPR. Indeed, efforts need to be concerted to make GDPR fit for technological change.

Infamous cyber-attacks such as NotPetya and Wannacry have left Europe with a lot to cogitate on. A unified and coordinated response is what is needed to prepare, adapt and recover from future incidents.

However, human failings in security are nothing new. Almost two centuries ago, Europe witnessed its first major cyber-attack as bankers hacked a mechanical telegraph system. They bribed tower operators who encoded messages to share market information before it reached their competitors.

It was also apparent legislators had to adapt policy to tackle novel challenges. Indeed, at the time there were no laws addressing the misuse of data networks, making it hard to convict the Blanc brothers.

Leaders must devise future-proof policies that will allow European people to be safe and prosper. The ability for organisations to absorb shocks and recover make *cyber*-resilience the motto of today's interconnected world.

Cybersecurity: "work in progress"

Pilar DEL CASTILLO

MEP (EPP Group), Member of the ITRE Committee, Chair of the European Internet Forum

As we arrive to the end of the European Parliament's term, a multitude of events are taking place, and articles are written, with the objective of spurring the debate on what should the priorities be for the next legislature. My belief is that if there is to be one common denominator of the EUs "must do" list in all of these events and articles, that would be without discussion, security in general, and cybersecurity in particular.

This, however, must not be interpreted to be caused by the inaction of the EU institutions during the current legislative term; quite on the contrary, a great deal of important initiatives have been adopted, such as the security provisions of the Electronic Communications Code or the very recent Cybersecurity Act. Nevertheless, if we are truly to be efficient in cybersecurity matters, we must avoid being self-indulgent. Cybersecurity must always be understood as "work in progress".

Indeed while our daily lives and economies become increasingly dependent on "digital", we also become increasingly exposed to cyber threats, making cybersecurity vital to both our prosperity and our economy. However, the cyber threats are just as dynamic as the digital transformation.

Clearly, the "Cybersecurity Package" by building upon existing instruments and presenting new initiatives, will further improve Europe's cyber resilience and response to security threats. Indeed, ENISA, Europe's cybersecurity agency could no longer function properly without a permanent mandate and we must strengthening operational cooperation and crisis management across the EU.

In addition, we have created a European digital security framework, which will help develop measures on cyber security standards, certification and labelling to make ICT-based systems, including of course Internet of things, without undermining the principles of transparency and openness that already today govern standardisation processes.

Nevertheless, particular attention must be paid to the fast evolving cyber threat landscape that accompanies the digital transformation of Europe's economy as the Internet of Things, smart infrastructures, connected cars, digital health and eGovernment applications are massively deployed.

One very recent example is the attention that has been given to a specific international tech vendor, and the ban that the United States, Australia, New Zealand and Japan have issued to this particular company from taking part in the building of in 5G mobile network infrastructure.

In my view, and without pre-empting the result of the debates that are taking place in Parliament and the possible resolution that will follow, our actions in this field must be balanced and extremely rational.

Clearly, we must deal with the technological security risks posed by increasingly high market penetration of external vendors at EU level by means of a common approach based on the effective and efficient use of expertise from within the Member States and industry. However, we must do so with all the facts and the best professional expertise possible. As I write these lines the UK, Germany and France have not yet published any definite conclusions.

From this perspective, and while we instruct security experts from the European Commission and the Member States to undergo a thorough analysis of the situation, we must not forget that a competitive, dynamic market for telecom vendors is in the strategic interest of Europe. Having a broad choice of suppliers is essential to ensure they compete on quality, reliability, and of course also in the security of the equipment.

In the meantime, the Union needs to continue to drive the cybersecurity agenda by supporting cybersecurity across the entire value chain, from research to the deployment and uptake of key technologies. In this regard, proposals such as the Digital Europe Programme, which, if Council agrees, will earmark 2 billion euros for financing state-of-the-art cybersecurity equipment and infrastructure, will undoubtedly play an important role.

In addition, the EU must continue to support public private partnerships that are able to stimulate the competitiveness and innovation capacities of the industry to ensure that there will be a sustained supply of cybersecurity products and services. Let us not forget that industry standardization bodies, such as the 3GPP, have already approved security standards for 5G and are further working on future standards.

Lastly, and here there is a great deal of room for improvement, as the latest development with regards third country vendors has shown, cybersecurity requires essential policies, and global cooperation. Europe cannot go about it alone, it is very important to work together with international partners and create initiatives by building a mutual and international consensual regarding an open, interoperable, secure and reliable cyberspace.

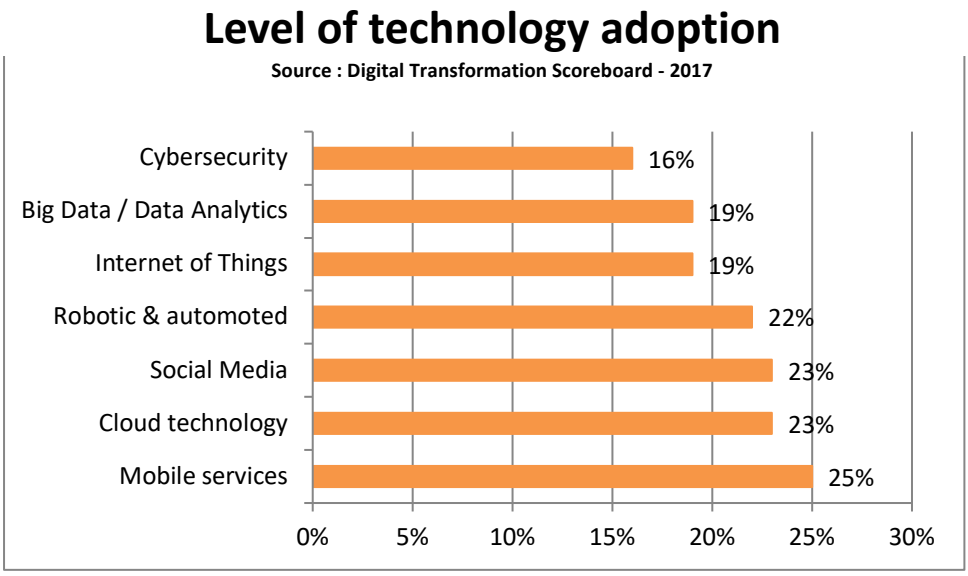
In this regard, international cooperation must strive to: Develop international norms of behaviour in cyberspace; Promote compatible policies with our international partners; Promote collaboration in cybercrime investigations; Create International cybersecurity capacity building; Secure infrastructure and devices; And secure online safe, trustworthy transactions not hacked or impersonated.

