



# THE EUROPEAN FILES

January 2016 - n°40

Cybercrime  
Cybersecurity  
Cyberdefence  
in Europe







## CyberSecurity

Sophisticated solutions and services for protection against targeted cyber attacks.

[www.cybersecurity-airbusds.com](http://www.cybersecurity-airbusds.com)

PIONEERING THE FUTURE TOGETHER

 **AIRBUS**  
DEFENCE & SPACE

## EDITORIAL

## Cyber Issues

Our civilization must deal with issues no other people have ever experienced. The world is more sensitive and interconnected than ever before, and our actions today may decide whether or not our civilization will still be here 100 years from now. It is from this perspective that the European Union chooses to tackle the issue of cybersecurity. Globally, the uncertainty around this new world of activity is understandable. The connections are complex and it is obvious no single government or organization has the capacity to answer all the problems we see today. This issue of *The European Files* assumes an explorative role in the subject of “cyberpower” and its consequences. Essentially, this new realm of activity must be properly defined. Our contributors are acutely aware of the need for a paradigm shift regarding our perspective on cyberdefence. Ultimately, the Internet transcends the European Union’s key operations as well as the lives of its citizens. Indeed, solutions will necessarily require a collaborative effort from a multitude of actors present in this magazine.

Firstly, the policymakers and experts are uniting their spheres of operations to best identify the priorities and objectives within the realm of cybersecurity. The threats to our personal privacy and national security are constant and understated. National governments and international defence organizations alike are overwhelmed by attacks to infiltrate and uncover sensitive information about Europe’s infrastructure. Cybercriminality networks that support violence, extremism, racism, and pedophilia are protected by the complexity of cloud computing. Additionally, businesses are weary of the reputation lost amongst consumers when their information centers

are cracked. It is a legislative priority to protect and promote a balance between privacy and security in this hyper-speed network. The future of European innovation is at risk and national governments such as Germany and Estonia are leading the way in providing revolutionary public and defence policies to deal with these new threats. The infrastructure for most crucial sectors of European activity rely heavily on the progress made in cyber-networks and states are looking to pool expertise to support the weakest links in the network.

Fortunately, within the European community, there is certain richness in capacity and policymaking regarding cyberstrategies. Whether it’s the European Defence Agency or the International Telecommunication Union, coordination and transparency underlie each step of this journey. Although the priorities many vary from one organization to another, the strategies demand for a stronger partnership between the public and private sector. Like all relationships, it is built on trust and each joint effort highlights the importance of a normative framework that empowers businesses and people through greater awareness of the issues ahead. The Cyber Convention Committee provides the international precedence regarding the efforts taken by states across the world to set standards of security. Organizations such as NATO share the urgency and dynamism felt in this sector of defence without necessarily discussing the sources of the threats to our security. All actors do acknowledge the sensitivity of this information and each provides their own motivations to set aside their inhibitions to cooperate more effectively.

This issue also unites the activity of all citizens, private or public. As cyberspace is

the basis for billions of euros in economic activity, it is only natural that action plans created by governmental and non-governmental institutions should focus on a new kind of relationship. Public-Private Partnerships should play a central role in tackling the issues regarding cyberspace. This tool is a favorite of the European Union to promote united markets and innovation across the continent. In this case, actors discuss the areas of cybersecurity that will benefit most from a freedom of information and expertise. Many hope the Public-Private Partnerships will not only be a tool for innovation, but also develop into a standard of European economic activity. Ultimately, these partnerships will be judged on their ability to tackle the many challenges created by an evolved sphere of criminality and insecurity.

The challenges of cybersecurity are pushing the European Union to devote considerable resources to better equip its citizens with the capacity and confidence to protect themselves in this new world. Proposals from governments and supranational departments reiterate the importance of education through trainings and academic curriculums as the basis for a better future. The solutions of tomorrow will also rest on our ability to collaborate on issues such as information freedom. No matter the actor, the consensus is that action must be comprehensive. This edition of *The European Files* unites the many players involved in developing this framework that our world will need for a brighter and more confident future.

LAURENT ULMANN

**Management:** The European Files / Les Dossiers Européens - 19 rue Lincoln, 1180 Brussels

**www.europeanfiles.eu** - ISSN 1636-6085 - **email:** dossiers.europeens@wanadoo.fr -

**Publication Director and Editor-in-Chief:** Laurent ULMANN - **Intern:** Raphaël Benros, Clémence Vorreux

**Copyrights:** European Commission

**Layout & printing:** VAN RUYS PRINTING

# TABLE OF CONTENTS

**Partnerships to step up cybersecurity in Europe**  
**Günther H. Oettinger**, European Commissioner for Digital Economy and Society

**A Joint Approach to Cybersecurity – Enhancing IT Security in Germany**  
**Thomas de Maizière**, German Federal Minister of the Interior

**Cyber security and the protection of critical infrastructure**  
**Hannes Hanso**, Estonian Minister of Defence

**The National Cyber Security Strategy of the Czech Republic for the period of 2015-2020**  
**Milan Chovanec**, Ministry of the Interior, Czech Republic

## I. Cybercriminal and cybersecurity threats

**Cyber space - ultimate case for trust**  
**Tunne Kelam**, Member of European Parliament (EPP Group)

**Protecting data to enhance cybersecurity in Europe**  
**Isabelle Falque-Pierrotin**, Chairwoman of the Article 29 Working Party and Chairwoman of the French data protection authority (CNIL)

**European cooperation in the fight against cybercrime**  
**Matthias Ruete**, Director General, DG Immigration and Home Affairs, European Commission

**Data driven security, contribute to fight against cybercrime**  
**Michal Boni**, Member of European Parliament (EPP Group)

**NATO's response to a dynamic cyber threat landscape**  
**Ambassador Sorin Ducaru**, Assistant Secretary General for Emerging Security Challenges, NATO

**6 Towards a European Cyber Defence Policy**  
**Michael Gahler**, Member of European Parliament and spokesperson on security and defence of the EPP Group in the European Parliament

**8 Towards a more consistent level of cyber defence capabilities across the EU**  
**Jorge Domecq**, Chief Executive of European Defence Agency (EDA)

**9 Mankind, sea, space and cyber defence**  
**Dr. Isabelle Tisserand**, Anthropologist

**10 Ensuring a high common level of network and information security across the Union**  
**Pilar del Castillo**, Member of European Parliament, (EPP Group) Rapporteur concerning measures to ensure a high common level of network and information security across the Union

**14 Cybersecurity: Global solutions for a global issue**  
**Houlin Zhao**, Secretary General, International Telecommunication Union (ITU)

**15 EU-level Cyber Crisis Management**  
**Prof. Dr. Udo Helmbrecht**, The Executive Director, EU Agency for Network and Information Security (ENISA)

**Providing and managing information security**  
**Gerold Huebner**, Development Executive, Chief Product Security Officer, SAP Global Security

**Towards a Public-Private Partnership on cybersecurity and beyond**  
**17 Luigi Rebuffi**, CEO of European Organisation for Security, whose membership includes Europe's major companies and research centres representing two-thirds of the European security supply market.

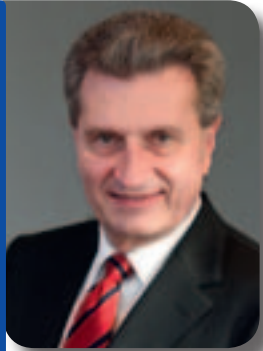
**Data protection and a secure information environment for consumers go hand in hand**  
**31 Giovanni Buttarelli**, European Data Processing Supervisor (CEPD)



# Cybercrime, cybersecurity, cyberdefence in Europe

<b>Challenges of cybercrime - Chances for cybersecurity</b>	<b>32</b>	<b>Cyberpower: stakes and challenges for Europe</b>	<b>44</b>
<b>Monika Hohlmeier</b> , Member of European Parliament (EPP Group)		<b>Dr. Prof. Solange Gheraouti</b> , Director, Swiss cybersecurity Advisory & research Group, University of Lausanne	
<b>Digital Transformation and the increasing need for data protection</b>		<b>No allies in cyberspace</b>	<b>45</b>
<b>Mathieu Moreux</b> , Strategic Marketing, Critical Information Systems and Cybersecurity, Thales	<b>34</b>	<b>Olivier Kempf</b> , Director of La Vigie, Strategic Analysis letter and associate researcher at IRIS	
<b>Towards European Digital Sovereignty</b>		<b>Education, research, economic development: the broad-based approach of the Cyber Centre of Excellence</b>	<b>46</b>
<b>Guillaume Poupard</b> , General Director of ANSSI	<b>36</b>	<b>Paul-André Pincemin</b> , Project Manager of the Cyber Centre of Excellence (France)	
<b>Cybersecurity is one of the cornerstones of our fight against terrorism</b>		<b>Why must Europe invest in cybersecurity?</b>	<b>47</b>
<b>Gilles Pargneaux</b> , Member of European Parliament, (S&D Group)	<b>37</b>	<b>Guillaume Tissier</b> , CEIS Managing Director	
<b>Cybersecurity and eCommerce: ensuring consumer and infrastructure trust</b>		<b>Advanced Persistent Cybersecurity Threats (APT): Preparing for the New EU Cybersecurity Directive</b>	<b>48</b>
<b>Maurits Bruggink</b> , EMOTA Secretary General, Fédération européenne du e-commerce	<b>38</b>	<b>Adam Palmer</b> , Director, International Government Affairs at FireEye (Based in Munich)	
<b>Substantive European criminal law regarding the fight against cybercrime</b>		<b>Cybercrime and the risks for the economy and enterprises at the European Union and Italian levels</b>	<b>50</b>
<b>Isidoro Blanco Cordero</b> , Professor of Criminal Law, University of Alicante, Deputy Secretary General, International Association of Penal Law	<b>39</b>	<b>Fancesca Bosco</b> , Associate Project Officer, UNICRI	
<b>The Budapest Convention on Cybercrime: impact and outlook</b>		<b>Cybersecurity for a resilient European infrastructure</b>	<b>52</b>
<b>Alexander Seger</b> , Executive Secretary, Cybercrime Convention Committee, Council of Europe	<b>40</b>	<b>Hans ten Berge</b> , Secretary General of Eurelectric	
<b>II. Securing networks: a necessary prerequisite</b>		<b>Cyber-security and hybrid codes</b>	<b>54</b>
<b>The individual and the digital world in a changing society</b>		<b>Zbigniew Sagan</b> , Chief Technology Officer, Advanced Track & Trace, member of ITSA Board of Directors*	
<b>Christian Aghroum</b> , CEO of SoCoA Srl, Former head of the French National Cyber Crime Investigation Unit (OCLCTIC)	<b>43</b>	<b>Threat Intelligence</b>	<b>56</b>
		<b>Filip Chytrý</b> , Security Researcher, Avast Software s.r.o.	

# Partnerships to step up cybersecurity in Europe



**Günther H. OETTINGER**

*European Commissioner for  
Digital Economy and Society*

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

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

People will not use what they do not trust. Greater confidence and security are absolutely

fundamental for a more widespread use of digital technologies, including e-payments, cloud computing and machine-to-machine communications which are at the heart of our digital economy and society. However, currently only 22% of Europeans have full trust in search engines, social networking sites and e-mail services and only 38% of Europeans feel confident about online purchases from another EU country.

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

against cybercrime is also at the core of the European Agenda on Security presented in April last year.

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

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

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





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

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

To act, the EU has its own tools. Since 2004, the European Union Agency for Network and Information Security (ENISA) has helped the Commission, the Member States

and the business community to address, respond and especially to prevent network and security problems. In particular ENISA helps collect and analyse data on security incidents in Europe and emerging risks. It also promotes risk assessment and risk management methods to enhance capability to deal with information security threats. Our permanent Computer Emergency Response Team (CERT-EU) is also great instrument to protect the EU institutions, agencies and bodies from cyberattacks.

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

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

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

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

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



# A Joint Approach to Cybersecurity – Enhancing IT Security in Germany



**Thomas DE MAIZIÈRE**

*German Federal Minister of the Interior*

**T**he digital revolution is fundamentally changing the way government, business and society work. The resulting new opportunities and potential also come with growing dependence on IT-supported processes and systems, creating digital vulnerabilities in all areas of life. In the coming years, this will be a central challenge for our society. Germany's Federal Government is actively shaping this transformation.

Security is the cornerstone of our free society. We want to be able to move as freely in the virtual world as we do in the real one. Every form of digitization must therefore be grounded in security in cyberspace. Four years ago, the German Federal Government laid the foundation with its cyber security strategy for Germany. With its Digital Agenda 2014–2017, among other things, it is moving ahead with the goals of this strategy.

A milestone of the national digitization policy is the IT Security Act, which entered into force in July 2015. It is a clear expression of our fundamental conviction that cyber security can arise only in a secure environment, and that cyberspace is only as secure as the systems and infrastructures linked to it. Operators of critical facilities in sectors including energy, information technology and telecommunications, transport, health, water, food and the financial and insurance industry must therefore maintain a minimum

level of IT security. They are also required to report significant IT security incidents to the Federal Office for Information Security (BSI). The BSI analyses all the information it receives and forwards it to all infrastructure operators as quickly as possible so that they can better protect their infrastructures before they too are attacked.

The IT Security Act is also intended to create a basis for close and trusting cooperation between government agencies and the private sector, which are working together to draw up minimum standards, design monitoring systems and establish reporting channels. In the spirit of this cooperative approach, the new law provides only very moderate powers of government enforcement. We have consciously embarked on this new approach which departs from typical government regulation and relies instead on self-regulation within a legal framework. Such an approach is somewhat unusual for government, but digitization has created a new and radically accelerated environment for government action. It therefore makes sense to question traditional ways of doing things and try a new approach, if necessary.

This approach is also in line with the currently discussed EU Directive on Network and Information Security (NIS Directive) and enables us to use the expertise and experience of relevant operators as effectively and as far as possible. We believe this is the right response to the complexity and speed of ongoing digitization. Technical specifications and conditions in the individual areas of critical infrastructure are too diverse for the government to set rigid requirements. Our new approach means that this legislation will continue to be viable in the future, that it allows for innovations in IT security and that it is reasonable and practical for companies to comply with.

The IT Security Act also calls for measures in addition to critical infrastructure protection. To increase security on the Internet, for example, the new law has much stricter requirements for providers of telecommunications and telemedia: They must inform their customers of cyber attacks on their networks so they can protect themselves effectively. At the same time, the law gives the BSI more powers to warn the public and advise the

German private sector, reflecting the agency's increased importance at national and international level.

Because the future will continue to bring new challenges, government must develop new ways of thinking and acting. For example, in view of the growing complexity of IT systems, stakeholders in government and the private sector will have to work together more closely as equal partners, because cyber security is a joint effort. Neither the government nor private industry can achieve IT security on its own; each must do its part.

This also applies in the European context, especially with regard to critical infrastructure, which by its very nature touches on a wide range of national interests and responsibilities. These must also be respected. As with the private sector, with Europe too it is clear that, in a thoroughly connected world, we cannot ensure cyber security on our own, but only in cooperation with others.

The cyber security of the European Union is only as good as the security in each of its member states. This is why the NIS Directive is an important step forward and a key anchor of trust which will enable our citizens to use the Internet freely and safely and will help the EU's digital economy to flourish. Our common goal must therefore be to continue to develop our common European cyber security culture so that we can profit from the opportunities offered by global interconnection.



# Cyber security and the protection of critical infrastructure



**Hannes HANSO**

*Estonian Minister of Defence*

Cyber security has become a buzzword of today's world, every day we hear about cyber-attacks against national institutions, business-sectors and our citizens. With a rapid development of the Internet, we are benefitting from the economic and social advantages that e-commerce and social media offer us. However, this is always coupled with ever higher vulnerability forcing all of us to focus more on the security side of the cyber world.

One can say that Estonia was lucky enough to go through nation-wide cyber-attacks in 2007. While at that moment everybody's life was somewhat disturbed, these attacks had much more significant effect for the future as they showed our vulnerabilities as well as the way forward. In other words, that moment made us focus on what does it actually mean for a government to be responsible for the functionality of the e-lifestyle that Estonians had got so used to. Already then, Estonia was leading the world in terms of e-services that both the government and private sector offered to the citizens.

As one of the lessons learned, in 2008 we established our first cyber security strategy which set initial goals of cyber security, mainly through reducing our vulnerabilities through internal and international cooperation. The strategy set the structures for cooperation with the private sector, including addressing

the question of information sharing making it mandatory for the critical infrastructure enterprises. The experience of 2007 attacks were painful enough so that public-private partnership was seen as a reasonable way to counter future cyber threats.

Also, in 2008 the NATO's Cooperative Cyber Defence Centre of Excellence was established in Tallinn to enhance the cyber knowledge of the alliance. Currently, there's 18 nations participating in the CCDCOE with their experts.

From the other perspective, we are also constantly developing and spreading our cyber-knowledge to the education. Ministry of Defence helps to organize an annual Cyber Olympics for the college students, we also offer cyber defence scholarships for the students. This autumn started the first high school in Põltsamaa focusing on cyber defence. The support of cyber education is the most efficient way to boost the knowledge and develop the domain in long run. We already see the next generation of cyber-savvy youngsters in the field.

While the cyber security in Estonia is viewed primarily through making sure that the vital services and critical infrastructure are sustainable, one could ask, what is the role of the Ministry of Defence? The answer lies in the comprehensive approach to security – this is relevant for conventional as well as cyber security. It demands extensive cooperation with the private sector as the latter is the provider of many of the vital services and as a rule, private sector is able to hire the best experts. The key question therefore is, how to build up a truly functional partnership.

One of the solutions we came up with in Estonia is called a Cyber Defence Unit of the Estonian Defence League (the latter is a volunteer military organization, similar to the National Guard in the US). The Cyber Defence Unit is a voluntary organisation, consisting of experts from governmental agencies as well as private companies with a mission to protect Estonia's high-tech way of life, including protection of information infrastructure and supporting broader objectives of national defence. It is a great example of bringing together the skills and knowledge of people who otherwise would not be reachable to the Government.

Furthermore, the Cyber Defence Unit serves also as a so-called collective brain where members can exchange experiences, train and when needed, act together. Bringing together experts from public and private sectors enables us to make sure that this cooperation does not work only in theory, but is backed with practical activities. Through their routine cooperation they learn about each other's expectations and how to act in more critical situations.

It does not matter whether we come from civilian, military or private structures. Present day cyber threats demand us working together in a comprehensive manner. The adversaries in cyber space are very versatile and cannot be defeated by any single institution. In essence, public-private partnership through information sharing and practical cooperation is not a mere wishful ideal but a real necessity. In cyber dimensions there is no relevance of the size of the nation or its physical proximity to the others. A small nation can be big in cyber space if there's enough good brains and they are orchestrated to act together. This is the Estonian strength in the cyber world.

# The National Cyber Security Strategy of the Czech Republic for the period of 2015-2020



**Milan CHOVANEC**

*Ministry of the Interior, Czech Republic*

It is clear that cyber threats and risks do not know any borders. The Czech Republic, as an active member state of the European Union, is aware of its duties and responsibilities in the area of cyber security and monitors the current situation globally, i.e. not only cyber security, but also cyber criminality and cyber defence.

As one of the first steps toward fulfillment of provisions of the National Cyber Security Strategy the Czech Republic has adopted the act No. 181/2014 Coll., on Cyber Security, which came into force on 1 January 2015. This act has launched the process of actual implementation of organizational and technical

requirements and regulations within the state administration institutions.

The National Cyber Security Centre together with the Department of Cyber Security, Coordination of Information and Communication Technologies of the Ministry of the Interior has developed methodologies and procedures for the implementation of the Cyber Security Act, which were communicated to the state administration institutions. The Ministry of the Interior is cooperating with other EU Member States and, through activities of the National Security Authority, takes part in workshops – Cyber Exercise to practice coping with cyber emergencies.

## What governs the new legislation?

Key organizational measures under the Cyber Security Act:

- Adoption of Policy of Information Security Management System of the Ministry of the Interior on the basis of the Act No. 181/2014 Coll., on Cyber Security,
- Creation of the Cyber Security Council,
- Appointment of persons into the key positions with specific roles and responsibilities (manager, architect, auditor),
- Implementation of the Information Security Management System of the Ministry of the Interior (ISMS),
- Certification of the Information Security Management System of the Ministry of the Interior according to ISO 27000-27010,
- Launching of e-learning module to raise the awareness of the obligations resulting from the Cyber Security Act and

even beyond its provisions; module will become a part of multilayer learning of personnel of the Ministry of the Interior, as well as of personnel of the Police of the Czech Republic,

- Strengthening the cooperation across the state administration institutions; in particular the relation between specialized police units dealing with cyber crime and the National Cyber Security Centre which is a competent national authority for the issues of cyber security in the Czech Republic,
- Creation of specialized cyber police unit with appropriate expertise within the Organized Crime Unit of the Criminal Police and Investigation Service of the Police of the Czech Republic,
- Creation of the Cyber Threat Prevention Team of the Ministry of the Interior, which prepares procedures to cope with cyber emergencies and cyber attacks and its consequences (Cyber Commandos).

Risks in cyberspace cannot be underestimated. In 2015, the Czech Ministry of the Interior has monitored 15 cyber incidents targeted to its systems and only due to using of adequate tools (e.g. demilitarized zones), centralized architecture of database services and timely activity of its personnel Ministry has prevented any damage and has taken the appropriate measures.

Currently, there are undergoing preparations for the establishment of a new cyber police unit within the Organized Crime Unit of





the Criminal Police and Investigation Service of the Police of the Czech Republic. The cyber police unit will be composed of two branches (methodology and coordination, and retrieval and investigation of crimes). The unit will also be actively involved in the investigation of criminal cases which, by their scale, complexity or transnational dimension, must be coordinated from a single national point. An integral part of the unit will be analytical capacity necessary for proper and fast orientation and decision-making in casual cases as well as in coordination of key areas and in connection with large amount of knowledge from cyberspace.

### Monitoring Centre being operational

Key step in the fulfillment of provisions of the Cyber Security Act was the construction and launch of activities of the e-Government Monitoring Centre to ensure cyber security monitoring — Security Operation Centre for Continuous Reliability (SOCCR) allowing to monitor information and communication systems which fall under the category of a Critical Information Infrastructure or/and important information systems.

Nowadays, two of twenty six information systems of the Ministry of the Interior have already been connected to the e-Government Monitoring Centre, i.e. the Agenda

Information System of the Police of the Czech Republic (AIS) and the Public Administration Portal (PAP). Connecting of individual information systems to the e-Government Monitoring Centre is being processed in compliance with the timetable envisaged by the law.

All information systems are carefully analyzed before being connected to the Monitoring Center — risk analysis submission followed by the statement of eligibility - subsequently, their technical parameters are properly adjusted to meet the standards of the Cyber Security Act. The results of analytical work as well as proposals for measures are simultaneously inserted into the Central Security and Monitoring System (CSMS).

Increasing volumes of processed data require strengthening the capacity of police specialists to evaluate data relevant in criminal proceedings in the area of cybercrime and this, of course, demands a material support. Because of this, it is expected that, over the period of three years, specialized police units will be equipped with new highly capable hardware in order to strengthen the capacity to combat fast growing cybercrime.

### And what next?

Among other measures that are important for ensuring cyber security within the Ministry

of the Interior some additional projects are being planned, e.g.:

- Preparation of the National Cloud Computing Project (task approved by the Action Plan of the National Cyber Security Strategy 2015-2020),
- Construction of database center for storage of data relevant for cybercrime investigation (co-financed from European funds),
- Unification of Traffic Data Project focused on effective administration of all hardware and software within the Ministry of the Interior.

The Ministry of the Interior will propose changes to the legal framework that will ease gathering of the evidence and clues needed to combat cybercrime, in particular collection of digital footprints in the information environment.

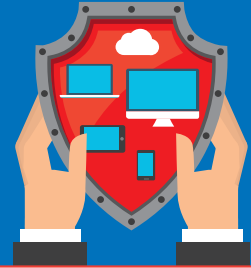
The main objective of the Cyber Security Act is to ensure the security of information and communication systems, especially those necessary for the proper functioning of the state administration and services provided to the public. Main responsible body for correct implementation of legal provision within the Ministry of the Interior is the Department of Cyber Security, Coordination of Information and Communication Technologies from the section of the Deputy Minister for Information and Communication Technologies.



# Cybersecurity

## Public-Private Partnership

A Digital Single Market initiative to boost European cybersecurity industry



### Cyberspace is a backbone of digital society & economic growth

315 million Europeans use the Internet everyday



across all areas of the digital society



ehealth



e-commerce



smart mobility



energy  
(e.g. smart grids)



finance  
(e.g. e-banking)



Internet of Things

### Cybersecurity incidents may

disrupt the supply of essential services such as



water



healthcare



electricity



mobile services

Undermine trust in digital services & products

only 22% of Europeans



have **full trust** in companies  
such as **search engines**,  
**social networking sites** &  
**e-mail services**

Only 38% of Europeans



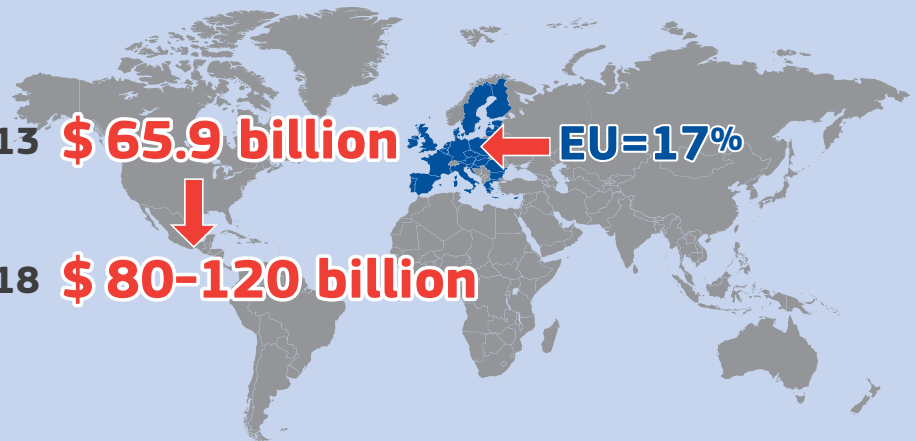
feel **confident** about  
**online purchasing** from  
another EU Member State

### Cybersecurity is an economic opportunity for the EU

The  
cybersecurity  
global market

2013 \$ 65.9 billion

2018 \$ 80-120 billion

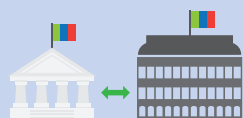


European  
Commission



## A key obstacle: the fragmentation of the EU cybersecurity market & industry

While cybersecurity threats (& opportunities) are borderless by nature, the EU cybersecurity market is highly fragmented due to



development of solutions historically driven by governmental needs



existence of **different Network Information Security policies** across Member States



lack of **interoperability** for cross-border purchase



lack of **trust** for cross-border purchase

### The impact of market fragmentation

#### For EU companies



it's **hard to compete** on the **European & global level**



**smaller companies** are more subject to **merger & acquisition** by **non-EU large companies**



**outflow of know-how & specialists** looking for career opportunities beyond Europe



difficulties to **access** innovative, competitive & user-friendly **technology** that takes into account **European rules & values**

## A Public Private Partnership to strengthen the European cybersecurity industry

mobilising public & private resources under Horizon2020 to boost European cybersecurity

helping turn Europe's world-class cybersecurity research into products & services that are innovative, competitive, user-friendly and take into account European rules & values

building trust among users, businesses, public administrations

defining minimum common digital security & privacy requirements across different sectors (e.g. energy, health, finances)

## Your views matter – help us shape the PPP on cybersecurity

To prepare the launch of the PPP in 2016, the European Commission would welcome your views on



**cybersecurity risks & threats** people & **businesses** in Europe are facing



**cybersecurity market conditions** in Europe



**support** needed for European **cybersecurity industry**



PPP **technical priorities** for research & innovation



**possible other supporting measures** (e.g. standardisation, certification, labelling, skills)

## Have your say!

Participate in the European Commission's public consultation

[bit.ly/cybersecurityEU](http://bit.ly/cybersecurityEU)

#cybersecurity



European  
Commission

# Cyber space - ultimate case for trust



**Tunne KELAM**

*Member of European Parliament  
(EPP Group)*

In cyber space, all boils down to trust. Trust between States, between institutions, citizens and businesses. Only the existence of trust makes people to share sensitive information, to act and to cooperate. Such a trust needs to be universal and reciprocal. On the other hand, trust is based on common values, common assessments and common efforts to achieve a high level of technical preparedness and resilience.

It is the end of the year 2015 and legislative acts, related to cyber security, can be counted on the fingers of one hand. Only recently has the EU accomplished its first binding legislation on cyber security – the Network and Security Directive. The latter opens the way to establish common standards on cyber security, applicable to critical infrastructures and information systems. These standards should cover different areas from energy to finance, health and internet providers, including also online market spaces and cloud services. This will be an essential step forward in increasing the level of trust between the public and private sector, between State and citizens, who are predominantly users and consumers of multiple services. As the EU is about to step into the era of a digital union, the directive in question in association with the forthcoming legal acts on data protection, will hopefully create the foundation of trust between different actors and levels.

Still, not all Member States have managed to complete their national cyber security strategies that could and should become the cornerstones in building trust and expanding the information sharing and cooperation. The persisting differences in the domain of political motivation, technical preparedness and coordination indicate the underlying need to cyberize the European way of thinking. Not only many users of cyberspace, but also many lawmakers, civil servants and entrepreneurs seem to lag behind dramatically accelerating developments. It is high time to fully acknowledge and mainstream the cyber security aspect in all areas of human and public relationships.

Next to trust-building and preparedness, a major challenge is an efficient information exchange. To achieve this, one must be strategically committed to tearing down the traditional walls between specific policy areas, to eliminate barriers that hinder different authorities from cooperating. Cyber space is forcing policy makers to abandon their traditional clustered thinking; in fact, it could provide an incentive for a major re-thinking in how policies are designed and developed. One of the first indications towards such a rethinking could be seen in the April 2015 Communication on European security agenda that promotes building of a real cooperation between internal and external security. Such a development will be highly essential in the ongoing fight against terrorism and in safeguarding on the basis of mutual solidarity and collective actions the security of both the Union and its Member States from outside challenges.

One of the greatest concerns regarding sharing information is the sensitive nature of the information. States as well as businesses are equally reluctant to expose their vulnerabilities by sharing information about cyber attacks that have targeted them, not to speak of damages inflicted. They have serious reason to worry about loss of reputation which will mean losing trust. True, the NIS directive has set clear criteria of resilience for infrastructure and information system operators. Unfortunately it has exempted public administration, unless the latter operate critical infrastructures and information systems. If the EU wants to be serious and credible in its efforts

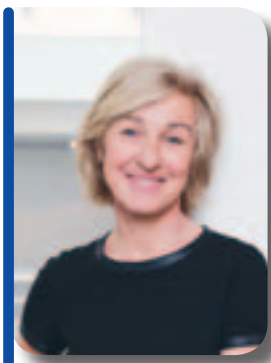
to efficiently improve information-sharing, it cannot exclude enhancing cyber security resilience of public administrations. In reality it means maintaining the highest security level both for soft- and hardware and to ensure that all staff members, without exceptions, who are operating any connected device will be fully aware of cyber security risks and know how to minimize them. This all would start from the very basic cyber hygiene-routine trainings, adequate cyber risk analysis and management, up to date contingency plans both in private and public sector.

At this moment the EU has to concentrate on stepping up the efforts. A substantial part of soft- and hardware in use originates from producers situated outside Europe. In such a situation it is more difficult to strike acceptable balance between privacy and security-a balance that is essential for the EU citizens. It is time to realistically build all- European cyber-digital industrial base therefore Europe needs to significantly increase smart investment. Being able to develop and build European security-in-by-design devices, systems, programmes would strengthen citizens' trust in cyber space towards European policy makers, as they would be guaranteed the highest security and privacy standards legally valid all over the EU. It would reassure that sensitive information can be shared in secure environment, developed and built from scratch in Europe. And lastly, it would boost the human capital that Europe needs-invaluable capital that currently is being brain-drained out of Europe.

Following the example of gradually overcoming its inhibition for police cooperation, the EU has to overcome also its inhibition for cyber cooperation. Member States need to level up their resilience and preparedness. Only by doing that they can build trust in their counterparts to share and cooperate in the super sensitive area of cyber space.



# Protecting data to enhance cybersecurity in Europe



**Isabelle FALQUE-PIERROTIN**

*Chairwoman of the Article 29 Working Party and Chairwoman of the French data protection authority (CNIL)<sup>1</sup>*

Cyber threats have been expanding at an alarming rate over the last years. As our society turns digital, they now increasingly target data. Indeed, data and in particular personal data stand for a financial asset. Companies use them to get to know the tastes and expectations of their customers and to offer them new personalized services. Data are the new levy of the digital economy and the motor of innovation. Consequently, they attract the greed of public or private entities. Of course, not all of these threats are new: bank data, for example, have long been affected by this phenomenon. But as data are everywhere and connected objects are pervading our whole environment, the phenomenon is getting decentralized and difficult

to master. Moreover, it may affect new types of data such as health data.

People are starting to worry about these threats that may impact their everyday lives. The same holds true for private companies. A recent report states that the cost of data breaches will amount to 2.1 trillion dollars globally by 2019, increasing to almost four times the estimated cost of breaches in 2015. Even states are now faced with cyber security challenges that tend to become a menace to national defence. A spectacular illustration thereof was given by the attack having stricken the US agency that manages the civil service of the federal government in April 2015. The personal data of an estimated 18 million federal employees were affected. In respect to such a ubiquitous threat, it is therefore vital that cyber security awareness develops in every sector of society and business. Only on this condition will we be able to address the challenge.

Data protection authorities have a crucial role to play in this context. Digital security has historically been a major concern for them because there can be no privacy without security. In France, for example, CNIL is empowered to control and sanction the lack of personal data security (French data protection Act, article 34 bis). But this role of the data protection authorities is about to become even more important. Against the emerging threats to personal data, the forthcoming European Regulation on the protection of personal data will provide them with answers up to the new challenges.

First and foremost, the Regulation will enhance the liability and accountability of data controllers and make them somehow “co-actors” of the regulation. It will even

extend these obligations to the data processors. While cloud computing has acquired a central position, these requirements are key to securing the digital world. To help insure the effectiveness of the rules, The Regulation will also organize the deployment of a series of compliance tools for data controllers. For example, Article 33 will impose the setting up of a “data protection impact assessment” prior to the implementation of a processing when it exposes those involved to risks to their privacy. This kind of tools, as well as the “codes of conduct” (art. 38), will be particularly helpful for disseminating good cyber security practices throughout the variety of small and medium size enterprises with which the Data protection authorities interact on a daily basis. The Regulation will also extend to the data controllers the requirement to notify data breaches while it previously applied only to e-communications service providers. Data breaches will have to be notified, according to the possible risks, to the data protection authorities and the people involved.

So the future Regulation will make personal data security a major element of data protection authorities’ action. I believe that these new rules and tools will also give a key competitive advantage to our continent at a moment when these questions are becoming of a vital importance in the eyes of consumers and citizens globally. They will be a positive incentive encouraging tech professionals in Europe to address security and privacy concerns early on in the process of designing their new products. By the same token, they will provide individuals with more control over their personal data. To sum up, I am very confident that we are about to set a solid framework for the digital development of Europe that could even prove an attractive model outside Europe.

<sup>1</sup> The Article 29 Data Protection Working Party was set up under the Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

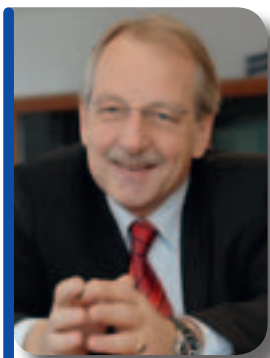
“The Article 29 Data Protection Working Party is composed of:

- a representative of the supervisory authority (ies) designated by each EU country;
- a representative of the authority (ies) established for the EU institutions and bodies;
- a representative of the European Commission.

The Working Party elects its chairman and vice-chairmen. The chairman’s and vice-chairmen’s term of office is two years. Their appointment is renewable.



# European cooperation in the fight against cybercrime



**Matthias RUETE**

*Director General, DG Immigration and Home Affairs, European Commission*

Cybercrimes are becoming more frequent, more aggressive and have a significant economic impact. Moreover, organised criminal networks are increasingly using (and abusing) digital means to carry out illicit activities. Hacking into a harbour's information system to avoid custom checks to enable drug smuggling shows how the Cybercrime-as-a-Service business model is spreading;<sup>1</sup> the threshold in difficulty for committing cybercrime has decreased immensely in the past few years. No technical skills are necessary, as the relevant tools and services are available online in user-friendly versions at reasonable prices, offering anyone the opportunity to commit cybercrimes.

Cybercrime offences also frequently constitute a violation of fundamental rights, for instance in the cases of identity theft, data interception or child pornography. Citizens have a right to an effective protection against such violations, which requires an effective law enforcement response.

The rule of law must apply online as it does offline.

Businesses also suffer from increasing costs: reliable statistics are hard to come by but estimated worldwide costs range from several hundred million to several trillion Euro per year, across different studies. However, all agree that costs are on the rise and cyber risk insurance has become a new boom industry.

Cyber-enabled crime presents unique challenges as compared to many traditional forms of crimes: it has an inherent cross-border element and its effective prevention, investigation and prosecution requires a coordinated international response, both within the EU and beyond. At the same time, the location of cybercriminals and their data becomes more and more difficult and sometimes impossible to track down. Software has become available for IP dissimulation that requires lengthy investigations to determine the true location of the data, if it can be found at all. Cloud services allow cybercriminals to avoid storing any illicit material on their own computer. The fluidity with which data can be transferred across jurisdictions in a matter of seconds, multiple times within the hour, further complicates investigations.