Indeed, "work in progress".

The success of the digital transformation of organisations will require cybersecurity

Nicolas ARPAGIAN

Director of Strategy and Public Affairs, Orange Cyberdefense



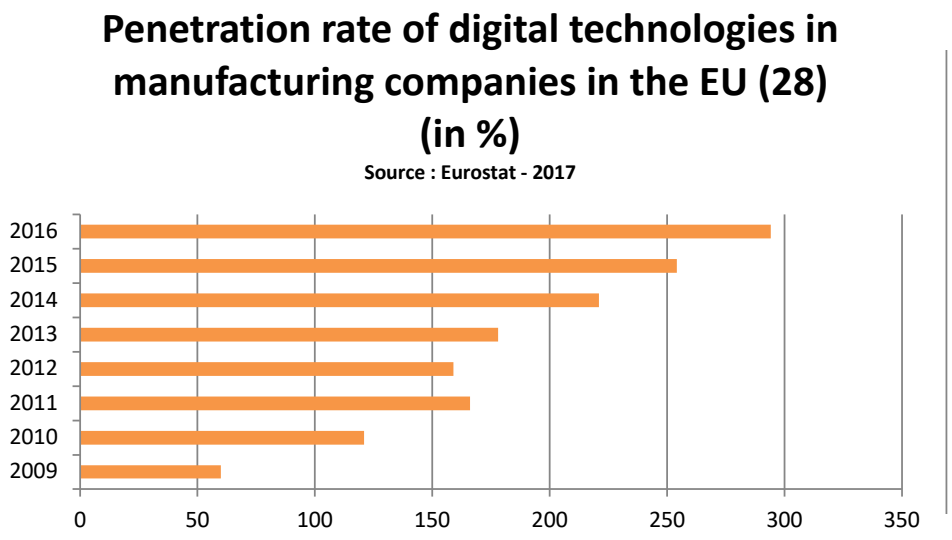
Digital uses shape our way of producing, consuming and trading, as well as manipulating our uptake of knowledge before we make decisions. This digital intensification of both our personal and professional lives is being seen continuously in regard to the technology that is ever-present in our daily actions. We take control of these tools, which were designed for intuitive use shaped by the careful observation of our behaviour. Above all, such designers are looking to enhance the availability, reactivity and fluidity of the uses of digital information: ensuring that any technical limitations diminish, in favour of features which help and facilitate interactions between people, companies and public authorities. This ever-increasing integration of technologies of information has been identified by the authorities of the European Union, as a priority, also to support growth, jobs and competitiveness at a global level. They are seeking to ensure that this digital up-take is smooth and efficient within the 28 Member States.

This digitalisation certainly achieves value creation, but is also likely to find itself weakened by insufficient consideration of cybersecurity criteria. This is crucially the case when equipment falls victim to hacking and when this is organised in succession in order to maximise the effect on production lines, financial exchanges or the activity of public services. This digital exposure is all the more important in the industrial sector, which has in the past few years, been making up for lost time in terms of computerisation and is making use of more and more robots in its production lines.

According to the International Federation of Robotics (IFR), the sale of industrial robots will increase on average by 14% per annum in the years between 2019 and 2021. In the year 2018 alone, the industrial companies acquired some 421,000 new robots. This represents an increase of 10% in comparison with 2017, which had already been a record year with its 30% increase against the year before.

Security measures supporting digital transformation

A country like France has 137 robots for 10,000 employees; in South Korea, the figure is 710. It is in this context that the Orange Cyberdefense experts have been active within companies since 2013, initially in major companies and increasingly in small and medium-sized enterprises, to support the security



measures of the digital transformation of these organisations.

Relying on a considerable number of facts found during hundreds of audits carried out in the industrial sector by Orange Cyberdefense since 2013, we have established a ranking of identified weaknesses in terms of digital security.

Number one rank weakness identified would be taken up by the lack of detection capabilities. This prerequisite evidently limits the capacity to evaluate the very principle of possible security breaches of the company. The lack of hardening of the information systems is the second point of weakness of industrial organisations which too often insist on using basic solutions without particular precautions, such as encryption, for example. The same is true of the frequent use of Operating Systems, protocols and unsecured firmware. In any case, the management of human–computer interaction control procedures leaves you wanting more. For that reason, the continuous connection of the said Human-Computer Interaction (HCI) is generally the rule, without any real reflection in regard to the management of such practices. This culture of sharing information is a decisive step towards greater security. In benefitting from the experiences of one's peers, we are able to angle our strategic choices more effectively. This assistance is very valuable in a context where pending decisions are made in a changing and often unstable environment. This is the reason why Orange Cyberdefense prefers to take a partnership-based approach which gives its major customers the opportunity to exchange ideas peer-to-peer in order to share their expertise.