So, not only does it make sense to cooperate in the fight against cybercrime, we simply have to.

When it comes to law enforcement cooperation, both within the EU and beyond, the European Cybercrime Centre at Europol (EC3) has led the way in a number of successful, multinational cases – botnet takedowns<sup>2</sup>, dismantling of a “ransomware” ring hijacking users’ computers<sup>3</sup>, or eliminating a ring of child sexual abusers and taking down their infrastructure<sup>4</sup>, to name but a few recent successes.

Still we face significant challenges especially when it comes to cooperating with the private sector, which is crucial, as the Internet infrastructure is largely owned and managed by private actors. Valuable efforts are already underway at the European level, in addition to the existing EU legislation<sup>5</sup>: the European Commission launched an EU Internet Forum in December 2015; the EU has funded a growing number of Centres of Excellence on Cybercrime Research, Training and Education; and the EC3 has created various fora for the

exchange of strategic information with the private sector, such as its advisory groups. Many more examples exist at the national level.

We need to build on these initiatives and take them farther. Given the key role of private actors, it is difficult to imagine any effective approach to cybercrime without a stronger and expanded role of the private sector. It is our task to create the right conditions to enable the private sector to live up to that responsibility. Many companies are already making significant efforts. However, companies still operate in a grey area and may find themselves accused of performing “private policing” and censorship. Understandably, this does not incentivise companies to increase their efforts. To succeed, we have to provide them with legal certainty when it comes to their liability for content, for sharing information with public bodies and law enforcement in particular.

The key problem that has emerged in criminal investigations is the difficulty to get access to electronic evidence when data is stored outside the territory of the investigating law enforcement agency – as is increasingly often the case. Access to such data is complicated and may take many months using existing procedures, and widely varying approaches have developed across countries and companies. This situation impedes the effectiveness of criminal investigations and prosecution, in particular in terms of reliability and admissibility of evidence in courts.

To respond to these challenges, the **European Agenda on Security** includes a package of actions to support the fight against cybercrime. One key action is the removal of obstacles to cybercrime investigations, such as the ones outlined above. The European Commission is working closely with the Member States on identifying and implementing possible solutions. It also includes a strong commitment regarding the implementation of European legislation, such as the Directives on attacks against information systems and on child sexual abuse and sexual exploitation and child pornography.

The European Agenda on Security acknowledges the need for a shared agenda, for European Union institutions, Member States and partner countries, national agencies, and for the private sector, to work together in the fight against cybercrime and in this way making an important contribution to the strengthening of the European area of Freedom, Security and Justice.

2 <https://www.europol.europa.eu/content/botnet-taken-down-through-international-law-enforcement-cooperation>

3 <https://www.europol.europa.eu/content/international-action-against-gameover-zeus-botnet-and-cryptolocker-ransomware>

4 <https://www.europol.europa.eu/content/organised-crime-networks-targeted-huge-law-enforcement-operation-europe>

5 On cybercrime, the 2011 Directive on child sexual exploitation and the 2013 Directive on attacks against information systems are prime examples of recent efforts to approximate laws of the Member States.

1 Europol's 2015 Internet Organised Crime Threat Assessment

# Data driven security, contribute to fight against cybercrime



**Michal BONI**

*Member of European Parliament  
(EPP Group)*

The world becomes more and more digital. And the core of the multidimensional digital growth is related to the data driven development. It means collecting, processing, and transferring of data for many purposes, ranging from better analytical opportunities in the area of research, commercial activity, administration, education, medical services, to the area of security in the modern world. It includes fighting cybercrime, where offences are growing in numbers. The economic value of cybercrime in 2014 was estimated at USD 575 billion! Nobody is safe from cybercrime.

Two factors are crucial: privacy protection and ensuring the security as a background for trust, essential value for further digital development. Better security and privacy protection requires good legislative framework, institutional solutions and cooperation, as well as technical possibilities, like security and privacy by design.

But what are the most important actions? To have much more secure infrastructure, to encourage companies to establish privacy and security policies, to raise awareness of the security challenges and incorporate practical solutions and behaviours into everyday life and work, to have the possibility to process all data (not only personal data), which can improve security also by preventive measures.

Of course, there are good examples but we still need to work on some issues.

We feel that there are some gaps and deficits in the area of security in the Internet.

Firstly, it is related to the lack of readiness for sharing the knowledge and the data. Sometimes it depends on legal rules and the lack of strong obligations (among Member States, among intelligence of different countries, among law enforcement units) - so we need the NIS directive, and we have to finalise the work on the EU Data Protection Package, Regulation and Directive. The latter will set data protection rules for exchanging specific data to fight criminal and terrorist activities. It is important to understand that we need to harmonize the legal framework to ensure higher level of cybersecurity in Europe, but first of all we need to make sure that the Member States are cooperating in this area. Sometimes the high level of cybersecurity depends on the existence of technical capacity to be able to exchange data in the real time and to share the data automatically, as only this can guarantee the swift reaction. But, sometimes it depends on existence of trust and ability for cooperation among stakeholders.

Secondly, it is clear that the only way for security, and data driven security need to be based on effective cooperation, a partnership involving all stakeholders: citizens, police, intelligence units, business, NGOs, civil, democratic institutions and authorities in order to guarantee the democratic oversight on data processing in the fight against cybercrime.

Thirdly, we need to solve the problem of encryption. Encryption is widespread and it is important for users to ensure their privacy and increase security for transmission of data. So, it is also essential for business. On the other hand, this is also a tool used by the cybercrime perpetrators and terrorists. I believe, it should not mean that we introduce a ban on using encryption. It rather poses a challenge for law enforcement authorities on the one hand to acquire knowledge on how to crack the codes and on the other to ensure legal and practical conditions for law enforcement to operate in this area, if necessary.

Fourthly, it is important to precisely define what kinds of data are needed to be processed to ensure security. It can be all kinds of data, not only personal data. But, if they are personal, we should finalize European efforts to establish clear rules for data protection in order to be able to use them by the law enforcement. The rules should include the principle of proportionality, adequacy, as well as rules for retention and masking data (as it is in the EU-PNR Directive).

Fifthly, there are many new technological possibilities, especially oriented on all kinds of data, with algorithms, which can help us fight cybercrime. Spectrum analysis of photos can support us in finding sexual abuses of children or give us, after a thorough comparative analysis, substantial knowledge on preparation of terrorist attacks encrypted in pixels. If we want to develop data driven security opportunities we need to change the tools we are using from time to time. Analysis of the frequencies of key words can help us in finding the sources of cybercrime but it is not the only tool we may use. This type of data collection inevitably leads to creation of big data bases. It is better to use adequate, well-designed algorithms, so that we collect less but more targeted data that are almost entirely useful to us.

Sixthly, the only way to achieve the success is to find the equilibrium between the security needs, individual rights and technological possibilities. Under those terms, we can develop the data driven security.



# NATO's response to a dynamic cyber threat landscape



**Ambassador Sorin DUCARU**

*Assistant Secretary General for Emerging Security Challenges, NATO*

The interconnected character of cyberspace has offered unprecedented opportunities for our economies and has transformed the fabric of our societies. By the same token, this interconnected space also makes us vulnerable.

NATO, like any other large organisation has been increasingly targeted over the past decade and is confronted by a range of cyber threats. We see a rapid evolution in the threat landscape – not only in terms of scale, but also in sophistication and velocity. Each day our systems register millions of suspicious events, with a handful requiring further analysis by our experts. The main aims of cyber-attacks against NATO networks are functional disruption and cyber espionage. We are also concerned about the potentially growing nexus between cyber and terrorism. Increasingly, threat actors are taking advantage of the digital underworld as a rapid and cost efficient means of harnessing capability. Recent events in Ukraine have also illustrated the utility of cyber as a tool in a hybrid warfare context.

Against this background, Allied Heads of State and Government have adopted the *Enhanced NATO Policy on Cyber Defence* and its associated *Cyber Defence Action Plan* at the 2014 NATO Summit in Wales. This *Policy* encompasses three key themes: re-shaping NATO's cyber defence paradigm; reinforcing

cyber defence capabilities and capacity; and exploring new ways of doing business both within NATO and with partner countries, international organisations and with industry and academia.

The first theme of the *Policy* acknowledges that the principle of collective defence also applies to threats emanating from cyberspace. This is significant because it marks an evolution in our conceptual understanding of the cyber realm. Cyber defence is therefore explicitly recognised as part of the Alliance's core task of collective defence, as is the notion that international law is applicable in cyberspace. To this end, NATO continues to support the development of norms and confidence-building measures to ensure a more secure yet open cyberspace for all.

Second, to enable the Alliance to fulfil its core task of collective defence, we must have robust capabilities and capacity, both at NATO and across member states. The NATO Computer Incident Response Capability (NCIRC) represents NATO's technical cyber defence capability acting upon real-time data from our networks. We also have a Cyber Threat Assessment Cell (CTAC), which produces long-term reports and analysis combining information from a variety of sources. Allies in turn continue to develop their capabilities through the NATO Defence Planning Process and Smart Defence projects. Training, education and exercises also form an essential pillar of the Alliance's cyber defence efforts. Finally, cooperation across borders, notably information-sharing on threats, to reinforce the resilience of networks and help to prevent, respond to, and recover from, cyber-attacks is critical.

Third, we recognise that cyber defence is a cooperative effort. Put simply, NATO can protect its networks more effectively if it works with others. In this spirit, NATO is actively engaged with its partners on a wide range of cyber defence issues, including policy and strategy development, exercises and training activities. With a network connecting more than 65 countries from Europe to the Asia-Pacific, to the Middle East and North Africa, engagement is tailored and based on shared values and common approaches to

cyber defence. Most recently, seven partner countries took part in NATO's largest annual cyber defence exercise – Cyber Coalition. Three new partners – Japan, Jordan and Georgia were observing the exercise for the first time. The importance of engagement with industry and academia has also been recognised and NATO is enhancing information sharing with industry for better situational awareness, notably through the NATO Industry Cyber Partnership (NICP).

Finally, deepening cooperation with the European Union to advance mutual cyber defence objectives is also a priority for NATO. We have engaged in staff-to-staff level talks and briefed our respective committees to share information, avoid duplication of effort, and leverage synergies where possible. In practical terms, there are two particular areas to potentially deepen further our engagement. First, through information-sharing initiatives to improve cyber incident/attack prevention, detection, prediction and response. NATO and the EU could also share cyber defence best practices – for example on technical innovations, incident handling methodologies and secure configuration of networks. A second area focuses on cyber defence exercises. The EU is invited to participate in NATO's exercises. Similarly, NATO could participate in relevant EU exercises once the parameters have been fully developed. Ultimately, the aim is to test the crisis management procedures of both organisations with a view to enhancing the ways in which we work together. Effective cyber defence encompasses not only technology, but also people and processes. Cooperation through information-sharing and exercises is therefore imperative for bringing coherence to these key elements.

To conclude, an increasingly dynamic international environment gives rise to a number of considerations that will challenge policy development, capabilities, information-sharing, cooperation and partnerships in the years ahead. The wide range of NATO cyber defence activities are not conducted in a vacuum. Instead, they are continuously assessed within the context of the existing geopolitical and technological landscape as we prepare for our future in an increasingly digitised and connected world.

# Towards a European Cyber Defence Policy



**Michael GAHLER**

*Member of European Parliament and  
spokesperson on security and defence of the  
EPP Group in the European Parliament*

The rapid evolution of cyberspace in the last two decades not only fundamentally changed our way of living and has offered vast economic opportunities, it also confronts us with new security challenges. The dependence of public infrastructure and global economic relations on availability of, secured access to and stability of cyberspace makes our societies vulnerable at a new level. This new dimension of vulnerabilities was clearly illustrated by the cyber-attacks in Estonia in 2007 and on the European institutions in 2011. Furthermore, in the light of hybrid warfare, as we can experience these days, cyberspace also transforms into a fifth domain of warfare. Considering additionally that cyber infrastructure poses the backbone of any military operation and its success, the issues of cybersecurity and in particular of cyber defence become even more severe. In the past years the EU has started to actively address this issue of cyber defence. The initiatives taken so far can be considered as a starting point for a common cyber defence policy.

In February 2013 the EU took an important step by publishing its cybersecurity strategy in which developing a cyber defence policy was mentioned as one of four priorities. The December 2013 summit on EU's Common Security and Defence Policy (CSDP) reaffirmed that by recognising cyber defence as a key priority for capability development. Following

these events, the Council adopted the EU Cyber Defence Policy Framework (CDPF) in November 2014. This Framework outlines five priority areas for EU cyber defence with special regard to CSDP: supporting the defence capability development related to CSDP, enhancing the protection of CSDP communication networks used by EU entities, promotion of civil-military cooperation and synergies with wider EU cyber policies and relevant institutions, improvement of training, education and exercise opportunities, and finally enhancing cooperation with international partners, especially with NATO.

According to its function as a key actor for capability development in the context of CSDP, the European Defence Agency (EDA) plays an important role in encouraging Member States' cooperation and coordination concerning capability development in cyber defence. Therefore EDA created a project team on cyber defence already in 2011. Furthermore, EDA works in close cooperation with the Member States and other EU bodies and institutions engaged in the issues of cybersecurity and defence, especially the EU Military Staff, the 2004 founded European Network Information Security Agency (ENISA) and the Commission. For example, EDA is participating in several cyber security projects launched by the Commission to evaluate their possible dual-use opportunities.

Although the CDPF and the initiatives of EDA pose important elements of progress towards a common European cyber defence policy, cyber defence still remains one of the most critical areas of shortfalls in capability development as stated by the annual report on CSDP. The projects launched by EDA mainly focus on training while the operational dimension of CSDP is still not comprehensively addressed as envisaged by the CDPF. In particular, a unified cyber defence concept for CSDP covering military operations and civilian missions is not yet formulated and the feasibility assessment of a cyber-defence training facility for CSDP remains to be completed. Likewise no CSDP exercise entirely dedicated to cyber defence has been conducted yet. For the time being there are only plans to include cyber aspects into the CSDP exercises MILEX 2015 and Multi Layer 2016. In comparison ENISA conducted pan-European cyber

security exercises in 2010, 2012 and 2014. Furthermore, promotion of a single market for cyber security products and fostering research and development as mentioned in the cybersecurity strategy needs to be intensified. This is especially necessary with regard to the development of the European Defence Technological Industrial Base thus reducing the risk of dependency on suppliers outside Europe.

Beyond the measures taken so far, there are additional issues that need open-minded discussions in the near future. First, since cyber defence capabilities evolved to an essential asset for crisis management, the option of developing cyber defence as an active, EU-owned capability for CSDP missions and operations should be thoroughly investigated. While the EU bodies could provide the infrastructure of such a cyber defence center, Member States would be required to deploy the necessary staff. Second, an open-minded dialogue concerning the development and potential use of offensive cyber capabilities as means of achieving operational goals within CSDP should be initiated. For example, cyber capabilities could be used to disrupt the communication of human traffickers in Libya to support the objectives of the EU naval operation Sophia off the Libyan coast. Third, the increasing utilization of cyberspace and social networks for information warfare as a central part of hybrid strategies demands the EU to develop a comprehensive strategic counter narrative addressing the external as well as the internal audience. This issue should be reflected in detail within the forthcoming framework on countering hybrid threats. Finally, following the invocation of the Mutual Defence Clause Article 42.7 after the devastating terrorist attacks in France and with regard to NATO's recognition of cyber-attacks as a case for Article 5 in Wales 2014, the upcoming debate on the Mutual Defence Clause of the EU should also take cyber-attacks into account.

# Towards a more consistent level of cyber defence capabilities across the EU



**Jorge DOMECQ**

Chief Executive of  
European Defence Agency (EDA)

## Introduction

No single country is capable of facing the wide range of today's security challenges in a full and comprehensive manner on its own. This is especially true in the case of cyber threats. Whether as part of a hostile hybrid campaign, or as an isolated malicious attack, cyber threats have the potential to severely and negatively impact a country's security. As they operate across borders, they must be tackled in a similar manner.

Budgetary constraints may impose limitations, and therefore lead to either defence capability shortfalls or obsolete technologies. Combining efforts and resources through defence cooperation is a clear solution to this, ensuring the availability of the right capabilities for Member States. The necessity for broader defence cooperation at the EU level and the need to work collaboratively to bridge defence capability gaps were indeed among the key motivations for the establishment of the European Defence Agency.

The cyber domain, interrelated as it is with information protection, is closely associated by the Member States with national sovereignty. With this in mind, the European Union and, accordingly, the European Defence Agency, have been advocating a well-balanced strategy for an open, safe and secure cyberspace. The

Cyber Defence Policy Framework, adopted in 2014, expanded on the concept and proposed - among other things - further development of cyber defence capabilities within the Common Security and Defence Policy (CSDP) context, promoting civil-military cooperation and synergies with wider EU cyber policies, private sector and international partners, as well as encouraging cyber education.

## The EDA efforts towards improving cyber defence capabilities

The European Defence Agency, the powerhouse for European defence capabilities, has a very important role to play as regards cyber defence capabilities. The EDA-led landscaping study conducted in 2011 indicated that the cyber defence capabilities of Member States were far from equal. Following the concept that "a chain is only as strong as its weakest link", the Agency has been addressing the identified shortfalls in order to leverage and further develop capabilities. Additionally, the Heads of States and Governments at the European

Council meeting in December 2013 identified cyber defence as one of four main programmes for the Agency to focus on. It should be stated, however, that the Agency's role is more that of a transmitter or facilitator of competences; it is the Member States who need to have the right arsenal and be in position to respond to emerging cyber threats.

The Agency's activities, in very broad terms, focus on the development of proactive and reactive technologies and the building of a cyber defence military workforce, as stated in the most recent EDA Capability Development Plan.

In accordance with the Cyber Defence Research Agenda, ninety-nine project proposals were put on the table for further consideration and prioritisation. The areas identified for the military to explore and improve within the Research & Technology domain contributed to the first cyber defence flagship project on Advanced Persistent Threats (APT) detection.





In the area of privacy protection, the EDA's focus has been placed on cryptology. The EDA intends to transfer well-developed academic expertise into innovative and market-competitive products, which can also be used by the military.

Pooling & Sharing is an important keyword for a number of the EDA activities. On the one hand, it is the most efficient and cost-effective way to share expertise and know-how among the Member States; on the other, it is fostering defence cooperation at the EU level. The Federation of Cyber Ranges is an effective implementation of the concept, allowing for the maximisation of available assets. The ranges are multi-purpose environments, enhancing knowledge development, assurance and dissemination. Accordingly, they may consist of three complementary functionality packages: Cyber Training & Exercise Range, Cyber Research Range and Cyber Simulation & Test Range functionalities.

Considering the importance of the human factor in tackling cyber threats, the Agency joined the cyber hygiene initiative of 2015. The

aim of the initiative is to set internal public sector guidelines for best practice behaviour against cyber threats by the end of 2016.