Integrating security measures as early in the process as possible

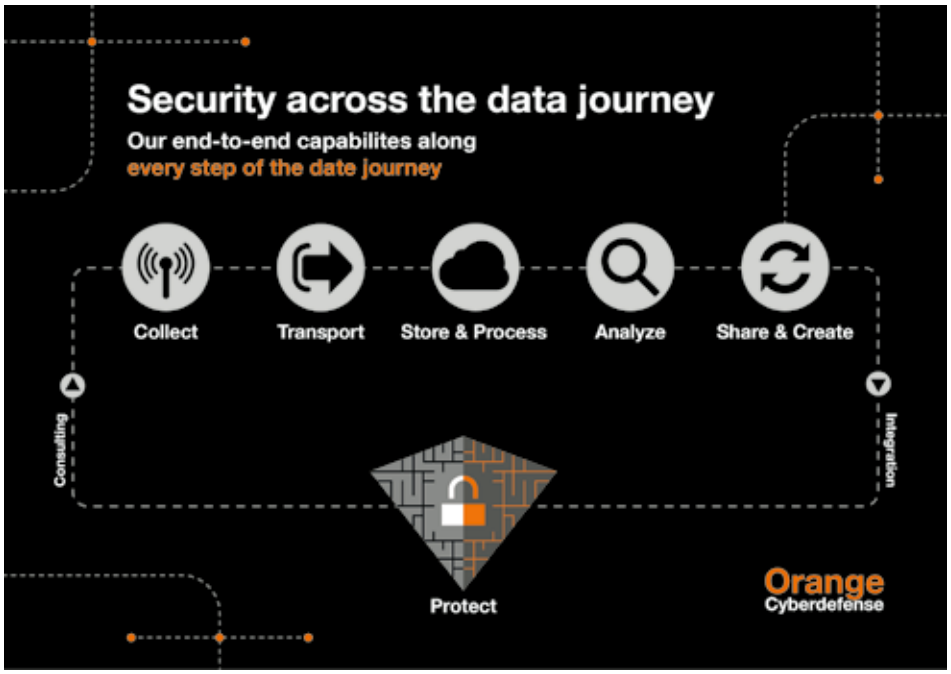
In order to support this unprecedented economic transformation, companies must be able to rely on advanced consulting and reviewing skills despite the diversity of technological delivery specific to each business sector. It is also necessary to have a good command of the legal context in order to ensure the compliance of very demanding texts such as the EU General Data Protection Regulation (GDPR) or the Network & Information (NIS) Directive. This makes it possible to advise on technical choices in the best possible way so that compliance process does not affect the competitiveness of companies. It is also important to increase the overall awareness, competencies and security level across the European Union, reason why the Cybersecurity Act recently adopted at EU level is welcome.

In terms of cybersecurity management, one must be in the position of guaranteeing availability, integrity and interoperability of the data which is collected. We ensure that we are present at each stage of the production cycle and exploitation cycle in order to verify in particular compliance with rules on data protection.

Monitoring for early detection of & response to attacks

Thanks to monitoring tools, notably nine Security Operations Centers (SOCs) which are spread across the world, we are able to ensure constant monitoring of companies' computer equipment. Something to react as quickly as possible when unusual behaviour is detected: machine learning tools are fed continuously by the mass of technical information gathered on the infrastructure of companies. This artificial intelligence assists analysts by developing response scenarios. Its algorithmic capacity ensures an exploitation of these billions of security events. This analysis is equally powered by all technical signals recorded on the telecom network of the group Orange. This presence on a global scale provides an unparalleled basis for observation among security service providers. The sharing of information via the international alliance of Computer Emergency Response Team (CERTs), which Orange Cyberdefense is part of, usefully completes the decryption grid for malware in circulation. For this reason, the work of the epidemiology lab and of Signal Intelligence of Orange Cyberdefense adds a rare expertise in regards to the analysis of malicious software. Like medical teams specialising in viruses, in the long-term they study these aggressive programmes in different technical environments. This is done in order to understand their characteristics and the intentions of their developers: this empirical approach is useful in identifying attack strategies used by the hackers. Their classification, informed by this analysis of the laboratory's experts, reinforces their ability to anticipate digital aggressions.

This expertise is gathered so as to act as early as possible before a cyber-attack begins or in order for measures to be taken early enough to limit its impact. If the crisis couldn't be prevented for technical reasons or because the company didn't use sufficient protection devices, it is the responsibility of incident response specialists (CSIRT, Computer Security Incident Response Team) to be available to intervene as quickly as possible in the case of emergency regardless of the geographical location of the body in question. This ability to mobilise experienced practitioners to intervene as quickly as possible and take appropriate action to protect the client's interests, preserve evidence and promote a return to normality is a major differentiating factor in choosing one's cybersecurity partner. Orange Cyberdefense is particularly dedicated to ensuring this service, which supports decision-makers and companies at a time when cyber-attacks are at their most destabilising. Being the trusted partner in the service of protecting the essential data of companies is certainly part of Orange Cyberdefense's missions.



Multi Stakeholder Participation to Lead European Research and Innovation for Cybersecurity

Kees VAN DER KLAUW

Chairman Management Board, Alliance for Internet of Things Innovation

The importance of cross-disciplinary, multi-stakeholder approaches in research and innovation is often undervalued. Most research and innovation programmes are still conducted in relatively isolated silos. While this may be appropriate for deep research, creating fundamental knowledge, technologies and methodologies, a reliable a and trustworthy cyberspace for Europe and its citizens requires a more integrative approach.

Traditionally, engineering education focused on creating functionalities, i.e. what systems can do. For many years competition in the market was based on adding more functionalities and performance while reducing cost. With the advancement of electronics and software many functions have become commodities in a very competitive global landscape.

Even though new functionalities are still on the rise, particularly based on connectivity, data and artificial intelligence, there is a growing attention for so-called non-functional characteristics of complex systems, i.e. how systems do things. This particularly relates to growing concerns regarding reliability, security and privacy matters.

While functionalities are becoming commodities, it is the non-functional characteristics of these systems that will allow differentiation.

Cyber security is one of the major requirements for the Internet of Things. Devices and systems will become massively connected and this fact introduces a complex security challenge that cannot be handled with a single approach. End-node devices, that generally have a low energy, memory and computing footprint and may reside in remote or difficult to reach areas need to be secure. Networks (wired or wireless) for communications need to be secure. Aggregation and control nodes need to be secure and algorithms running on them need to be secure. Cloud services need to be secure. All systems, communications and their data need to be secure. And those systems will need to be updated in a secure way with new, secure software for functional and non-functional reasons.

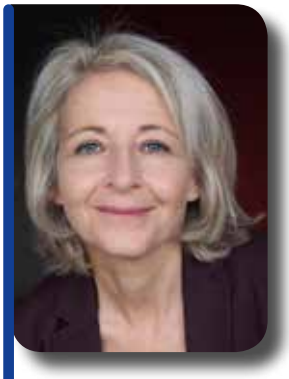
Unfortunately, a system of secure components does not imply system security. Nor does a system of secure systems imply security at the highest level. And even a secure technical system on the highest level may still be at risk because of human behaviour, intentional or unintentional. Even security itself needs to be secure. This requires addressing processes in addition to architectures and technologies.

Thus, establishing cybersecurity requires a multi-layered and multi-disciplinary approach building on expertise in individual areas. Component research, embedded software research, systems engineering, data science, and research and innovation in cloud systems and services should team up to take a holistic perspective in security in an end-to-end approach. Researchers and research programs with those wide scopes will be essential. Interestingly, artificial intelligence systems will support those researchers in integrated design, verification, validation and monitoring of systems and their security.

However, a multi-disciplinary approach is not only of technical and rational nature, but also has non-rational elements that are important for creating trust with users of cyberspace and cyber physical systems. This is closely linked with perceived cybersecurity. Secure systems may still be perceived as insecure and the other way round. This will have a strong impact on the adoption of these systems. Therefore, and to include the human factor in cybersecurity, participation of socio-economic and behavioural researchers as well as representatives of end-user groups in society is essential in research and innovation. And systems should become transparent and explainable to users, not only to experts.

Not everyone needs to engage at every stage in the process, but an integrative approach is increasingly important for many digital innovations and specifically for cybersecurity. The Alliance for Internet of Things Innovation (AIOTI, www.aioti.eu) was established a few years ago to take such approach. AIOTI features working groups on horizontal, common matters such as technologies, standards, interoperability and policies while taking an application perspective in many domains such as smart cities, farming, industry, buildings, mobility, energy, water... The implementation of technologies in those domains requires to talk 'domain language' and be involved in practical cases and AIOTI plays that bridging function via its members in several European programs, Large Scale Pilots and Innovation Hubs. Contributing to an innovative and secure Europe.

A global strategy for cybersecurity in Europe, competences and investments



Laure DE LA RAUDIÈRE

Member of the French Parliament and Co-rapporteur of the Assemblée national Study Group report on « Blockchains, a matter of sovereignty »

Companies, administrations, citizens, public services, infrastructures... the whole society is nowaday connected to the Internet. The boom in connected objets and the increasing use in Artificial Intelligence will reinforce this trend. No activities will anymore be independent from the Internet! The digital era is bringing astounding progress and opportunities, but such an almost total dependency carries new risks.

How to protect ourselves against threats such as the theft of data, espionage, manipulation of public opinions, the takeover of infrastructures or the blockading of public services? In otherwords, how to prevent from a massive disorganisation of our society?

First, we need to educate. Starting by teaching our kids to use the Internet safely, to identify malicious sites and frauds, to change regularly their passwords or to protect their personal identities on social networks... Raising awareness of adults is also a priority because cyberattacks to individuals are growing. Techniques of self-protection must be spread to the general public to promote a citizens' empowerment in cybersecurity. Citizens urgently need to adopt safety attitudes. Information and prevention must be promoted to all.

Companies and administrations must also become more aware of the cybersecurity threat, since they are first-choice targets for cyberattackers. For years, the issue of cybersecurity has been the competence of directorate for Information Services in big companies or big administrations. But since recent attacks with huge damages - such as the WannaCry virus in 2017 - the cybersecurity issue is becoming more often a prerogative of Strategic Committees. Yet, SMEs are vulnerable to these attacks because they have less resources to implement strong means of self-protection. Greater public support is therefore needed.

Second, it is essential to developp numerous and specific competences. States must invest in trainings of cybersecurity. Today, all of them suffer from a huge gap in qualified human resources to adress the issue of « Security by design ». As an example, France should make greater use of its unique network of « digital schools », in coordination with the *Grande école du numerique*, the national agency in charge of supporting the development of schools delivering digital trainings. These schools are spread all over the territory and are flexible enough to implement new trainings efficiently.

The fight against cybercriminality requires recruiting a large number of experts in cybersecurity to help all stakeholders to protect themselves. This is new jobs that should be attractive for the new generations of people who are born in the digital era.

In the field of cyberdefense, the French Minister of the Army has just launched the creation of a « cyberarmy » in January 2019, by recruiting 1000 extra « cybersoldiers » until 2025 and by allocating a budget of 1.6 billions euros to the fight in the cyberspace.

Third, the fight against cybercriminality calls for strong investment efforts, to support innovation in cybeprotection devices and services. Commission's proposal for a European Cybersecurity Competence Network and Centre is an important step for the development of a competitive European cybersecurity industry. Not only this is an economic issue in a fast growing market but also an issue of sovereignty to avoid any dependency from third parties in terms of cyberprotection.

The increase and sophistication of cyberattacks further calls for strong support in research and development. The *blockchains*, a subject for which I have been co-rapporteur of a report from the French Parliament[1], is an interesting technology that could help fight certain types of cyberattacks.

The principle of decentralised and shared management of *blockchains* and the guarantees it offers - integrity, confidentiality, traceability, authenticity of the data - could help protecting identities, integrity of data and infrastructures. More research in this fiel is nonetheless necessary before talking of a revolution of cybersecurity by the *blockchains*.

Finally, we must strengthen our cooperation. All these initiatives would have the effect of a sword cutting through the water without a common strategy and a pooling of resources at the European scale. Because this threat is global, powerful and dematerialised. Perpetretors of attacks are not always idenitified, but this war takes place obviously in the context of a strong global competition, both from an economic and a diplomatic point of view. Industrial spying and cases of interference during elections through the manipulation of the public opinion on social networks (ex. during the Brexit campaign) are telling examples.

The resilience of the European states against this challenge represents an issue of sovereignty. We need to protect our citizens, our companies and our political institutions. But also our values. Promising initiatives have recently been untertaken by the European Union, such as the Cybersecurity Act, and must be key priorities for the next European Commission.