An elaborate "training needs analysis" resulted in an EDA-led series of training events. Three exercises have already taken place, addressing strategic senior decision-makers and their supporting staff from the Member States. When applicable, dual-use solutions have been promoted in order to maximise the training results, and also to underline civilian-military synergies.

Additionally, in order to meet growing expectations regarding developing and maintaining cyber situation awareness, the EDA has initiated the development of deployable Cyber Situation Awareness Packages (CySAP) for headquarters. These aim to provide a common and standardised cyber defence planning and management platform to assist decision-makers while on missions.

To this end, the EDA also offers direct support to Common Security and Defence Policy operations by increasing cyber defence

awareness as well as integrating cyber defence into military planning and execution of operations. This includes courses for the staff of the EU military operation in the Central African Republic (EUFOR RCA) and the southcentral Mediterranean (EUNAVFOR MED).

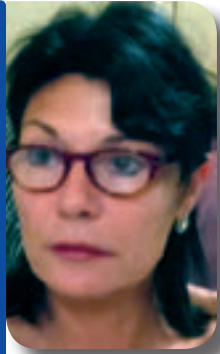
### Summary

The European Defence Agency is taking varied and multi-layered steps to properly shape defence capabilities in order to face the cyber challenges of tomorrow. Within the last four years alone, the Agency has completed or initiated cyber defence related projects with a financial volume of approximately two and a half million euros, which amounts to approximately 10% of the EDA's operational budget.

The aim is clear: to serve the Member States by offering them a wide array of available opportunities, thus gradually levelling out and enhancing cyber defence capabilities. If we are to do this in the most efficient and cost-effective manner, for the sake of European defence, the European Defence Agency is the most appropriate catalyser and booster for cyber competences.



# Mankind, sea, space and cyber defence



**Dr. Isabelle TISSERAND**  
Anthropologist

**W**e have chosen an anthropological and prospective approach in order to better understand the ins and outs of the relationship between Mankind, the sea, space and cyber defence the latest worldwide cultural creation.

This article also builds on our discussions with astronaut Jean-François Clervoy from the ESA (*European Space Agency*) and European Maritime Cluster President Francis Vallat.

Human and social sciences, as well as their representatives – who study Mankind in all its complexity and past, present and future developments – have been labelled as “soft sciences” for too long. This segregation, incited by fear – as these sciences aren’t subject to any taboo and because they encourage Man to continuously and fearlessly question himself by all possible means –, has been a considerable waste of time for a Europe that is advocating interdisciplinarity, after doing everything in its power to undermine these particular sciences.

Now, we are embarking on a new chapter in human history. If an archaeologist were to map all the cultural achievements on our planet Earth, he would say that we have everything at hand - or are about to have - and that time has come for us to transcend our limitations so as to, at long last, further explore ocean depths and venture deeper into space.

If an ethnologist were to record his observations, he would say that Man’s Earth, the

sea and space are crisscrossed with cables, networks, satellites and terminals that allow the information and many other actions, including interpersonal relations, to be dematerialised, and he would also argue that these connections have dramatically altered our frame of reference.

If a sociologist were to participate in this study, he would state that anything recently built should be secured through cyber defence, the same cyber defence the great powers have been striving to develop because they rely on the effective functioning of essential operators.

If you were to ask a psychologist for his opinion, he would claim that confinement is a state that characterises many human activities in this era of man-machine interface (computer, mobile phone, tablet), be that aboard ships or human space flights.

The success of this new human, sea and space enterprise will not only require technological progress, but, above all and more than ever before, it will have to be based on a prospective human and social understanding and preparation for the future of Mankind in a globally connected and networked world that has changed rapidly, with little or no resistance from anything or anyone.

As for the numbers regarding the human race, they speak for themselves: the world population reached an astonishing 7.35 billion in August 2015, recording a 1 billion increase in the past twelve years<sup>1</sup>. The average age of the world’s population today is 29.6 years. Global population is set to hit the 8.5 billion mark by 2030.

We will need to be anthropologically, socially, politically and economically organised because new waves of migrants will keep going. So how will life on earth remain possible and well-balanced? How will we protect our species and ensure its evolution without cyber defence?

In this respect, the sea represents an immense hope. Francis Vallat has reminded us in a recent study<sup>2</sup> that the turnover of sea-related activities will exceed 2,500 billion euros within the next ten years. This will be made possible thanks to the new sea-based industry: renewable marine energies, deep seabed mining (food and mineral resources) and biotechnologies.

1 Béchir Ben Yahmed, *La revue pour l'intelligence du monde*, September-October 2015.

2 *Sécurité Alternative*, Editions l'Harmattan, Paris 2014, page 177.



Vallat doesn't hesitate to claim that the 21<sup>st</sup> century will be the most maritime century in history and that the principle of *Freedom of the seas*<sup>3</sup> should be taken into consideration more than ever while being applied in such a fashion that too much freedom doesn't kill freedom (at a time when oceans themselves are threatened).

The same goes for space: Jean-François Clervoy has recently reported that "in order to ensure the long-term survival of the human race, Man should learn to live elsewhere"<sup>4</sup>. However, on the subject of long space voyages to Mars, he emphasises that the connection problems with planet Earth involve fundamental questioning and that the need will arise to train humans to realise that life on Earth - which they won't be able to see any more given the distance -, is over: "their home planet will be their spacecraft from then onwards"<sup>5</sup>. All of this calls for increased cyber defence capabilities.

Cyber defence's primary objective is to protect technological, numerical and digital artefacts crucial to the functioning of human activities of small, medium, high and par-amount importance.

Without it, not only will there be no strategic development projects, but the prospect of extensive destruction of vital infrastructures will loom and threaten the human race to return back to the Stone Age, as Jean-François Clervoy puts it.

Cyber defence rests on new and crucial human activities which are partially mobilised on the security of terrestrial, maritime and space activities.

However, as cyber defence is becoming more and more part of our lives, it is obvious that we aren't devoting adequate time to teaching it with the view to properly integrating it into our education system and culture, nor are we working on the necessary developments with

regard to managing the cyber defence actors. Some of these actors are part of the new generation that human and social sciences have observed as pushed around, even sacrificed and in some way abdicating, as evidenced by the fact that they often tend to expatriate themselves after graduating.

Only when cyber defence is smartly integrated into our ways and when our vital infrastructures are protected using interdisciplinarity will then Man be able to focus on exploring new frontiers, in the hope of either preventing his extinction or preparing the human species to swarm elsewhere, which isn't necessarily programed in its genes.



<sup>3</sup> *Freedom of the Seas*. This principle stresses freedom to navigate the oceans. It also disapproves of war fought in water.

<sup>4</sup> Jean-François Clervoy, *La revue pour l'intelligence du monde*, September-October 2015, page 12.

<sup>5</sup> *Ibid*, page 15.



# Ensuring a high common level of network and information security across the Union



**Pilar DEL CASTILLO**

*Member of European Parliament, (EPP Group) Rapporteur concerning measures to ensure a high common level of network and information security across the Union*

**B**y 2012 the European Institutions had focused their attention on the cybersecurity challenges and had acknowledged that Member States had not the proper coordination to properly respond to a transnational challenge that grows every day.

The figures are eloquent: Currently there are more than 150000 types of computer viruses, the World Economic Forum estimates in 10% the possibility of critical networks

infrastructures being interrupted in the next ten years causing damages of up to 250 billion dollars, according to Symantec victims of cyberattacks globally suffer yearly losses of approximately 290 billion Euros, and according to “Verizon’s Data Breach Investigations Report” between 2013 and 2015 personal data compromised by cyber incidents grew 78%.

Taking into account that reality, the European Commission, in February 2013, published a proposal for a Directive on Network and Information security (NIS) accompanied by a Communication establishing a Cybersecurity Strategy for Europe. On the 7th of December 2016 the negotiating team of the European Parliament and the Luxembourg Presidency of the Council reached a political agreement that will be ratified by the Council and the European Parliament by the 1st quarter of 2016.

The NIS directive is the first legislative piece on cybersecurity to be applied in the EU and is structured in three areas.

Firstly it establishes obligations requiring that operators of critical infrastructures (energy, transport, health and financial services) and key digital service providers (search engines, ecommerce platforms and cloud computing providers) implement security measures, based on state of the art technologies, and notify security incidents to national authorities.

Secondly, Member States will design horizontal national cybersecurity strategies and designate Computer Security Incident Response teams (CSIRTs) to analyse and monitors threats and, eventually, respond to cyberattacks. In addition Member States will have to identify Single Points of Contact that will coordinate the information received from market operators and communicate with their counterparts from other Member States.

Finally, the directive establishes two channels for Member States to cooperate, and exchange information and best practices. A cooperation network, constituted by national authorities, and a more technical body formed by Member State CSIRTs, which, in addition to exchanging information and best practices, will undergo simulation exercises.

The NIS directive constitutes a first important step in comparison to the prior situation, where information amongst Member States only flows voluntarily and where national capacities and the preparedness of the private sector vary greatly. In sum, from now on, the European Union will be better equipped to face the constant threats to which cyberspace is confronted, and by doing so, allowing a safer environment for the digital economy to grow.



# Cybersecurity: Global solutions for a global issue



**Houlin ZHAO**

*Secretary General, International  
Telecommunication Union (ITU)*

Cyberspace is evolving at a tremendous pace, and the immense opportunities it brings also come with equally substantial challenges in terms of building trust and confidence in information and communication technologies (ICT).

In today's world, everything depends on ICTs – and particularly on the networks which underpin them. This includes essential national infrastructure and services, such as emergency services; water supplies and power networks; food distribution chains; aviation and shipping; navigation systems; industrial processes and supply chains; health care; public transportation; government services; and even our children's education. Increasingly, with wearable technology, the Internet of Things (IoT), and embedded ICTs everywhere, cyber-incidents will have greater effects in the physical world. Therefore, it is no longer just about money and data – however important these are – now it is also about lives.

Securing cyberspace is a global issue and requires global solutions. We are as strong as our weakest link, and in this interconnected world, this weak link could be in any part of the world. Therefore, our common global goal of ensuring trust in cyberspace cannot be achieved by just a set of countries or a set of stakeholders working by themselves. This holds true as much for Europe as for any other part of the world.

Europe has emerged as a pioneer and a leader in technology-related public policy matters. It has strong mechanisms in place for regional discussions on cyber issues, and also closely cooperates with a number of partners.

While this is commendable, it may not be sufficient. It is important to realize that in cyberspace, vulnerability can come from and be exploited from anywhere. Therefore, a vital part of the European cybersecurity strategy should be its global commitment to help ensure cybersecurity everywhere – not because of altruism or developmental instincts, but also because this is the only way to ensure that European citizens can enjoy the cyberspace with trust. Europe has become a benchmark for many Member States in other regions to emulate, and it must fulfil this role by helping others.

The only way to secure cyberspace is for everyone to work together – all stakeholders from all nations.

The United Nations plays an important role in this regard as a global convener and facilitator for different stakeholders to come together to discuss, identify and implement solutions towards building a universally available, open, secure and trustworthy Internet.

As the oldest member of the UN family – ITU celebrated its 150th Anniversary on 17 May this year – and the UN's specialized agency for ICTs, the Union is honoured to continue playing its part in bringing the benefits of secure and trustworthy ICTs to all – through the coordination of global resources, including spectrum and orbital slots; through standardization; through development support; and by convening policy dialogue.

Over the last two decades, ITU has worked under its mandate on several aspects of building confidence and security in the use of ICTs, including cybersecurity. The World Summit on the Information Society (WSIS) was initiated by ITU in 1998 in response to the growing spread of the Internet worldwide. In close collaboration with the entire United Nations family, ITU organized the two phases of WSIS in 2003 and 2005, which established a common vision for the information society. It was the most wide-ranging, comprehensive and inclusive debate ever held on the future of the information society.

At the Summit, Heads of State and Government entrusted ITU to be the facilitator of WSIS Action Line C5 on building confidence and security in the use of ICTs. In fulfilling this role, ITU has placed particular emphasis on helping countries overcome substantial challenges in terms of building trust and confidence in ICTs, especially in the development of human and technical capacity.

ITU has focused on assisting Member States in defining a national strategy on cybersecurity, raising awareness in key stakeholder communities, conducting training workshops, developing programmes for child online protection, and establishing national computer incident response teams (CIRTs) as well as facilitating their international collaboration, amongst other activities.

ITU's technical study groups provide a neutral, global platform for all stakeholders to come together and work on security-related standardization on a variety of topics, including security architectures and frameworks; identity management; the security of applications and services for IoT; and smart grids.

ITU is also playing a very active facilitating role within the United Nations System, working closely with other agencies and bodies to improve the UN's internal coordination activities on cybersecurity.

Following the endorsement of the post-2015 sustainable development agenda in September 2015, ITU will reinforce its coordinating and facilitating efforts in order to continue building confidence and security in the use of ICTs, as an acknowledged component of global development efforts.

Throughout its 150 years, ITU has benefitted from the active contribution of the Europe Region Member States to its policy-setting work and project implementation. ITU looks at Europe as a key partner in its efforts in assisting countries around the world to be better prepared to tackle challenges arising from ICT development.

ITU welcomes and looks forward to a fruitful collaboration that would allow the ICT sector to reach its full global potential and bring its enormous socio-economic benefits to every corner of the world.

# EU-level Cyber Crisis Management



**Prof. Dr. Udo HELMBRECHT**

*The Executive Director, EU Agency for Network and Information Security (ENISA)*

## Introduction

The societal developments of the last decade have made Information and Communication Technology (ICT) systems a crucial part of our daily lives. The last decade has brought new possibilities and produced unprecedented developments within the areas of communication and information sharing. However, these developments have at the same time brought with them new risks and threats. Today, European societies require functioning ICT infrastructures and services. Reliance on ICT and cyberspace have been increasing and continues to grow rapidly in many other critical sectors, such as Energy. This entails that vulnerabilities in the systems can have great consequences, both for individuals as well for societies at large.

A crisis is an event that is unexpected and far removed from the ordinary and mundane, affecting many people and large parts of society while threatening fundamental values and functions that cannot be handled with ordinary resources and organisation, and that requires coordinated action from several actors [1]. Cyber incidents are commonplace [2] and the likelihood for a crisis to be caused by one or more of these incidents increases every day (see incident escalation Figure 2). There is a high possibility that even terrorists may try to launch a cyber-attack against the control system of an electrical grid or of a nuclear plant.

Because of the borderless nature of cyber incidents, their mitigation requires multinational cooperation; the EU is ideally placed to foster cooperation between governmental and non-governmental bodies at the national as well as international level in that regard. This is notably demonstrated by the numerous crisis management frameworks in place at EU level which structure such coordination in their respective sectors. Unfortunately, because of their sectorial limitations, none of them fully absorbs the cross-sectorial nature of the threat posed by cyber incidents.

From a general crisis management perspective, there have been significant achievements both within EU Member States and at the EU-level. The principles of crisis management have been reflected in national strategies and policy documents, focusing on crisis prevention, preparation, response and recovery. Education, training and exercises in cooperative mechanisms for cross-border and

sector dependent crisis management have also taken place. To what extent have these achievements and knowledge been transferred to cyber-related crisis management? What characteristics can be identified within cyber crisis management that bring to light similarities or differences with the more well-known general crisis management? To what extent do the cooperation mechanisms resemble cooperation within crisis management?

## EU-level Political Crisis Management

In recent years, the need for a robust EU-level response mechanism to manage cross-border threats has become overwhelmingly apparent within several sectors. The challenges faced by the EU and the Member States in coordinating a common response have been highlighted as a result of a number of crises, in particular, the volcanic ash cloud over Iceland, pandemic diseases, terrorist attacks and the migrant crisis.

In the aftermath of the terrorist attacks in Madrid (2004) and London (2005) [3], the tsunami in the Pacific and the Indian Ocean (2004) [4], the EU set up its Emergency and Crisis Coordination Arrangements (CCA), to enable the Institutions and its Member States to provide a strategic and political response to crises in a coordinated manner. In 2013, the Council approved the EU Integrated Political Crisis Response (IPCR) [5], the update to the CCA following the Lisbon Treaty and in particular the Solidarity Clause. The latter treaty stipulates that the role of the EU is to facilitate

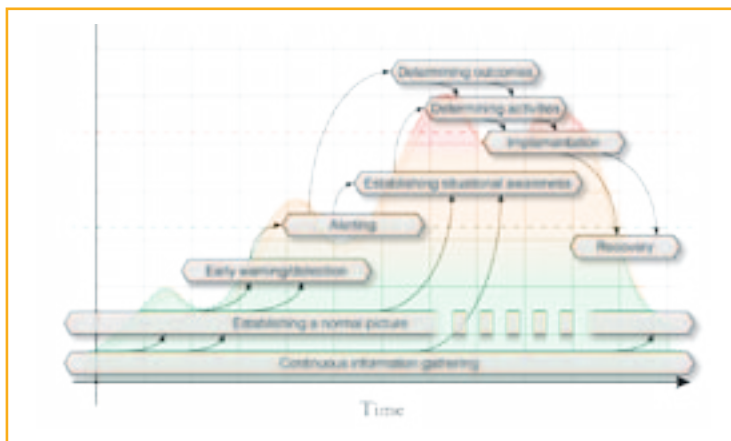


Figure 1: Practical crisis management activities overtime (source ENISA [1])

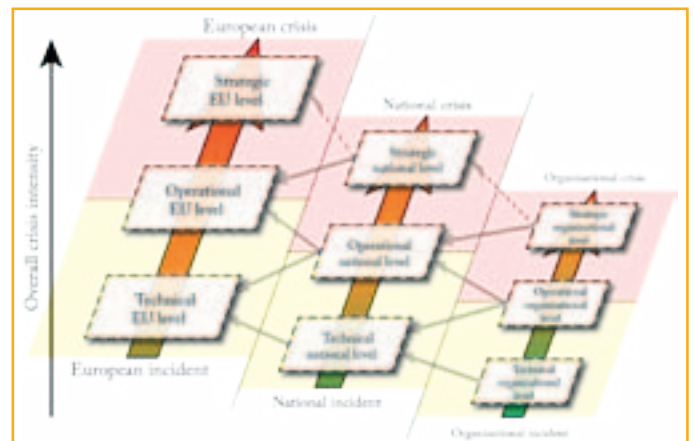


Figure 2: Crisis escalation: from organisation to national and EU levels (source ENISA [1])



cooperation between Member States, complementing national policies especially to cover monitoring, early warning, and combating serious cross-border threats. In this regard, the IPCR can be seen as the EU's ambition to have a coherent response during crises, avoiding unnecessary duplication of efforts. As of then, in the event of a crisis, the Council Presidency, possibly at the request of the affected Member State(s), activates the IPCR. The Presidency further gathers advice and support to develop proposals for action to be presented to the Committee of the Permanent Representatives of the Governments of the Member States (COREPER)/the Council of Ministers and even the European Council [5].

In parallel, the European Commission developed a procedure to produce Integrated Situational Awareness and Analysis (ISAA) reports [5] that can support decision making at the highest level, based on inputs from the Member States but also very much from the Institutions services, Directorate Generals and Agencies. Depending on the sectors affected, legal and operational frameworks in place between Member States and these services allow for information exchange and crisis coordination at operational level, before strategic discussions take place in the IPCR process.