1 Information report, Assemblée nationale, French Parliament, on *Blockchains*, n°1501, 12 decembre 2018 : http://www.assemblee-nationale.fr/15/rap-info/i1501.asp#P732_249058

Cybersecurity for space activities

Eric MOREL DE WESTGAVER

European Space Agency, Director of Industry, Procurement and Legal Services

Massimo MERCATI

European Space Agency, Head of the Security Office

The global security framework is evolving. With hyper-connectivity and the revolution that the internet has brought to society and the global economy, a new threat has emerged, now omnipresent, and to which societies must adapt and respond: cyber threats. These cyber threats are now at the core of another multidimensional phenomenon: hybrid threats. Building strong and resilient cyber security has thus become a worldwide priority, particularly in Europe, an issue recurrently addressed directly by European Heads of State and Government and the European Parliament alike.

Space assets are an integral part of Europe's economy and security: our reliance on space data makes space infrastructure a primary target for any adversary. In an increasingly unpredictable and contested strategic environment, satellite infrastructure can be either a target in themselves, or a link in an attack against a third party, or even simply a collateral damage. Regardless, the real impact is on its users: firms, banks, critical infrastructures, public services and institutions, unmanned vehicles, etc. that also rely on unhindered space-transmitted data.

A space or ground segment of a system can be spoofed, jammed or hacked. Such cases have occurred on two earth observation satellites operated by NASA, Landsat 7 and Terra, hacked in 2007 and 2008 via a rogue signal relayed by a satellite station located in Europe. In each instance, the attacker achieved all steps required to command the satellite but did not issue commands. More recently, on 7 September 2018, Florence Parly, French Defence Minister publicly declared that France's governmental satellite communication asset, *Athena Fidus*, had been spied on by *Louch-Olymp*, a Russian governmental satellite. Minister Parly further suggested that this eavesdropping spy satellite had then been observed as it manoeuvred to monitor other space assets. This is the reality of space today.

The information and data managed, collected, maintained and cured by the European Space Agency (ESA) is of critical value. A space programme's security objectives are to safeguard data integrity, data availability and data confidentiality. In short, cyber security aims at getting the right version of the right information in the right form to the right person at the right time. ESA, as Europe's intergovernmental space agency, is a decisive link in the chain of the overall cyber security continuum and is bound - as one of the world's most significant provider of satellites and data - by an answerability towards the protection of our Member States' investments.

Managing cyber security risks is a holistic, integrated process. The key aspects for an organisation such as ESA are its ability to create a secure environment for the design and development of space systems. This entails having an efficient security governance framework, performing risk analyses and threat assessments as baselines to steer security decision, owning the capability to monitor and control threats and vulnerabilities and finally reacting to these with the appropriate countermeasures. In a cyber security context, the effectiveness of countermeasures greatly relies on the ability for a Security Operations Centre and of a Computer and Communications Emergency Response Team to work in complete synergy. In addition, a robust accreditation of space systems must be performed in compliance with existing security requirements.

ESA's cyber security activities are all-encompassing, ranging from regulatory adaptations, mission-specific requirements, IT security, dedicated studies of an R&D or operational nature, training, thanks to ESA's cyber range located in the European space Security and Education Centre at Redu in Belgium, to the development of partnerships, such as the ones ESA develops with the European Defence Agency or EU Satellite Centre.

All domains of space technologies need to be covered. Indeed, developing "protected" signals in space able to ensure that satellite navigation services are resistant to cyber threats like spoofing and jamming, are critical to protecting *e.g.* mobile and unmanned vehicles. In addition, satellite imagery and its derived products need to be transmitted to critical users by secure telecommunication capabilities. Every space-reliant application needs to be monitored and controlled from an infrastructure vulnerability point of view, which begets the need to have a European security operations centre capable of providing users with the adequate cyber services they require.

As the developer and user of strategic space networks, ESA is but one of the never-ending links in the cyber security chain and is at the forefront of cyber security and thus continuously adapts and upgrades its capabilities, policies, regulations, in order to face any type of cyber threat. In order to go further, security improvements and activities will be part of the proposals ESA expects to present to its Council at ministerial level in November 2019, in Seville, which could be instrumental in effectively tackle the breadth of the issues linked to an effective ESA cyber response while developing a vision and a policy for further supporting and protecting citizens, industry, and Member States alike.

International cyber security: why is there an emergency!

Guillaume TISSIER

Heads CEIS, strategic and risk management consulting company. CEIS is one the organisers of the International Cyber Security Forum (FIC).

What can the 51 signatory states of the Paris Call, launched by President Macron on November 12 2018, for trust and security in cyberspace, do while the United States, China, India, Israel, North Korea, Russia or even Iran did not deign to sign the text? Not much, at this point. Nonetheless, the Paris Call is an essential step in the long road that will lead us to the creation of an international system of a collective international cyber security which can be the only guarantee of a sustainable "digital peace". But it is now necessary to make some rapid operational progress in order for it to not remain purely incantatory.

Actually, the French initiative responds to two emergencies.

On the operational side, the Wannacry and NotPetya attacks sounded like wake-up calls, showing the systemic impacts that cyber-attacks could bring, and emphasizing the need to strengthen international cooperation between states, but also between states and companies and between companies themselves. Recently, the attacks on the DNS system (management of domain names) were a new alert: whether it is the addressing system or the road exchange protocol between routers which are making able the connection between different autonomous systems (BGP), the infrastructures that constitute the heart of the Internet are largely vulnerable. As all collective systems are first based on common standards definition, it is therefore essential, after the failure of the last negotiations of the Governmental Experts Group working under the authority of the United Nations, to revive the discussions on behaviour standards of public and private actors on the Internet by closely associating companies. From this point of view, the French initiative has scored points since it has rallied many companies, as digital giants (Microsoft, Facebook, Google, IBM, Kaspersky Lab, HP, Samsung ...) or vertical actors (Enedis, Airbus, Lufthansa ...) to the cause.

Politically, it was also urgent to make France a major actor in "digital diplomacy". Beyond the operational challenges, digital technology has indeed become a political "object" in its own. As Russia pushes at the UN a project of a convention on the subject, numerous private initiatives, such as the Charter of Trust launched by Siemens or the Tech Agreement promoted by Microsoft, appear and resumption of discussions should take place at the UN in June 2019, a unifying initiative involving public and private actors was needed. After this first step, it remains to put quickly into practice some of the 9 principles contained in the text thanks to some "quick wins". Among the work areas: the integrity protection of the "public heart" of the Internet, the cooperation in the prevention of interference in electoral processes, the better integration of digital security for products and services...

In order to succeed, the exchanges will have to avoid any Manichean vision of the subject.

There are not the "victim" companies on the one hand and the "guilty" states which would threaten, with their cybernetic bellicosity, the digital security and, consequently, the world economic prosperity, in the other hand. It is true that companies are the first victims of attacks, whether they are launched by states or non-state actors. The new empires of the GAFA also play an increasingly key role in world peace and stability, sometimes against their will. For example, never their influence on public opinion has been so important. But while globalization has further diluted state sovereignty, states still remain, to this day, the only guarantors of international stability and, for at least some of them, a model of a democratic society.

Likewise, to summarize the current debate by an opposition between those who are for a "global, free and open Internet" and the supporters of a hard policy aimed at restoring the sovereignty and the States control over their portions of the Internet, between virtuous countries, defenders of digital peace, and rogue states, cantors of the cyber war, is a bit short. Like Estonia, Iran is one of the countries that have experienced an attack on its critical infrastructure ... In geopolitics, there are only states seeking to promote and defend interests, often divergent. On the one hand, the United States are seeking to maintain its hegemony and now openly claim, even in the digital domain, their opposition to multilateralism that could weaken their power. On the other hand, China and Russia, for whom digital technology is a fantastic means of technological and economic catch-up, do not intend to restrict their capacity for action. Between the two, a Europe, still Lilliputian numerically, who chose the path of "law" to regain some of its sovereignty, largely dissolved by its dependence on GAFA and its de facto submission to the US law extraterritoriality. Hence the European Regulation on the protection of personal data, the Privacy Shield, the debates on the "GAFA tax" and now the Paris Call. It took two world conflicts for the League of Nations and then the UN to be created. We do not have to wait for an international cyber-attack to lay the foundation of a collective cyber security system.

Blockchain and Cybersecurity: what role for the Postal Operators?

Alain ROSET
Blockchain & Traceability Director, La Poste

The distributed ledger technologies / blockchain are full of promises including in the cybersecurity fields. Its resilience, its tamperproof, its distributed architecture, may effectively consolidate some cybersecurity functions. La Poste[1], as an operator managing thousands of employees with a close contact with all the French citizen, is also sensible to the human factor in the security of any digital system. Furthermore, we have to keep in mind that the actor's identity in a digital system establishes the base of the security of any interactive digital services and their control must be operated together in compliance with the General Data Protection Regulation (GDPR) and the framework of some specific markets, like the banking operations.

The blockchain systems are based on a structure of data representing transactions grouped in blocks interconnected by cryptographic functions. This write-only database is controlled and stored by a network of peer-to-peer nodes under the authority of several stakeholders. The governance of this peer to peer network is built on-chain with software services to organize the consensus on the content of a new block of data to add to the chain and off-chain by explicit or implicit covenants applied by the stakeholders.

The advantages of the Blockchain based systems result from these intrinsic characteristics:

- Resilience and immutability because of the mix of cryptographic functions and decentralized independent nodes network, which means that any change is visible by the all the members of the grid and the corruption of the data go through the necessary corruption of a large part of the nodes.

- Transparency and auditability by the large distribution of the data among several nodes.

Since their first implementation (Bitcoin January 2009) these technologies have been significantly improved in 2014 (Ethereum's launch) with the introduction of modules of software ("smart contract") as the pieces of data managed by the network. The smart contracts have the same characteristics: immutability, tamperproof, transparency, and resilience.

The introduction of a blockchain into a digital system may therefore improve the global security of the services by easily supporting some cryptographic functions like Zero Knowledge Proof. This would allow the dissociation of the data and the proof of some assertions based on these data. In complement, some multisignature systems avoids tracking of the activities of one user or the risks of a single user corruption of a blockchain system.

In addition, the decentralization of storage possibility coupled with the logical centralization of the proof of correctness of the data applied to any data may abstain from central storage of such data eliminating any risks of corruption, of hijacking. In the case of document certification, the usage of a statement is thereby certified by the electronic signature of a reputable entity and by the immutable encrypted storage of the proof of exactitude of this data on a public blockchain.

The decentralized execution of the smart contracts on a multiple nodes network with the guaranty of the blockchain allows the interconnexion of silos of data split in various entities, while keeping the self-government of each digital system, while logging a notarization of the interfaces. These architectures simplify the overall security analysis of the interconnected systems by placing a secure trusted module as common interfaces. This technology opens the way for the successful automatization of processes split over several firms as it is often the case for structures of markets operated by postal operators (parcels networks, banking markets for instance).

However, a blockchain system has some drawbacks such as the scalability, computer's power for cryptographic functions and the quality of the external information collected to validate the transactions Thought, we can imagine that the multiple research teams will rapidly overcome those challenges.

For La Poste, the most difficult issues will revolve around the empowerment of users (employees and further citizens) in decentralized architectures of data. Indeed it requires not only a long training of individuals, but also the development of user-friendly interfaces and to wait for generalization of specific hardware secure elements inside the smartphones. The historical role of trusted service providers of the postal operators remains essential except that skills have to be adapted to match the blockchain technologies: for instance, with the help of the networks of the postmen and the post offices, the proof of the multiple information injected in the transactions of a blockchain may be secured.