### Recommendations for efficient EU-level Cyber Crisis Management

Despite a number of initiatives within the European Network and Information Security community to establish frameworks and standard operating procedures, **the EU-level response to cyber incidents**, and in particular these which lead to crisis situations, **lacks consistency**. Today, should a crisis arise from a large-scale cyber incident, Member States would lack a harmonised framework to effectively respond to the challenges posed by this incident.

**The formalisation of a legal framework with regards to EU-level crisis management has drastically increased the efficiency of the European response to crises in all critical sectors, other than cyber.** Clearly defining the roles and responsibilities of the key actors may speed up the response time considerably when faced with a crisis situation. Conversely, the lack of it is seen as an impediment for the relevant bodies to operate effectively as they lacked a common strategy and were not legally mandated to do so. Lastly, in areas related to sovereignty, it is recognised that **trust** is a significant issue which legislation can help improve, though not enforce. It is highly **recommended** to *revise the current EU legislation with regards to crisis management to better reflect upon the separation of causes and impacts and leverage the development of the field of cyber crisis management as an essential*



*tool in the mitigation of crises induced by cyber incidents.*

Looking at **governance issues** under the operational framework, **it is clear that there is significant added value for EU Member States when EU bodies and Agencies with EU-wide competencies act as a facilitator** for information sharing and resource pooling. One of the most prominent examples is the role of Eurocontrol during crises in the aviation sector. Crisis management should remain in the hands of Member States, but crisis coordination at EU-level is naturally best handled by EU bodies. One of the **main challenges** identified is the occasional **lack of consideration** for the capabilities of the EU-level body, and the fact that **multinational crisis management is not always a priority** for individual Member States. Independently from the entering into force of the Network and Information Security Directive it is highly **recommended** to *develop and formally adopt an EU-level crisis management plan specific to crises induced by cybersecurity incidents.*

Also, it would be advisable at an early stage to build upon the lessons learned from other sectors, such as aviation and border control, and attempt **to create an EU-level pool of cyber crisis experts**, which role would be first and foremost to **exchange information and best practices** in the event of cyber incidents and related crises. In this context for the efficient cooperation of experts is

**recommended** to develop and formally adopt EU-level Cyber Crisis Cooperation Standard Operating Procedures.

### References

- [1] ENISA, "Report on Cyber Crisis Cooperation and Management," European Union Agency for Network and Information Security, November 2014 (Available at: <https://www.enisa.europa.eu/c3/nis-cooperation-plans> [Accessed: 10 Dec 2015]).
- [2] ENISA, "Threat Landscape report," European Union Agency for Network and Information Security Agency, Brussels, 2014 (Available at: <https://www.enisa.europa.eu/media/press-releases/enisa-draws-the-cyber-threat-landscape-2014> [Accessed on: 10 Dec 2015]).
- [3] E. C. European Parliament, "Directive 2009/136/CE du Parlement Européen et du Conseil".
- [4] E. Council, "Council Decision of 23 October 2001 establishing a Community mechanism to facilitate reinforced cooperation in civil protection assistance interventions," EU, Brussels, 23 October 2001.
- [5] E. Council, "The EU Integrated Political Crisis Response Arrangements," EU, Brussels, 2014 (Available: <http://eur-lex.europa.eu/legal-content/EN/NOT/?uri=celex:32014R0970>. [Accessed 23 11 2015]).

# Providing and managing information security



**Gerold HUEBNER**

*Development Executive, Chief Product Security Officer, SAP Global Security*

Digital attacks on companies and public services have increased dramatically - not only in number and complexity but also in finesse. Today, the question is no longer whether a company will be attacked, but when this will happen and to what extent. This means that security cannot be a secondary concern. Security requires fundamental attention to people, processes, and technology. It is essential that **information security** evolves from an IT focus to being at the core of critical operational decisions for government and business.

The term "cyber security" is widely used today primarily linked to security issues related to the Internet. It refers to the technologies and processes designed to protect computers, networks and data from general cyber threats

(such as unauthorized access, vulnerabilities and attacks delivered via the Internet by cyber criminals). SAP, in addition, needs to focus on security of business applications as these provide the fundamentals for our customers' core business processes. By their nature, SAP's business applications are much closer to customers' business processes than to their infrastructure such as networks and operating systems. As a consequence, the risk of a successful attack would not be mitigated adequately if SAP would merely rely on countermeasures, such as firewalls, network security and anti-virus software. Additional threats could be posed by lack of staff awareness, insufficient authorization and control points, or insider threats - to only mention a few - and these potential threats must be managed. This is why we at SAP rather more concretely talk about information security and not "cyber security".

Security remains a neck-and-neck race between hackers and software vendors and cloud service providers. SAP has a long tradition of clearly understanding its customers' expectations in the context of confidentiality, integrity, and availability when customers entrust their business to SAP software systems and services. Customers can rely on the fact that SAP constantly monitors the evolution of the threat landscape, adjusting countermeasures to mitigate evolving threats. At the core of these countermeasures, SAP has defined and implemented a company-wide strategy to systematically counter risks to information security our customers' might be facing which is based on three pillars: "Prevent- Detect - React":

The "Prevent" pillar encompasses all measures that are put in place from the very beginning of a product's lifecycle. Baking security in from the first thought about a product has been proven to be the most effective way to ensure a high security level. This spans from secure architectures and developing secure code to enabling SAP's staff by continuous training and awareness campaigns, defining and implementing the necessary processes and controls, the deployment of strong security features and providing an integrated tool landscape. "Prevent" is complemented by SAP's security research team investigating the latest security trends and features to be embedded into SAP's products and solutions.

Within the "Detect" part of the security strategy, SAP focuses on an early detection of deviations from what has been defined within the security framework laid out in the "Prevent" section. This includes, but is not limited to, an ongoing analysis of the threat landscape outside of SAP to prepare for adequate countermeasures - for example, by social media analytics to detect security issues discussed or communicated on the Internet within the security researcher community at an early stage. It also comprises technical measures such as a dedicated application to continuously monitor an entire system landscape for harmful events - this is "big data" analytics for security. This application (Enterprise Threat Detection based on SAP Hana) is also made available to customers.

At the core of the "React" pillar, SAP has set-up a mature organization to immediately react upon and professionally manage security

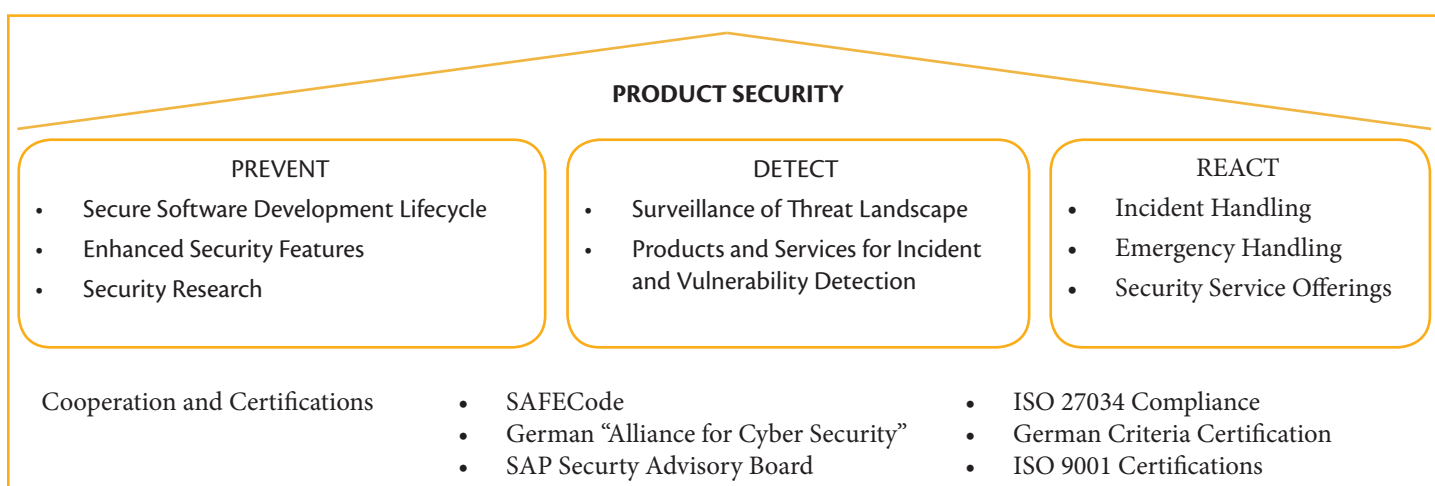


Figure: SAP Product Security Strategy

incidents. This ranges from detected vulnerabilities, the handling of security threats and incidents on an infrastructural layer with potential impact on both SAP's internal IT infrastructure as well as the cloud offerings as well as incidents that happen in SAP's business environment such as attempted social engineering attacks or an attempted break-in to SAP facilities. It also includes all relevant measures to inform and protect SAP's customers – for example, by means of SAP's monthly Security Patch Day. Security is a joint effort. Many public-private partnerships and collaborations for understanding new security requirements and threats, especially for critical infrastructure, have been in existence for decades. Substantive cyber security issues that affect the digital ecosystem and digital economic growth should be addressed based on broad consensus, coordinated action, and the development of best practices that will substantially improve security for organizations and consumers.

SAP stays in close contact with security experts in companies and associations all over the world. This is so that SAP can stay at the cutting edge of knowledge about current threats and the state-of-the-art knowledge

to prevent even sophisticated attacks. SAP actively collaborates in a variety of international professional and governmental organizations, such as BITKOM, TeleTrust, the European Union Agency for Network and Information Security (ENISA), SAFECode, European Commission: Workgroup Cloud Select Industry Group (C-SIG): Security and Information Governance, and the German Alliance for Cyber Security.

SAP joins forces with computer emergency response teams of governments and other global players to be able to exchange information on attacks as quickly as possible. As a founding member of SAFECode, SAP contributes to actively educate the software eco-system on the topic of secure coding and supply chain security. "Deutschland sicher im Netz" translated "Germany secure in the net" is a great example, on how SAP supports Internet security for children, the citizens and small and medium businesses in Germany in a public-private partnership.

SAP has a continuous exchange with governments to increase awareness toward business application and information security. When setting policy and designing procurement rules, it is essential for governments

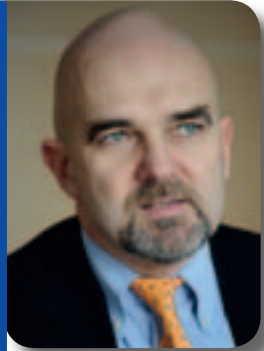
to maintain a position of neutrality and avoid mandating use of technologies or technical standards. Procurement rules should be based on a balanced risk view of all relevant factors rather than being prescriptive to one, particular security risk or security level. The development of common standards for risk management and security measures at the international level is crucial and well developed but allows for the independence of organizations to apply controls appropriately and based on their risks assessments.

Policies must enable governments to respond to actors, threats, and incidents domestically and internationally. Generally, existing legislation covers the activities of cyber criminals and terrorists as well as fraud and theft, for example. Legislation in the field of information security should focus on ensuring that critical infrastructure providers are concentrating on truly essential services that have appropriate network and information security measures in place. If necessary, material law must be updated to cover computer misuse and criminalize harmful hacking not done for testing and threat research.





# Towards a Public-Private Partnership on cybersecurity and beyond



**Luigi REBUFFI**

*CEO of European Organisation for Security, whose membership includes Europe's major companies and research centres representing two-thirds of the European security supply market.*

In light of the acceleration of the digital transformation and the construction of a European Digital Single Market (DSM), the urgency to implement strong protective measures of our data and network information systems against attacks and leakage is imperative. Europe is facing new challenges which affects not only its economy and security but more importantly have deep ramifications into its core values and civil society.

The European market for cybersecurity products is dominated by global suppliers and Europe is lagging behind. Low efficiency, technological dependence, privacy concerns and market fragmentation (at EU and national level) make the challenges even greater. Moreover, trust and information-sharing across countries still remains a concern in the development of an EU cybersecurity platform.

Against this grim overview of the current situation, Europe seems to have lost many battles but it has, however, not definitely lost the chance to build a leading "Smart and Secure Digital Europe".

## Europe as a potential market leader

Europe has several thousand innovative SMEs with great potential but too few opportunities to grow in this fragmented market. Even though Europe has not a leading role in certain mature ICT domains and applications, there is still time to recover this situation by

focusing innovation and investment in new ICT areas currently under development like the Internet of Things, Cloud Security, Big Data, Mobile and the Cyber Physical Systems, etc., in which Europe can still claim a leadership position.

We are not missing ideas, but we are lacking political and financial support for the development of our industry and a harmonised market. Today's considered investments in Europe would not be enough to close the widening gap of research and capacity-building with the U.S, which has envisaged a federal budget for "cybersecurity" of \$14 bln, in majority for "defence" applications for 2016. This gap, if not contained in time, would widen the already critical divide we have in ICT and ICT security. The question we need to ask ourselves today is how Europe can overcome these challenges and control its data when it is not even controlling its own ICT infrastructure and services, as revealed by the Snowden case. For that, we must reconsider our future investments, focussing them towards priorities which would have a real and positive impact for the creation of jobs and growth and the protection of our cyber space.

## Public-Private Partnership (PPP): a first step

To reach this goal, the European cybersecurity PPP to be set up in 2016 is a major opportunity to build a stronger technology base, leveraging upon an industrial strategy to effectively meet the interests of Europe and better contain the "digital colonisation" from non-EU countries.

The foreseen PPP will primarily support the improved coordination of Research & Development (R&D) activities, and a structured public-private dialogue for the protection of the DSM. This scope, however, might remain insufficient as there is an urgent need to better consider and support the competitiveness of Europe by building a genuine European cybersecurity industry supported by harmonised investments in capacity building.

## Looking ahead: EOS' response to ensure a "Smart & Secure Digital Europe"

EOS has developed a full "cybersecurity Flagship Initiative" based on a unique in-house

study of the European cybersecurity market. This initiative, starting with the envisaged PPP and supported by an overarching EU cybersecurity industrial policy, would allow, by 2025, our industry to become a world leader in key strategic sectors, implementing trusted European cybersecurity solutions and assure a greater digital autonomy. In this Flagship approach, EOS calls for a targeted investment of € 13 bln over 10 years both for research and capacity building.

In view of rapidly emerging threats, we must plan the next coming years in a smart and strategic way. Massive investment campaigns to build all the supply chain for IT components and services in Europe would demand a too large effort. Instead, we need to cooperate with non-EU companies in order to protect the growth of the DSM. In this case, a good balance must be found between the use of certified trusted non-EU technologies and the development of European solutions in vital areas (e.g ICT infrastructure and public services), in applications where Europe is a market leader (e.g aeronautics, car manufacturing, finance services and all sectors falling under the Industry 4.0). In parallel, areas of higher competence in Europe like Identification and Access Management (e.g smart cards) as well as Data Security (e.g. encryption) should be continuously improved to maintain leadership, while competitiveness should be increased in strategic components for Network Security Systems and Management of Security Services.

Moreover, EOS also advocates for the creation of a European cyber ecosystem starting with citizens' education in schools, providing training for professionals, and increasing awareness on cyber threats for decision-makers. This ecosystem would allow the creation of investment funds, like in the U.S, to support growth and competitiveness of our industry and in particular of SMEs.

The findings of the EOS study show that the cyber "war" is not yet lost, but concrete actions need to be taken to raise Europe to the level it deserves in the global cyber chessboard. All this is possible with a political agreement among Member States and sufficient strategic investment.

# Data protection and a secure information environment for consumers go hand in hand



**Giovanni BUTTARELLI**

*European Data Protection Supervisor (CEPD)*

**T**he digital environment is developing rapidly. Big data is the perfect metaphor for understanding what is actually happening. Big data means the collection and use of massive amounts of information in an era where individuals are constantly connected. When this information is combined and analysed in an intelligent way, this could greatly benefit our societies. The use of big data in health care is a good example. Big data could lead to significant improvements in the prevention and treatment of diseases based on an analysis of huge amounts of information. It can also help to prevent or detect an individual contracting a disease by combining patterns in personal information concerning him or her.

Another example is consumers enjoying a wider choice of goods and services online based on their personal preferences collected by internet companies. One of the great attractions of the internet is that consumers do not pay money for many of the services they receive. The price for enjoying these services, however, is the requirement to hand over personal information. And this personal information is subsequently used for various purposes, typically described in terms such as 'improving the customer experience'.

It is my mandate as European Data Protection Supervisor to promote strong privacy and data protection in a world where people exchange ever more information. It

is important, in the exercise of my mandate, to acknowledge that big data does not only involve benefits, but also risks for society, because revenue streams and product development in the big data economy often depend on the processing of vast amounts of personal data.

Privacy and personal data protection are essential values in our democratic societies and are, as such, included in the Charter of the Fundamental Rights of the European Union. Privacy and data protection are expressions of people's dignity and autonomy. Obviously, this goes beyond the protection as consumers in online markets. Changes in our society and the economy do not change the importance of privacy and data protection.

Another connected risk relates to the security of information in cyberspace. In order to deliver better health care on the basis of data analytics, a lot of data needs to be available. Moreover, the analytics itself produces new information. Free internet services, too, generate personal data. More data enhances the security risk. The phenomenon of identity theft illustrates this. Where personal data is widely available, it is more complicated to protect this data and to ensure that the internet is secured and identities cannot be stolen.

A secure internet environment is a prerequisite for the functioning of our digital economy, and equally for people's privacy. There is a close link between security as an economic driver and privacy.

Also the Court of Justice of the European Union recognises this link between protection and security. The data retention ruling, a recent landmark case in my working area which led to the annulment of the European directive on the retention of telecommunications data for police purposes, contains an interesting consideration from this perspective. The Court analysed what should be considered the essence of the individual's right to data protection, concluding that technical and organisational measures taken to safeguard the security of information belong to the essence of this right. The citizen may, as part of his right to data protection, expect from companies - and from governments - that they

take the proper measures to secure his or her data.

In short, effective data protection and security go hand in hand. This link will even be stronger under the new General Data Protection Regulation. This regulation includes a number of instruments that directly relate to security. The most obvious of these instruments is the obligation to notify data breaches. Under the new law, a company must notify, within 72 hours, a data leak to the national data protection authority. This obligation, which already exists in most parts of the United States, should lead to a more secure environment. Companies, and governmental bodies, are expected to be more vigilant, to avoid the risk of having to go public when there is a data breach.

Another instrument which will be included in the new law is known as privacy by design, ensuring that considerations of privacy and data protection are built into the design of technical systems.

Breach notifications and privacy by design are examples of measures which are tailored to promote internet privacy and data protection and, at the same time, online security.

Technology can help achieve both these objectives. The EDPS strategy prioritises privacy engineering and encourages IT developers and designers to apply privacy by design and privacy by default. There is also a need to integrate privacy and data protection into all phases of development of systems, services and applications.

Making systems more data protection friendly also makes those systems more security proof, making the data less prone to abuse by cybercriminals.

# Challenges of cybercrime - Chances for cybersecurity



**Monika HOHLMEIER**

*Member of European Parliament  
(EPP Group)*

**P**eople, businesses, governments - they all are increasingly dependent of electronic networks, communication technology and information systems. Every day a huge and increasing mass of data is moving over IT networks worldwide. However, they all - people, businesses and governments - face the same threat of criminality in cyberspace.

The three most common areas of cyber criminality are cyber-attacks, payment fraud and the distribution of illegal online content,

including child sexual abuse material and incitement to racial hatred or to terrorist acts.

A typical characteristic of cyber-attacks is the loss of control over the own data by the user, business, bank or public institution. Hackers block the access to the data, change their content or steal valuable information (e.g. from credit cards) or other personal information about the user. Every day thousands of new forms of malware are created. Some years ago the malware tools have exclusively been executed by IT-experts. Times have changed, the Crime as a Service-model (CaaS-model), challenges cyber-users more and more often. Clients of CaaS-networks can buy a kit of services and products which are easy to handle even for non-professionals (e.g. DroidJack).

When it comes to the distribution of illegal online content, especially child sexual exploitation material, the modus operandi of criminals to hide their criminal activity develops in line with the possibilities of technology and with the increasing number of clients for sexual abuse material. The most common threats in this context are based on the P2P-Environment, the Darknet and live-streaming. The variety of tools to enhance anonymity and non-traceable payment possibilities make it extremely difficult for law enforcement authorities to track down the distribution of abusive content. The safer the

criminal abusers feel the more children are abused and the more child abuse networks and material occur. On most of the child abuse forums the production of fresh material is demanded as a condition for membership. Besides, the migration flow with an enormous number of children without parent and family relatives create unbelievable opportunities for terrifying crimes. The nameless children are the most vulnerable group in the world and most people are not aware of this horrific situation. Studies show, that the latest trend in this area are practices beyond cruelty, such as live streaming of on-demand abuse of children. According to Europol, this practice is likely to grow, fuelled by increasing broadband coverage in developing countries. Therefore, the sentences for clients asking for snuff-films or other severe sexual abuse material have to be sharpened massively. Law enforcement has to be more strict and consequent for all kind of sexual abuse as well as for all kind of facilitating and distribution of sexual abuse material and their clients. Severe legal consequences are part of a prevention strategy against future networks alongside with low-threshold offers of therapy for people who feel sexually attracted by children.

The challenges for law enforcement authorities in the fight against cybercrime are borderless in geographical terms and unlimited in scope. Law enforcement authorities fight





against a constantly developing tool set of internet services and the ingenuity of cybercriminals for whom every law enforcement success is a motivation to create even more sophisticated technology or encryption. Europol's Cybercrime Center (EC3) has been playing a key role in the fight against cybercrime since its establishment in January 2013, pooling European cybercrime expertise to support Member States' cybercrime investigations with great success. In addition to that, in July 2015 Europol started the pilot project of the Internet Referral Unit (EUIRU) with the mission to combat the threat of online radicalisation by identifying and tackling terrorist propaganda and related violent extremism on social media and other internet services. However, also for Europol, the fight against cyber criminality regularly meets a number of practical and technical obstacles.

Cybercrime is often underreported. In many cases, companies fear a loss of reputation, economic disadvantages or retaliation over the internet. It is nearly impossible to precisely determine the damages cybercrime causes in the EU. Most figures in the different publications can only be a rough estimation. To commit a crime in the cyberspace often has no judicial consequences and thus is very attractive for criminals. While some crimes are clearly specific to the internet and as such attributed to the category of cybercrime

(f.i. attacks against information systems via malware or phishing), others are only internet-facilitated, enabling traditional crimes to be committed on a large scale with less risk of persecution by the security authorities. In the case of industrial espionage a very technical obstacle is the lack of basic definitions and legal consequences. Industrial espionage is as old as industry itself, but has evolved from a small to a large-scale business "thanks" to the cyberspace. According to the joint report of the Centre for Strategic Studies (CSIS) and the McAfee Company in 2014, cyber espionage can cost up to 1,5 % of a country's GDP. In fact, industrial espionage can be led by single players and state actors. So far no answer has been given neither on European or international level (e.g. an inclusion of such a principle would be possible in the WTO agreement TRIPS or bilateral agreements) on how to sanction state perpetrators.

The EU and the Member States have put into place, a number of strategies and legislation to step up against cyber criminality and make the internet a safer place for private, industrial or public users. While it is extremely important and necessary, that adequate resources are given to prevention strategies in order to raise awareness of cybercrime and increase standards in online safety and information security, the key to tackle cyber criminality and to dismantle cybercrime

networks lays in cooperation on national, European and international level including public-private partnership. The internet and cyber criminality don't know borders, law enforcement does. We have to improve our international cooperation quickly. Member States should proactively share criminal intelligence related to cybercrimes with Europol and with other Member States via Europol or ENISA (European Network and Information Security Agency). The sharing of information and tactical analysis is crucial to better enable successful operations and coordinate law enforcement action. The ingenuity of cyber criminals often only extends to updating existing tools and methods by finding new ways to use and implement them. Thanks to Europol and national cyber security units, the EU has improved their technical capability and the number of skilled specialists. However, the fact that EC3 has 80 staff (17 for the IRU) to cover the whole EU-territory and a yearly operational budget of 10 Mio. Euro (2, 5 Mio. Euro for the IRU) clearly show that EC3 and EUIRU are underfunded and outnumbered by cybercriminals. The European Commission and Member States will have to double the staff in the near future in order to give Europol the necessary tools to keep pace in the fight against the most modern large-scale cybercrime in cooperation with the Member States.



# Digital Transformation and the increasing need for data protection



**Mathieu MOREUX**

*Strategic Marketing, Critical Information Systems and Cybersecurity, Thales*

“The more we depend on the internet, the more we depend on its security”. This quotation of Neelie Kroes, then European Commissioner for Digital Agenda particularly illustrates the issues and constraints inherent to the so-called digital transformation, an ongoing phenomenon across all public and private organisations supported by social, mobile, analytics and cloud (SMAC) technologies. We can also surely add the Internet of Things, the usage of which is increasing in many businesses.

However, the digital transformation is not only about technology, but it is also about new business opportunities. According to the European Commission, European manufacturing could achieve 15% to 20% growth if digitalised<sup>1</sup>. Indeed, digital transformation helps extend the reach and the market of businesses and enterprises, to speed up the development of their products and services, to develop new business models and to improve the decision making process by capturing and analysing massive amounts of data. This data also brings social and collective value by improving knowledge and efficiency.

Data. Digital transformation is fundamentally data-driven and will be more and more so as the Internet of Things spreads. According to IDC, the total volume of data is doubling every two years and is expected to reach 44 trillion gigabytes by 2020! If digital transformation implies more user devices and applications, more heterogeneous computing models and systems, then data is the real wealth, to such an extent that it is now commonly known as the oil of the 21st century.

Therefore, it is easy to understand the increasing importance of data protection in borderless organisations to ensure its confidentiality, availability and integrity and in addition, privacy matters from a consumer and citizen point of view.

“Business imperatives have driven the convergence of the Internet of people, computers and things, transforming most enterprises into digital businesses and reshaping cybersecurity”<sup>2</sup>, says Christian Byrnes, managing Vice-President at Gartner. More specifically, digital transformation must come with the prevention and management of IT security risks and comply with a more rigorous regulatory environment, especially in Europe where the respect of data privacy is particularly surveyed.

The first risks come from the speed of this digital wave or what Christian Byrnes calls “the race to the edge”. Indeed, IT departments are struggling to provide end users and business units with the right productivity tools. According to a study conducted by the Harvard Business Review, 50% of the 750 respondents said that their organisation had missed out on new technology-enabled business opportunities because their IT department is too slow<sup>3</sup>. Unmanaged devices due to the BYOD trend, services and applications, are often in use without control from the IT department and consequently introduce security risks. According to another finding from Gartner,

around 30% of IT spending occurs outside the IT department today, putting data at risk.

Another risk for data is the borderless and open organisation which uses cloud computing services and collaborates with customers, partners or investors. Today, 80% of enterprises use cloud computing services and infrastructure and 54% of them are actually hosting sensitive data in the cloud. But this data, if not properly protected, is at risk: from data collection by the cloud provider to a cyber intrusion into its infrastructure. The data is also submitted to the local regulation where the datacenter is hosted.

The third risk comes from the core-to-edge continuum, meaning all the interconnections between the physical and the virtual assets that are exploding with the Internet of Things. Today, the Operational Technologies, including sensors and industrial control systems, and enterprise business management systems, such as ERP and HR, are interconnected. However, those physical assets only have rudimentary security - if there is any - introducing new vulnerabilities and paths for attackers. This considerably enlarges the attack perimeter, putting the data in the IT systems at risk.

Finally, organisations must comply with regulatory requirements for data privacy of employees and consumers and for confidentiality of corporate intellectual property and governmental secrets, requiring the use of data protection technologies. In Europe, the upcoming General Data Protection Regulation will force European companies to adopt preventive measures that lower the risks of data breaches.

Cyber-attacks and data breaches have high business impacts, which are first of all, financial. According to the Ponemon Institute, the average total cost of a data breach is \$3.79 million, an increase of 23% since 2013<sup>4</sup>. Besides, there are indirect but important consequences in terms of lost business due to the incident. Customers are more and more concerned with the security of their data and turn away from companies which are not able to protect it.

<sup>1</sup> European Commission, [Digital transformation of European industry and enterprises, Report and recommendations of the Strategic Policy Forum on Digital Entrepreneurship](#).

<sup>2</sup> Gartner, [Gartner says cybersecurity professionals are the new guardians of digital change](#), Press release, October 7th, 2015

<sup>3</sup> Harvard Business Review, [The leadership edge in digital transformation](#), 2014

<sup>4</sup> Ponemon Institute, [Global data breach cost report](#), 2015





# Towards European Digital Sovereignty



**Guillaume POUPARD**  
General Director of ANSSI

## From “information systems security” to “digital security”

In October 2015, Prime Minister Manuel Valls unveiled the French national digital security strategy, confirming France’s ambition to meet today and tomorrow’s security challenges in the digital world.

In a decade, as several public examples have shown, threats to digital security have grown in size and in impact, ranging from cyber-enabled espionage activities targeting administrations and businesses to the risk of sabotage, now proven real.

In a context where attackers’ capabilities and skills are continuously improving, France has continued to reinforce its technical and operational capabilities to respond to cyberthreats – ANSSI has grown from 140 agents in 2010 to nearly 500 today – and to strengthen its national organisation – cyber coordinators have been appointed within the ministry of Interior and the ministry of Foreign Affairs and International Development.

In 2013, France also decided to adapt its legal framework in order to reinforce the ability of operators of vital importance to prevent and respond to cyberthreats by establishing, among other provisions, mandatory security requirements to be implemented by these operators on their critical information systems, defined by ANSSI in close coordination with the operators themselves.

While cybersecurity of administrations and operators of vital importance remains a high

priority for France, recent years have also shown that cybersecurity no longer concerns only governments and large businesses but also businesses of all sizes in every sector of the economy as well as private citizens themselves. Today, our mission is also to contribute to the protection of citizens’ digital lives, privacy and personal data.

While the scope of actors preoccupied by their digital security has widen, so has our daily work which is no longer restricted to the development of technical and operational capacities but is also about defining efficient governance models, adopting adequate regulations, establishing dialogue with relevant public and private stakeholders, or engaging with other countries and multilateral organisations, starting with the European Union (EU) ; in other words, using all available levers to safeguard the digital security of the Nation as a whole.

## From national digital security to European digital sovereignty

Even if States are primarily responsible for their national digital security, it is France’s vision that many challenges can best be addressed through a common and coordinated effort at European level.

This is why France strongly welcomes the upcoming adoption of the EU Directive on Network and Information Systems Security (NIS), which will (1) establish a common minimum level of Member States’ cybersecurity capacities across Europe (2) reinforce the cybersecurity of operators providing services that are essential to the economy and the society (3) and – even more importantly – strengthen cooperation among EU Member States, both at political and operational levels, with the establishment of a network of Member States’ Computer Security Incident Response Teams (CSIRTs).

The European Network and Information Security Agency (ENISA) – which France has been and remains strongly supportive of – should as well be called upon to play a key role in supporting the implementation of the NIS Directive, thus contributing to the development of the European NIS community as it has been doing since it was set up in 2004.

Beyond the development of EU Member States’ capacities and cooperation, the EU must as well recognize that European

digital security is challenged on other fronts, requiring a collective ambition to guarantee Europe’s digital sovereignty. Three challenges in particular are ahead of us:

- First, while the EU cybersecurity strategy (February 2013) identifies the “*risk that Europe [could] become excessively dependent on [Information and Communication Technologies] produced elsewhere*”, the EU must actively support the development of sustainable European industries in the field of digital security and in the wider digital domain, and when relevant encourage their design and production in Europe. By doing so, Europe will contribute to maintaining an adequate level of diversity in the products and services used in Europe, in an effort to reinforce our security and trust in the digital society.
- Second, the EU must guarantee Member States’ ability to evaluate and approve the security of digital products and services, through the evaluation of the internal technologies of the products as well as companies’ internal processes and staff’s skills. Beyond each State’s own procurement methods, the EU should as well encourage security certificates’ mutual recognition among EU Member States according to rigorous standards, as a key driver for the development of trust and security in the European digital economy.
- Third, the EU must preserve its capacity to choose autonomously how data and related services should be protected in Europe, to the benefit of our administrations, businesses and citizens. The EU should, in particular, accept that certain legitimate restrictions to the “global flow of data” – and its possible limitation to the EU or to each Member State’s territories regarding data requiring a certain level of protection – will not impair the development of the digital economy and society but to the contrary ensure a level of trust, making it possible to flourish.

While some may see here an evil plan to set up new frontiers in the digital space, the principle of digital sovereignty responds to the democratic urge to (1) maintain our collective ability to decide on how data and related services can be best protected, including when necessary through regulation and (2) guarantee the conditions of this protection.

# Cybersecurity is one of the cornerstones of our fight against terrorism



**Gilles PARGNEAUX**

*Member of European Parliament,  
(S&D Group)*

2015 has been a terrible year for Europe. Terrorism has struck our continent and our values and has also put upside down our southern neighbourhood, moving thousands of refugees from the Middle East to the EU.

Today our fight against terrorism is questioned. In fact, fighting Daech requires a comprehensive approach and creation of new tools. As we understand further the rise of this terrorist group, we realise that communication, and especially communication on internet, turns out to be a strong channel of radicalisation, spreading of terror ideology and a very large platform for recruitment.

Let's also remember the attack of TV5 Monde by terrorists to point out that these attacks often aim our freedom of expression and our right to information directly.

This is the reason why the fight against cyberterrorism and, as a consequence, for cybersecurity must be at the top of our political agenda.

Things are moving in some Member States. In France for instance, 1 billion euros are to be dedicated and 1000 jobs in this area are to be created by 2019. Basically, the aim is to thwart Daech propaganda and their cyber-attacks.



However, more must be done at the European level. The S&D group has taken strong position in favour of an ambitious European policy of cybersecurity. In our common position we share the idea that as the cyber threats and attacks become more common, sophisticated, and potentially damaging, the EU and its Member States have to develop a cybersecurity policy to face this evolving challenge. We uphold therefore that developing the adequate policies to defend against cyber threats should become an integral part of the anti-terrorism strategy of the EU. We further uphold the importance for businesses and public authorities to dedicate sufficient resources to the protection of their infrastructure.

We urge the EU to become a platform for common cybersecurity efforts by the Member States. The EU has to assume a much more ambitious role of coordination going beyond the current establishment of minimum

standards concerning criminal offences. Facilitating law enforcement cooperation through Europol, including with the newly established European Cybercrime Centre, is welcome, but not sufficient. It is impossible to cope with the threat of cyber-attacks by means of merely 'national' cyber defence policies and strategies, since the cyberspace spans worldwide and attack's origin can even be overseas.

In addition, the cooperation must also be carried out with big internet companies. If we make it impossible to reach websites like "Tawid wa jihad" ou "minbar al'ielam aljhada", we cut off the main sources of recruitment of terrorist organisations. These websites are meant to spread a radicalised and armed conception of Islam that we can no longer tolerate.

As often now, this is through an enhanced European approach that such a policy will be effective.

# Cybersecurity and eCommerce: ensuring consumer and infrastructure trust



**Maurits BRUGGINK**

EMOTA Secretary General,  
Fédération européenne du e-commerce

## Trust in eCommerce

eCommerce is perhaps the most trust dependent sales channels. In most cases consumers are asked to send money to a seller they don't always know for a product they have never touched and which they are promised to receive anywhere from 24 or 48 hours to 30 days or longer.

The trust chain in eCommerce is long and complex and all players can be exposed to cyber-attacks or just hacks (from the internet service provider to the seller, to the payments provider to the postal operator). In recent years we have been witnesses of several important attacks on online sellers that resulted in the publication of customer personal details, including payment information<sup>1</sup>.

This triggered a constant effort by online sellers to implement the most stringent security measures and educate consumers on the signs of a secure website/transaction in order to reassure. Industry bodies such as national eCommerce associations and EMOTA have made high security requirements a priority in their self-regulatory initiatives such as eCommerce trustmarks and other webshop label mechanisms.

At the EU level numerous policy initiatives aimed to address the trust and security concerns in networks by adding new

requirements, broadening the scope to define online marketplaces and platforms as critical infrastructure for the economy and by introducing trustmarks for service providers.

These developments entail of course additional costs for online sellers (and consumers) while raising several questions regarding the (sometimes offline and slow) enforcement approaches to online crime and the constant need for evolution and coordination not only at the European level but globally. The key is to ensure that the measures are adequate for the risks while not creating unsustainable hurdles for the system.

## How is the market reacting?

In some of the EU Member States over 80%<sup>2</sup> of consumers are confident to shop online and the EU average is over 50%. Cross-border the consumer perception is that in 15% of cases they purchased a service or product from a foreign seller. The use of "perception" here is justified because the consumer might see a website in their language, accepting their currency and cards and the product might be delivered by the local postal operator, but the seller might actually be based in another EU country.

Recent reports<sup>3</sup> show that the consumers in the most mature markets feel rather confident in purchasing from non-European sellers, mostly from Asia, without having the possibility to check security measures or basic website information (language barriers, automated translations). 9,5 million UK consumers, 7,5 million German consumers or close to 6 million Spanish consumers bought from China in 2014, ranking China as the third country for shopping preferences.

## What holds the future?

In 2016 many expect mobile eCommerce to exceed 40% of total online eCommerce (in some countries exceeding 60% or 70%), introducing yet another element to the equation, the mobile device with a new set of security threats (Wifi, Bluetooth, app marketplaces, social networks, etc.).

For the first time mobile eCommerce could outweigh desktop purchases. This means customers are expected to increasingly store their personal information on mobile devices. Sellers are expected and even required<sup>4</sup> to implement selling apps or adaptive website formats which interact with the core personal data storage of the device (which more and more often tends to be the social network account)<sup>5</sup>.