To conclude, Blockchain technologies contribute to securing interconnected digital systems through a new type of decentralization of data and processing. Nevertheless, La Poste does not forget on the one hand a necessary holistic approach of the security of a system and on the other hand the empowerment of end users which is essential to achieve the promises of the blockchain pioneers. The postal operators, through their frequent contact with all citizens and SMEs in a country may act as enablers and authentication entities for sensible data. They can ensure the correct identification of stakeholders for a given digital services, reducing the fraud, the hijacking risks or the fake news propagation.

1 The French postal operator

Blockchain: security by design, enabling new trust models

Luca COMPARINI

Responsible for the Blockchain Business at IBM, France

Cybersecurity best practices are continuously evolving to cope with the latest threat landscape. Creating impenetrable systems and relying on defensive structures to prevent intrusions is no longer a sufficient approach. Today, integrated security systems that are designed to help keep organizations safe from threats must be combined with proactive threat intelligence and cognitive risk management.

New technologies (think mobile apps, cloud…) often play catch-up with security best practices as they emerge through their early adoption phase. Blockchain technology, on the other hand, comes into the tech landscape with a bit of a leg up in terms of security; its main design point is to build trust and security for the information and processes held within it. By decentralising the information flow and using cryptography to prevent data tampering, blockchain can help mitigate threats to organizations. Organizations must apply the lessons learned from previous technologies and ensure that the supporting infrastructure of a blockchain implementation receives through security design and testing.

Blockchain is increasingly being deployed by organizations worldwide, including IBM. It enables users to share transaction information and business logic, which cannot be changed after it's been entered into the blockchain, making data more trustworthy and reliable, and providing three elements that help reduce cybersecurity threats.

1. Indelible notarisation based on provable data integrity: each block of the ledger embeds a "cryptographic picture" of the previous. A malicious attempt to modify the past would result in a mismatch between the indelible picture of its original state and the altered block. This chaining mechanism guarantees that a counterfeited vision of past data is exposed to all on the network and automatically discarded.
2. Non-repudiable proof of liability: each event written onto the ledger is digitally signed by a unique identity associated with each peer on the network. The content can remain private by using Zero Knowledge Proof technologies. The evidence of proof is also encoded, which makes blockchain a trusted digital notary of "who said what, when".
3. Fault tolerant consensus: the dissemination of the information or value relies on consensus mechanisms designed to protect the network against crashes, latency, ordering issues, "byzantine" attacks and distributed denial of service (DDoS) attacks.

Cryptocurrency is one application of blockchain. When a party wants to send money directly to another entity without the use of a centralized third party, there needs to be a record of that transaction that cannot be changed by anyone. Blockchain works in cryptocurrency because intermediaries are not needed to move things back and forth and transactions cannot be changed once written to the chain.

Enterprise blockchain, on the other hand, goes well beyond cryptocurrencies and tokens. Blockchain-based networks for the enterprise offer the opportunity to develop new business and trust models based on multiparty collaboration and process automation across organisational silos.

Blockchain can help improve the efficiency of existing process flows involving multiple parties, and minimizing disputes with a single view of the truth.

Blockchain is becoming the foundation for digital supply chains, empowering multiple trading partners to collaborate by establishing a single shared view of transactions without compromising privacy or confidentiality. Examples include:

- TradeLens, already in use by more than 100 organizations across the global shipping ecosystem, is the result of a collaboration agreement between Maersk and IBM to jointly develop and bring to market a blockchain-enabled shipping solution designed to promote more efficient and secure global trade. The platform brings together various parties to support information sharing and transparency and spur innovation in what has traditionally been a highly manual industry. Carriers, freight forwarders, port and terminal operators and customs authorities around the world can interact more efficiently through real-time access to shipping data and shipping documents, including IoT sensor data ranging from temperature control to container weight.
- IBM Food Trust is a blockchain-based network offering participating retailers (including Walmart and Carrefour), suppliers (such as Nestle, Unilever and Dole), and growers access to data from across the food ecosystem to enable greater traceability, transparency and efficiency. Using blockchain, in the event of a contamination and ensuing recall, food can be quickly traced back to its source in as little as a few seconds instead of days or weeks.

As well as supporting traditional business processes, blockchain can also fuel new business and service models that have not been invented yet.

A notable example is we.trade, originally conceived by a group of seven banks working in collaboration to develop a shared platform to make trade finance accessible for European small and medium-size businesses based on distributed ledger technology. Since the first deployment in July 2018, we.trade has accelerated the development of its platform to 14 banks across Europe. Recently, we.trade announced they are interconnecting with eTradeConnect in Asia extending the combined network to 26 banks.

With more than 500 blockchain projects globally, IBM is engaged across all industries, where European projects in particular are on the rise. According to IDC, "blockchain spending in Europe is now growing faster than anywhere else".

Cybersecurity

Horizon 2020 pilot projects

to prepare a European Cybersecurity Competence Network
& contribute to the European cybersecurity industrial strategy

More than €63.5 million invested in 4 projects

CONCORDIA
Cyber security cOmpeteNCe fOr Research anD InnovAtion

Partners: **46**
EU Member States involved: **14**

Key words
SME & startup ecosystem
Ecosystem for education
Socio-economic aspects of security
Virtual labs and services
Threat Intelligence for Europe
DDoS Clearing House for Europe
AI for cybersecurity
Post-Quantum cryptography

Cyber Security for Europe

Partners: **43**
EU Member States involved: **20**

Key words
Cybersecurity for citizens
Application cases
Research Governance
Cyber Range
Cybersecurity certification
Training in security

ECHO

Partners: **30**
EU Member States involved: **15**

Key words
Network of Cybersecurity centres
Cyber Range
Cybersecurity demonstration cases
Cyber-skills Framework
Cybersecurity certification
Cybersecurity early warning