Another important trend generated by the increase of mobile devices will be the use of peer reviews as a (possibly main) measure of security for consumers. Consumer reviews are gaining in importance rapidly and are likely to become even more significant and possibly automated<sup>6</sup>. This means the cost of the traditional "hard" security measures might become too high compared vouching by circles of acquaintances consumers seem to prefer.

The 2015 report of the European Central Bank on Card Fraud points to a relative increase in Card Not Present (CNP) fraud over the past few years<sup>7</sup> from 50% of total card fraud in 2009 to 66% in 2013. This is because online sales are constantly increasing and the level of sophistication in fraud constantly evolves. The total card fraud in Europe was estimated to 1,4Bn Euro in 2013. A relatively small number considering compared to the over 352bn Euro estimated eCommerce market<sup>8</sup>.

In August 2015 the European Banking Authority implemented the so called two factor authentication system for card payments and further measures are debated for card, mobile and micro payments. These will bring in new security measures for webshops and the tendency is to shift the responsibility for losses to the online seller rather than the payments provider.

Without a proper balance and risk/costs analysis the price for security and trust for the European online sellers based might prove too high and their competitiveness could be negatively affected.

4 <http://www.wsj.com/articles/google-gives-boost-to-mobile-friendly-sites-1429660022>

5 <http://www.smartinsights.com/social-media-marketing/social-media-platforms/social-sign-on-the-implications-for-e-commerce-sites/>

6 <https://www.google.com/trustedstores/>

7 [https://www.ecb.europa.eu/pub/pdf/other/4th\\_card\\_fraud\\_report.en.pdf](https://www.ecb.europa.eu/pub/pdf/other/4th_card_fraud_report.en.pdf)

8 EMOTA 2014 eCommerce Report <http://www.emota.eu/#!e-commerce-report-by-emota/cx0b>

1 <http://time.com/3647988/amazon-xbox-hack-password/>

2 2015 EU Commission Consumer Scoreboard [http://ec.europa.eu/consumers/consumer\\_evidence/consumer\\_scoreboards/index\\_en.htm](http://ec.europa.eu/consumers/consumer_evidence/consumer_scoreboards/index_en.htm)

3 [http://www.postnord.com/globalassets/global/english/document/publications/2015/en\\_e-commerce\\_in\\_europe\\_20150902.pdf](http://www.postnord.com/globalassets/global/english/document/publications/2015/en_e-commerce_in_europe_20150902.pdf)



# Substantive European criminal law regarding the fight against cybercrime<sup>1</sup>



**Isidoro BLANCO CORDERO**

Professor of Criminal Law  
University of Alicante  
Deputy Secretary General  
International Association of Penal Law

Our society is often described as an “information society”, in which is widely spread the use of Information and Communication Technology (ICT). The technological advances in ICT field during the last decades have had a significant impact on the legislative activities of the EU. The continuing evolution of ICT has created a new class of threats that societies must confront, especially crimes related to ICT and cyberspace, that affect individual and collective interests. There is not a legal definition of cybercrime, although it is usually used to cover a broad range of criminal conducts. For example, it includes “ordinary” criminal offenses, e.g., fraud, forgery, stalking or defamation that are committed by means of information and communication technology; offences against the confidentiality, integrity and availability of computer data and systems; content-related offences; and copyright-related offences.

Two factors have contributed to the intervention of the EU in the field of cybercrime: on one hand, the number of cyber-attacks against information systems has risen intensely around the world and in Europe; on the other hand, the transnational dimension of cybercrime, which usually transcends national

borders. Individual countries cannot effectively unilaterally create and enforce criminal laws to regulate cybercrime, cross-border regulation and cooperation are needed. In order to improve cooperation, the approximation of substantive criminal law of the Member States has been considered a priority. In this sense, Article 83(2) of the Lisbon Treaty included in 2009 “computer crime” among the offences of particular seriousness, with a cross-border dimension, so in the same category as similarly severe crimes, such as, terrorism, trafficking in human beings and sexual exploitation of women and children, illicit drug trafficking, illicit arms trafficking, money laundering, corruption, counterfeiting of means of payment and organized crime.

The EU adopted an important legal instrument addressing cybercrime in mid-2000, establishing minimum rules concerning the definition of criminal offences and sanctions in the area of attacks against information systems: Council Framework Decision 2005/222/JHA *on attacks against information systems*. This legal instrument, very much inspired by the Council of Europe Convention on Cybercrime of 2001, required that the Member States ensure that the illegal access to information systems (Article 2), the illegal interference in the systems (Article 3) and the illegal interference on the data (Article 4) shall be punished as criminal offenses. Nevertheless, the Framework Decision did not address content-related crimes (such as child pornography), other computer-related offences (such as fraud and forgery on line) and copyright violations (other EU legal instruments addressed this issues). A Directive was proposed in 2010 as a replacement to the Framework Decision 2005/222/JHA, due to the increasing of sophisticated and high-profile cyber-attacks in the EU. The Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013, *on attacks against information systems*, came into force on 3 September 2013, abrogating the Council Framework Decision 2005/222/JHA. The Directive includes most of the crimes contained in the Framework Decision, although new elements have been contemplated to address ‘new’ threats. Among these are the introduction of ‘illegal interception’ of information systems and the creation of tools used for committing crimes as criminal offences. It also strengthens cooperation between the judiciary and the police of the Member

States, introducing the obligation for Member States to make better use of the existing 24/7 network of contact points (including an obligation to answer within eight hours to urgent requests) and the obligation to collect basic statistical data on cybercrimes. Furthermore, the Directive introduces aggravating circumstances for crimes committed through organized crime, botnets, identity theft, causing serious damage, or against critical infrastructure. Finally, it raises considerably the level of criminal penalties.

The EU has also taken action against *content-related offences*, developing legal instruments to deal with child pornography and xenophobic material (this last one although the differences between the Member States on the criminalization of speech offences and the role and understanding of the freedom of expression guarantee). In this sense, the Directive on the *Exploitation of Children* (Directive 2011/92/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA) has distinct provisions concerning the production or display of child pornography and online grooming. The Framework Decision on *combating certain forms of Racism and Xenophobia* criminalizes public incitement to violence or hatred on the basis of race, colour, religion, descent or national or ethnic origin. Even in the context of *terrorism*, the Framework Decision 2008/919/JHA of 28 November 2008 deals with incitement to violence (“public provocation to commit a terrorist offence”), in which the Internet plays an important role.

Although the aim of the Commission to approximate criminal law sanctions concerning intentional infringements of *intellectual property rights* on a commercial scale, there was no consensus in the EU in favor of the criminalization of copyright violations.

To conclude, due to the cross-border nature of cybercrime, the EU has focused considerable attention in the context of the criminal law on the regulation of cybercrime, while other preventive measures are being left behind in the process. But cybercrime is essentially global in nature, so the effectiveness of the EU criminal regulation of this issue by a regional body can be questioned.

<sup>1</sup> This paper is included in the research Project funded by the Ministry of Economy and Competitiveness of the Spanish Government (“Adaptación del Derecho penal español al Derecho penal europeo” (DER2013-43883-P)).

# The Budapest Convention on Cybercrime: impact and outlook



**Alexander SEGER**

*Executive Secretary, Cybercrime Convention Committee, Council of Europe*

The Convention on Cybercrime offers an international criminal justice response to cybercrime and the problem of electronic evidence. It allows governments to reconcile their obligation to protect society and individuals against crime with human rights and rule of law standards. Some 15 years after its opening for signature in Budapest in 2001, it is more relevant than ever. The question is how new challenges can be addressed such as access to electronic evidence in the cloud.

## Cybercrime – a threat to core values

Cybercrime is not just about the functioning of computer systems but affects the fundamental values of our societies, that is, human rights, democracy and the rule of law. Every day, this is illustrated by millions of cases of theft of personal data, cyberattacks against media, civil society organisations and individuals, and denial of service attacks against public institutions and critical infrastructure. Sexual violence against children, xenophobia and racism and related radicalisation, or terrorist misuse of information technologies are proliferating.

In addition to cybercrime – that is, offences against and by means of computers – evidence in relation to any crime increasingly takes the form of electronic evidence on computer systems. And much of this electronic evidence

is now stored on, or moving between or fragmented over servers in the “cloud” and often in foreign, multiple or unknown jurisdictions.

Governments have the obligation to protect society and individuals and their rights against cybercrime and other offences involving electronic evidence. Securing computer data is essential in this respect. Without data, no evidence, no justice and thus no rule of law.

The search of a computer, the interception of a communication or other law enforcement powers interfere with the rights of individuals. They must, therefore, meet rule of law conditions, that is, be prescribed by law, pursue a legitimate aim, be necessary and proportionate, allow for effective remedies and be subject to guarantees against abuse.

Within this context, the Budapest Convention offers a criminal justice response.

## Scope and impact of the Budapest Convention

The treaty requires Parties to (a) establish a list offences against and by means of computers in their criminal law, (b) provide law enforcement with the powers to secure specified computer data in specific criminal investigations and in relation to any criminal offence, (c) limit such powers through rule of law safeguards and (d) engage in efficient international police-to-police and judicial cooperation.

To be clear, the Budapest Convention is about specific offences, specific investigations and specified data. Criminal justice rules and safeguards apply. It does not fall within the realm of national security measures.

All but two of the 47 Member States of the Council of Europe (the exceptions being the Russian Federation and San Marino) including all Members of the European Union are parties or have at least signed it. However, its geographical reach goes far beyond Europe. At present 66 States are either parties (the latest being Canada and Sri Lanka), signatories or have been invited to accede. At least double that number has used the Budapest Convention as a guideline for domestic legislation. Given that much of the IT infrastructure

and industry is based in the United States, the fact that the USA is a party since 2006 facilitates cooperation between European law enforcement authorities and the US Government as well as US-based service providers.

There is no doubt that the Budapest Convention has contributed to stronger and more consistent cybercrime legislation worldwide, more efficient cooperation between the parties, more investigations, prosecutions and adjudications of cybercrime and other offences involving electronic evidence, and more constructive public/private cooperation.

## More than a treaty

The Convention is backed up by:

- the Cybercrime Convention Committee (T-CY) comprising parties and observer States as well as European Commission, EUROPOL, EUROJUST, INTERPOL, the UN Office on Drugs and Crime and other relevant organisations. The Committee assesses implementation of the treaty in practice, adopts Guidance Notes and may also prepare additional Protocols to the Convention. This Committee is probably the most relevant inter-governmental body on cybercrime internationally;
- capacity building programmes to assist countries around the world in the strengthening of legislation, training of police, judges and prosecutors, or public/private and international cooperation. In April 2014, the Council of Europe set up a dedicated Cybercrime Programme Office (C-PROC) in Romania which is responsible for capacity building worldwide.

The Convention is thus more than the text of a treaty. It is this “dynamic triangle” of common standards, follow up and assessments, and capacity building which makes the difference.

The Budapest Convention furthermore relies on the political support by many governments and the European Union. The latter is reflected, for example, in the EU Cyber Security Strategy, the European Agenda for Security and joint capacity building programmes on cybercrime of the European Union and the Council of Europe.

### Need to address new challenges

In 2016, the Budapest Convention will turn fifteen. Given the difficulty of negotiating international agreements with respect to all things “cyber”, the greatest advantage of the Budapest Convention is that it is already in place and functioning.

Enhancing the quality of implementation and enlarging the quantity of members remains a realistic strategy.

Nevertheless, this may not be sufficient. Changes in technology and in the threat landscape may require additional solutions to protect the rule of law in cyberspace.

A major challenge is criminal justice access to data – and thus evidence – in the cloud.

The dilemma is that while law enforcement rules are tied by the principle of territoriality, data may be held temporarily or in parts by multiple layers of cloud service providers in various jurisdictions. It is often questionable how law enforcement authorities can legally access evidence in this context.

In the absence of clear international rules, government increasingly take unilateral action. The result is a jungle of approaches with risks for state-to-state relations and the rights of individuals.

The Cybercrime Convention Committee recently established a “Cloud Evidence Working Group” to identify solutions. Specific proposals should become available in the course of 2016.

There is no doubt that additional international rules are needed. It is also obvious that the challenge is complex and different interests may be difficult to reconcile.

Developing such rules within the framework of the Budapest Convention appears to be the most realistic option.







Cybersecurity and the fight against cybercrime are complex matters,  
which require vision, dialog and cooperation.

CyAN helps private and public organisation to identify trusted advisors  
from various disciplines and backgrounds

# to build a better future

find your trusted advisors or apply on [www.cyan.network](http://www.cyan.network)

# The individual and the digital world in a changing society



**Christian AGHROUM**

*CEO of SoCoA Sàrl, Former head of the French National Cyber Crime Investigation Unit (OCLCTIC)*

**D**ubbed the revolution of the twenty-first century, the rise of all things digital through the proliferation of internet-based technology is inexorable, the Arab Springs confirming the web's political role.

According to the ITU, internet penetration worldwide has increased almost seven-fold since the year 2000. In 2015, it was reported that there were 7 billion mobile phone subscriptions worldwide (compared to 738 million in 2000). Between 2000 and 2015, internet penetration thus increased seven-fold, going from 6.5 to 43 per cent of global population (2015 ITU Report).

This growth, hailed by all stakeholders as a spectacular achievement, is a source of progress and hope. It is a result of the globalization of exchanges, made possible by the development of transport over the twentieth century, followed by the development of communications via telephone, fax, and email.

The world of internet generates its own ecosystem. The whole range of human activity, from the creativity behind major projects, to the construction of factories and the supply chains of rare metals, benefits from this progress and from the prosperous market that is yet to be conquered. According to the ITU, 4 billion people living in developing countries are not yet online. Of the billion people living

in least developed countries, 851 million do not use internet. The resource is not yet evenly shared, making the market all the more attractive.

This economic progress brings with it unprecedented social and cultural opportunity with access to basic and further education, where the classroom has become a global lecture hall, providing access to culture in all its permutations through an increasingly complex virtual reality, and to healthcare through telesurgery and the live feed of medical data.

Everyone can find ways to break with isolation, improve their knowledge and develop skills. The range of possibilities has grown to give everyone a chance to express their talents and finance them through crowd funding (16 billion dollars raised worldwide in 2014) and alternative currencies. The news is live streamed through the social networks with varying degrees of professionalism. Freedom of expression, equal opportunities and solidarity can be shared equally through the endless possibilities provided by the internet.

In parallel, crime has taken over a whole new field of action where no patrols exist. The high-rate of cyber crime saturates the judicial systems of affected countries, but the multiplication of low-level prejudice generates an underestimated accumulated prejudice in the absence of sufficient awareness, reaching some 400 billion euros in 2014, according to McAfee.

Terrorist proselytism uses the cracks in the system and re-launches the debate on the boundary between individual freedom and necessary constraints.

The individual, whether acting as citizen, adviser, supplier or consumer, provides personal data with generosity and transparency. This is pillaged by a business sector that analyses their individual consumer habits and pushes targeted publicity at them. "BYOD", bring your own device, the ultimate individualization of the work tool is often used as a façade for externalizing companies' costs. The "Internet of Things", the paroxysm of fervent individualism, aside from the comfort that it provides, encourages consumption and enables systematic monitoring.

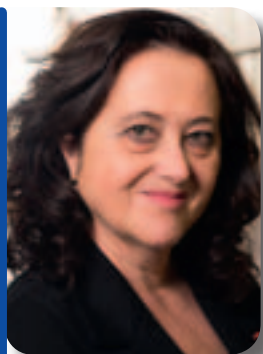
Individuals in our capitalist societies essentially fear being controlled by the rest of that society. They nevertheless provide a whole range of information that will eventually curtail their freedom: the animal believes itself to be wild but hands over its own leash. All this information and the permanent desire to be connected lead to the excesses that we now refer to as infobesity and cyberdependence.

The rapid radicalization of young people online raises questions regarding the way in which we should view the internet. On 19 October 2015, the European Parliament adopted a report on the prevention of radicalization and recruitment of European citizens by terrorist organizations, Title III of which is unequivocal.

The digital world glorifies individualism while opening a window onto the world. The relationship with society – or the relationship that is subject to the objective and controlled intervention of the regulating State – is in that respect necessary. Security, defence, economy and education maintain their sovereignty over the heart of the digital debate, moreover introducing a new dimension of interdependence. The absence of borders on the internet is taken as given, but this supra-citizenship is contradicted by the absence of any sense of supra-nationality. Of course, international organizations have individually tried to deal with the issues raised but, to date, there is no global or supra national secular legislation to regulate the relationship between individuals and the internet, or to bring balance to the power created by the web. Internet users consequently often feel very alone.

The digital world offers the individual a central role; but can they understand a version of History in which they act as both players and witnesses? HG Wells was looking for a World-State; is this what the World Wide Web is? "The history of Humanity is essentially a history of ideas" he said. Let's hope that the idea that man has of his position at the centre of the digital space will help him to find his way to a just and perfect World State.

# Cyberpower: stakes and challenges for Europe



**Dr. Prof. Solange GHERNAOUTI**

*Director, Swiss cybersecurity Advisory & research Group, University of Lausanne*

- the exploiting of vulnerabilities;
- the costs of cyberattacks borne by the victims;
- the difficulty in managing cyber risks;
- loss of confidence and a certain economic and emotional destabilisation.

The psychological impact of cyberattacks should not be underestimated. Terrorist groups have understood this well and cyberspace is not solely the domain of economic warfare. It is now also the means and the target of psychological warfare, war for influence. Warfare for and through information has become our reality.

The “enemy” knows us; we have willingly made ourselves available on the web. The data that the enemy needs is freely available or can be bought or hacked from the organisations that have acquired it, very often without our knowledge. We have perhaps on occasion agreed to the acquisition of personal data our consent is, however, rarely informed, and we are ignorant of its scope and duration and of the end use of the data provided. Our choices are often restricted, because the only alternative is to refuse to use the service, which is often impossible.

Whether they are carried out by patriotic hackers, terrorists, activists, hardened or amateur criminals, cyberattacks reflect our political, economic and social realities. The information technology tools and services offered are the fruit of our view of the world and of our culture. Cybersecurity technical measures will not be sufficient to counter the ingenuity and the absence of limits of some actors and the nuisance power that they wield through the Internet. Now it is more important to ask whether we are sufficiently robust and resilient than to ask whether we will be attacked. Yes, we are vulnerable, and yes, cyberattacks are targeting our systems.

Beyond the questions of responsibility and of who is going to pay for better security, we need to ask whether we are prepared to confront the changing paradigms that are resulting from information technologies, the digital economy and the reality of cyber risks.

All kinds of predators have made cyberspace into their playground on a global scale; while their victims are here, their commanders and armed wings are elsewhere, protected by the lack of effectiveness of legal, organisational and technical measures, protected by our incapacity to respond to increasing global risks and our incapacity to master a complex problem

linked to the growing interdependence of the economic, political, technological and societal spheres.