SPARTA

Partners: **44**
EU Member States involved: **14**

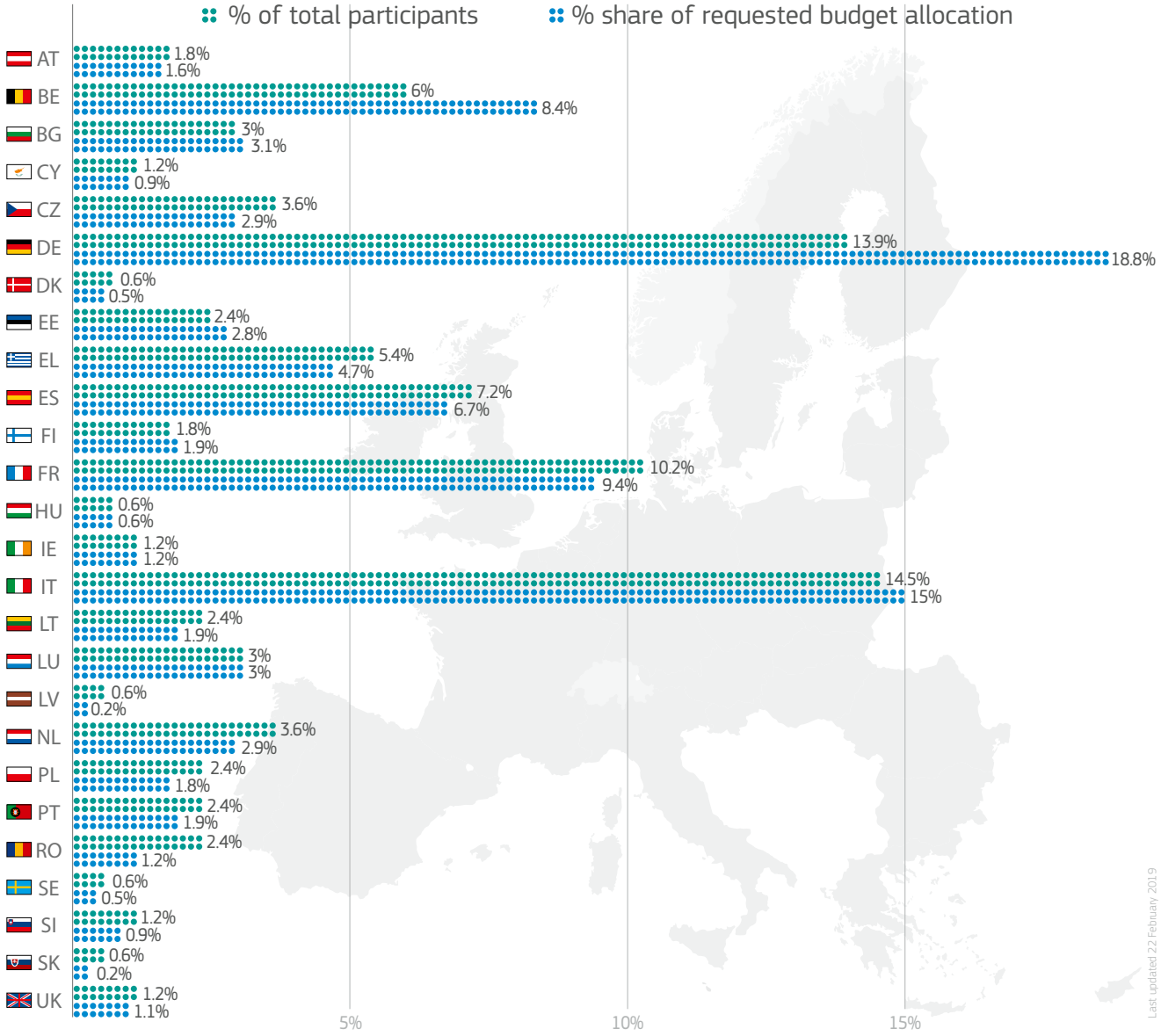
Key words
Research Governance
Cybersecurity skills
Cybersecurity certification
Community engagement
International cooperation
Strategic Autonomy

Last updated 8 March 2019

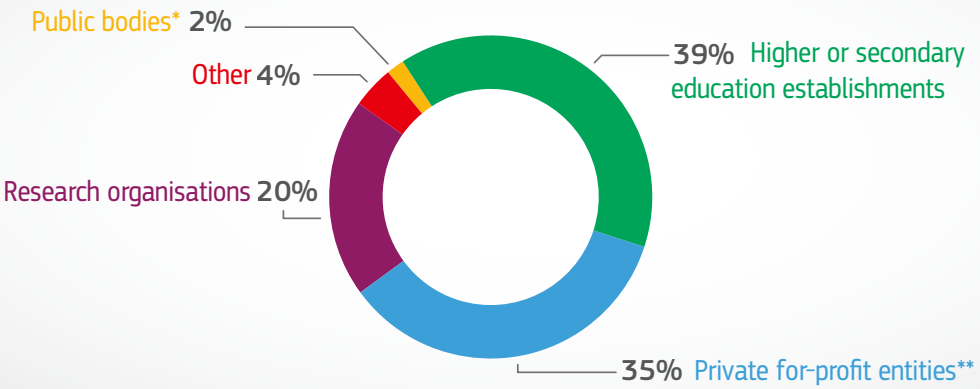
More than 160 partners from 26 EU Member States

European Commission

Source: Data European Commission,
Directorate-General for Research and Innovation (DG RTD) - Unit J5



A diverse cybersecurity ecosystem



* Excluding secondary or higher education establishments ** Excluding research organisations and secondary or higher education establishments

Last updated 22 February 2019

European Commission

Source: Data European Commission, Directorate-General for Research and Innovation (DG RTD) - Unit J5

ceis

Strategic advising & risk management

- **PROSPECTIVE STUDIES AND ANALYSES ON SOVEREIGN SECTORS**
- **CYBERSECURITY CONSULTING AND CAPACITY BUILDING**
- **CORPORATE INTELLIGENCE**

ceis

Organiser of the International Cybersecurity Forum

FIC **INTERNATIONAL CYBERSECURITY FORUM**

#1 European Event on Cybersecurity
Lille, France / Jan. 28, 29 & 30, 2020

In Partnership with the French Minister of the Interior

www.forum-fic.com

www.ceis.eu @ceis_strat