Let us design reliable and robust systems; let us reimagine cybersecurity in a holistic way; let us not yield to the facile to the detriment of the fundamentals of security. Let us avoid situations where the security remedy is worse than the illness; let us not make the criminals’ work easier by providing them with opportunities for malice in creating vulnerabilities that they know how to exploit.

All of us need to contribute to developing both a cybersecurity culture and measures that promote our economic development in a world that is complex, uncertain and full of conflicts. Creating cybersecurity requires understanding the world in which we live. We need to understand that the Internet marks a turning point in the history of humanity and that it is through this prism that we need to find the key to understanding the stakes in play in respect of controlling cyberspace and cybersecurity. We need to decrypt the place of the industrial and commercial logic of Internet players within the power politics of states, without forgetting to unpick the ambitions and operations of criminals in cyberspace, if we are to hope to address, efficiently, our needs to protect our digital heritage and our economy.

Cybersecurity should be at the service of a political vision of the durable development of a society and not only be a weapon to employ in economic or military warfare. Europe’s Cyberpower is related to its ability to answer problems created by the abusive or criminal misuses of digital technologies.

## Further reading

Solange Ghernaouti, “Cyberpower, crime, conflicts and security in cyberspace”, EPFL Press, 2013.

## Biography

Professor of the University of Lausanne, **Solange Ghernaouti** holds a Phd in Computer Science. She is Director of the Swiss Cybersecurity Advisory & Research Group, Associate Fellow of the Geneva Center for Security Policy, member of the Swiss Academy of Technical Sciences, and Chevalier de la Légion d’Honneur. She has been recognised by the Swiss press as one of the outstanding women in professional and academic circles.

**O**n the Internet, the marketing of war and terrorism sits alongside the marketing of legal and less legal businesses, and the black market in cybercriminality is doing well. The Internet has become a favoured environment for criminality and propaganda, for mass surveillance, business intelligence and for expression of all kinds of conflicts. Electronic attacks make it possible to make a country’s vital infrastructures malfunction, to implement criminal strategies, to cause losses of productivity or competitiveness, or even to seize power.

There are three types of organisations: those that have already been hacked; those have been hacked but don’t know it; and those that are going to be hacked. There are those that think that it only ever happens to others, those that take months to identify intrusions into their systems, and those that are immediately confronted by the reality of cyberattacks. This is most clearly the case when IT resources are hijacked and there is blackmail threatening to make sensitive stolen data public. In parallel, the vandalism of websites to insert material as for example related to the Islamic State, is an omnipresent threat and a directly identifiable attack. Although unlike in the case of the hijacking of resources the motivation of the terrorists is not linked directly to financial gain, these two types of attacks do have several points in common. These include:

- illicit intrusion into information systems and possibility that these have been infected by malware;



# No allies in cyberspace



**Olivier KEMPF**

*Director of La Vigie, Strategic Analysis letter  
and associate researcher at IRIS*

Snowden, Dilma Rousseff's mobile, Belgian Foreign Affairs, Bundestag, European Commission, Elysée: it is hardly a month without a «case» making the headlines. The scenario is unchanged: such state institutions have been spied for years - we do not know the authors - X is suspected (your choice: United States, Britain, Russia, and China). The only variation is due to the reaction of the victim: wrath, state affair, or embarrassed silence.

Most surprising, however, is that «allies» are spying on them. But it is logical as the conditions of cyberspace invalidate traditional alliances, for two main reasons. First, in a traditional alliance, whatever the political and strategic objectives, it is first necessary to add up the forces: troops and armaments are highly tangible, visible, countable, and assessable. However, the power of cyber is not counted in alignments of bytes or computers. It is based primarily on the creation of highly skilled teams, and that ultimately needs little equipment to work and progress. In other words, it is very difficult to add up intellectual capacity.

Especially, a second element is coming up: despite the appearances of publicity, opening and voyeurism of the Internet, facing the average user of cyberspace, it is a hidden, opaque, discreet space. It is very easy to act anonymously in cyberspace: not only to not be detected but even to impersonate others. Also, in all cases of recent years, we never had absolute technical proof of the alleged perpetrator's responsibility.

This is an unprecedented strategic novelty. In the world we were used to, we knew who the enemy was, so who was a friend. Admittedly, the criteria could be imperfect, alliances could vary in time, and unlikely compromises could

become possible. In cyberspace, you never actually know who is actually acting. The actor is always an unknown. Therefore, one cannot certainly describe it as an enemy. But if one cannot designate the enemy, then it is equally difficult to identify the friend, then the ally. This gap identification affects the whole mechanics of alliances.

This does not mean that there are no alliances in cyber. Simply, they are hidden, discrete, usually bilateral, confined to strictly defined and limited objectives. When two on a given project, we necessarily know who is who: oneself, the ally, the others. The mutual identification procedures can reveal «the others».

So, we can have a system of bilateral alliances. Me, country A, I ally myself with X on such a topic, with Y on another. But suddenly, my cooperation with X can affect Y with whom I have also another project.

Thus the embarrassment of many official reactions can be understood, as victims of a power with which they have also co-operation programs. Now, in the simplistic media world, this ambiguity is difficult to explain, even to justify. Thus, while one trumpets the myth of general alliances, one whispers that there are no allies in cyber, and restricted alliances are practiced in the greatest secrecy.



# Education, research, economic development: the broad-based approach of the Cyber Centre of Excellence



**Paul-André PINCEMIN**

*Project Manager of the Cyber Centre of Excellence (France)*

Initiated by the French Minister of Defence under the Cyber Defence Pact and with the support of the Bretagne region, the Cyber Centre of Excellence ("Pôle d'Excellence Cyber") develops its activities along 3 inter-related axes, with both national and international coverage: education, research and economic development.

Those 3 future-directed dimensions make up tomorrow's cybersecurity, in line with France's national priority regarding cyber defence and considering the stakes related to the escalation of threats: education addresses tomorrow's skills; research and innovation provide tomorrow's trusted products and services; economic development creates jobs in the future.

In order to develop its actions, the Cyber Centre of Excellence draws its strength, on the one hand, from an epicentre consisting of the cyber infrastructures of the Ministry of Defence in Bretagne (the French Defence Procurement Agency - DGA - Information Superiority, CALID Bretagne, École des transmissions, Saint-Cyr Coëtquidan Military Academy, the French Naval Academy, ENSTA Bretagne) and, on the other hand, from a rich region- and nationwide academic and industrial ecosystem.

Alongside the main regional agencies and the economic development and SMEs supporting associations, the Cyber Centre of Excellence

signed, in January 2015, a partnership with 13 major groups (Airbus D&S, Alcatel, Atos-Bull, Bertin, Cap Gemini Sogeti, DCI, DCNS, EDF, La Poste, Orange, Safran-Morpho, Sopra-Steria, Thales). In addition, a comprehensive research partnership agreement was signed in 2014 by the DGA, the Bretagne region, the CNRS, the INRIA as well as 9 universities or engineering schools. The first noteworthy effects were the doubling of cyber-related theses financed year in year out by the DGA, as well as the allocation of a budget of some 12 million euros over 6 years.

With, as of now, 50 partner organisations, both military and civilian, public and private, "cyber defence" in the strict sense of the term and "cyber security" in a more general sense, the Cyber Centre of Excellence is defined by a completely original operating mode with regard to its approach and organisation. Both are seamless, collaborative and network-based. "Clubs" (education, research and industrial development) and "working groups" (framework, platforms, communication), are led by a civilian-military tandem and systematically involve economic stakeholders in their work.

First example: a "compendium of the training offers from the partners of the Cyber Centre of Excellence" has been issued. It contains some one hundred pages, one for each initial training or continuing education programme, from A-Levels to PHD. The training offer, which is key to ensuring that the availability of skills is not a limiting factor for the development of the sector, has been compiled in close collaboration with the industrial players, in order to match their needs with the offer from the training providers. Under this joint initiative, over 20 trainings were created. Moreover, this input spawned new training tools, such as MOOC tailored to suit the expectations of the companies.

The "comprehensive overview of the research offer from the partners of the Cyber Centre of Excellence" was provided with the same spirit of dialogue. Early December 2015, a meeting gave researchers and laboratories the opportunity to present their work and lines of research to some 80 representatives of the economic actors and partners.

Similarly, existing or planned platforms (research, development, industrial testing, validation, education and training as well as showcase platforms) were mapped with the aim of efficiently focussing the efforts of the academic, state and industrial stakeholders as well as partners of the Cyber Centre of Excellence, through unifying programmes, optimised by the stakeholders and shared among the latter.

Another structuring approach: the DGA and the ANSSI (National Agency for Computer Security) presented their "technology roadmaps" for 2019 through several events targeting SMEs from the ecosystem. The visibility given in the process by the regulatory authorities is clearly crucial for the medium-term guidance, strategies and development of the companies in the sector.

Finally, another roadmap sets 6 main challenges for the economic development of the Cyber Centre of Excellence and its partners: developing interactions between the major ordering parties and the economic stakeholders; developing products and services that can address cybersecurity challenges with regard to the maturity of the technologies and to identifying shortages in the current offer of products and services; support services for company development, especially SMEs, and of course for exports; supporting measures for skill improvement of companies through cases of use, in order to create comprehensive offers; providing the tools and the necessary human and financial means; and of course a wide range of measures that will help ensure visibility, coverage, promotion and attractiveness of the Cyber Centre of Excellence and its partners, both at home and abroad.

This brief overview of some of the Cyber Centre of Excellence's main objectives, actions and outputs shows that what makes this major initiative of the Cyber Defence Pact unique and arouses such keen interest at national and European level, and even far beyond the confines of our continent, is the continuous and broad-based collaboration between the Cyber Centre of Excellence's 3 inter-related axes: education, research and economic development.



# Why must Europe invest in cybersecurity?



**Guillaume TISSIER**  
CEIS Managing Director

Cybersecurity is not merely a response to threats, it is first and foremost a true opportunity. It alone enables to generate the trust required for the digital transformation. Such an opportunity must be seized urgently, as Europe has valuable assets in the industry. This requires a clearly offensive approach, based on an accurate understanding of our common interests.

## A security issue

The first issue of cybersecurity is of course related to security: protecting our infrastructures and data in a context where threats and vulnerabilities are rocketing. The imperative objective: designing a collective response that involves public and private stakeholders, private individuals and organisations, and considering international cooperation as a priority requirement. While it is true that such cooperation is often hindered by national sovereignty concerns expressed in a clearly “coopetitive” environment, what binds us together at the European level is stronger than what divides us. Furthermore, in Western countries, 85% of computer assets are managed by private players. Paraphrasing Churchill’s “Never was so much owed by so many to so few”, referring to the RAF pilots during the Battle of Britain, never has collective security relied on such a diversity of individual behaviours.

## A societal issue

Cybersecurity should not merely be a technical response to a technical challenge, it should also contribute to the ethical and legal framework required to direct the multiple disruptions induced by the digital transformation. The issue is simple: now that software is eating the world, as stated by Mark Andreessen, the founder of Netscape, and technological barriers are disappearing, we must replace human beings at the heart of our concerns. And, for instance, enforce certain rights, such as the right to be forgotten and the right to informational self-determination. In this respect, Europe is a step ahead with the draft regulation on personal data processing, which will come into force very soon, and must thus secure its position.

## An economic issue

Digital uses will not develop unless there is an increase in trust, and thus in security and safety (or reliability). Cybersecurity must act as a facilitator, not as a retarder. Again, Europe has a major asset: despite the absence of global publishers and web platforms, it possesses a high-quality technological and industrial cybersecurity ecosystem, which also positively impacts other sectors. The future single digital market and the establishment of interoperability standards for secure transactions, with the eIDAS regulation entering into force in July 2016, should strengthen the industry.

But on one condition only: that we are able to finance the development and nurture the “business” of our cybersecurity gems within a more comprehensive digital ecosystem.

## A sovereignty issue

Lastly, cybersecurity is a sovereignty issue, at both national and European level. At a time of globalisation and progressive dilution of State sovereignty, the very concept of sovereignty may seem an anachronism. On the contrary: it is being revived by the sovereignty of individuals over their personal data, of companies over their immaterial assets, of States over their critical infrastructures, and so on. Indeed, sovereignty, defined as a State’s right to exercise its political authority over a geographical area or a community of individuals, must be reinvented, modernised and shared. But it is the only vehicle likely to effectively influence our future, largely connected to digital affairs. Furthermore, it consecrates the primacy of the political sphere and supports the democratic operation of societies.

With the European digital agenda unveiled in May 2015 only, we can say that it has taken a while for Europe to wake up. But now, we have a “vision”, and tools are being developed. 2016 will undoubtedly be a key year.

*CEIS is a strategic consulting firm. It organizes the International Forum on Cybersecurity (<http://www.forum-fic.com>).*





# Advanced Persistent Cybersecurity Threats (APT): Preparing for the New EU Cybersecurity Directive



**Adam PALMER**

*Director, International Government Affairs  
at FireEye (Based in Munich)*

## Introduction

2016 presents an unprecedented challenge for government and private industry in Europe—cybersecurity threats are now a persistent risk. The new EU cybersecurity policies now require compliance with “state of the art” security and international best practices. The EU has implemented the most detailed and comprehensive cybersecurity regulations in EU history. For the first time, organizations which fail to implement adequate security will face significant penalties of up to 10,000,000 Euros or two percent of

annual worldwide revenue if a security failure results in a privacy breach pursuant to the new EU Privacy regulation.

## Understanding Advanced Persistent Threats (APT)

Advanced Persistent Threats (APT) can be extremely advanced attacks that penetrate IT network defences with a clear goal – harm the organization and steal information. These attacks are designed to stay unnoticed inside an organization with some attackers averaging from 205 days and up to eight years inside networks<sup>1</sup>. An example of a recent APT targeting Europe was the French speaking international TV channel TV5 Monde that was attacked in April 2015 by the Russian group APT28. The station’s 12 channels were shut down for 18 hours in 200 markets and its General Manager Yves Bigot announced the channel would require 10M€ to strengthen cybersecurity.

APTs don’t always use advanced techniques and still rely heavily on social engineering to expose business secrets or access systems. One APT group currently targets medical and pharmaceutical executives with sophisticated spear-phishing emails. This group is believed to steal confidential information and use it

for stock trading<sup>2</sup>. This APT group knows its audience. Their e-mails seem to be written by native English speakers familiar with both investment terminology and the inner workings of public companies. The group’s spear-phishing emails frequently focus on shareholder and public disclosure concerns.

These examples demonstrate the sophistication of APT attacks and the likelihood that they will be successful in gaining access to a network. Rather than focusing solely on prevention, it then becomes necessary to shift focus to fast detection and response.

## Attacks using unknown vulnerabilities

The seriousness of zero day attacks was highlighted recently in a 2014 study by KPMG of 20 large European multinational companies finding that 93 percent of the organizations were breached, with 79 percent of the attackers stealing confidential data and 50 percent of these attacks were successful by exploiting previously unknown, zero day exploit vulnerabilities. This makes the detection and elimination of zero day vulnerabilities a primary concern for security managers trying to close the door on APT.

1 Mandiant M-Trends 2015 <https://www2.fireeye.com/rs/fireeye/images/rpt-m-trends-2015.pdf>

2 Hacking the Street? Fin4 likely playing the market <https://www2.fireeye.com/fin4.html>

## ADAPTIVE DEFENCE

### DETECT

SIGNATURE-LESS AND MULTI FLOW APPROACH THAT LEVERAGES THREAT INTELLIGENCE

### PREVENT

MULTI-VECTOR INLINE KNOWN AND UNKNOWN THREAT PREVENTION

### RESPOND

REMEDATION SUPPORT AND THREAT INTELLIGENCE TO RECOVER AND IMPROVE RISK POSTURE

### ANALYZE

CONTAINMENT, FORENSICS INVESTIGATION AND KILL CHAIN RECONSTRUCTION



### How “good” do you need to be?

Compliance, while important, is not adequate security. Most APT would successfully evade a system that has minimum “compliance” based security.

An organization must know the type of data that might be valuable to an attacker, the type of confidential information the company maintains, where it is stored and what is most sensitive. Although the security team might conduct much of this work, the Chief Legal Officer can also provide valuable insights on this information and probably already tracks the most important information for other legal purposes. Having senior “C-level” support is critical for a successful security programme.

Security is a process not a goal. It requires a governance framework to serve as the support mechanism to guide the program and resolve critical decisions. Having cross-functional support greatly helps in justifying policy change, budget, and the company culture required to be successful. This must be a “living” strategy that is adapted to maintain business awareness and effective response when a breach occurs.

Without a solid internal structure, you will have trouble building any success. Smart risk management policy and internal coordination are the foundation for preparing to defeat advanced threats and manage an effective security program.

### What are the policy trends related to APT Protection in Europe?

As noted above, the new General Data Protection Regulation (GDPR) will increase the level of security required for organizations

and the new Network Information Security (NIS) Directive will also require a wide range of companies to adopt “state of the art security” controls. As APT threats are becoming more pervasive, APT detection protocols are likely to be recognized as part of “state of the art security” requirements. Failure to adopt adequate APT protections may expose an organization to significant fines of millions of euros per violation.

Individual member states are also increasing security requirements and penalties for non-compliance with security standards. Germany recently adopted a new IT security law that also requires the adoption of “state of the art security.” The German law mandates *state of the art* organizational and technical security measures to avoid interferences of availability, integrity, authenticity and confidentiality of information technology systems. The law includes mandatory data breach reporting and regular audit requirements. Similarly, in France, the Military Plan Act of 2013 introduced a framework for state of the art incident detection and response to be implemented by critical infrastructure companies. These laws are examples of similar laws that are expected in 2016 to mirror the requirements of the new EU cybersecurity policies. Taken together, these policies suggest a strong trend at both the EU level and national member state level to implement heightened strong cybersecurity standards that include APT and incident response requirements.

### Incident Response

A holistic cybersecurity programme should include incident response preparedness. This should include both the capability to recover

quickly from cyber attack and a measurement of the time necessary to resume critical operations after an attack. Response should include the following considerations:

- Incident Management
- Service Continuity Management
- External Dependency Management

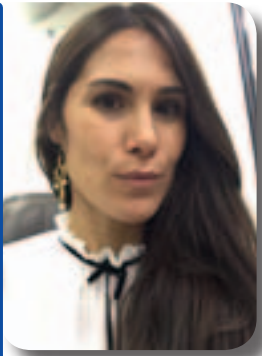
The Incident Response Strategy must establish an incident response coordinator and precisely define protocols to efficiently and effectively inform key stakeholders. These protocols should govern privacy disclosure requirements and assignment of work streams for investigation, remediation, communication, and execution of the response plan. It is critical to determine and plan response prior to the pressure and confusion of an actual breach.

### The Road to Success

Adopting a “*detect and respond*” strategy (anticipating a breach) vs. a prevention posture (that is likely to fail) is a strong and smart risk management model. Technical solutions are only part of the answer. Promoting the right internal risk management structure is key. By being actively evaluating security preparedness, you significantly lower the risk that an APT threat will cause significant harm. A “state of the art” security programme promotes compliance with EU regulation and, most importantly, improves the security of business operations.



# Cybercrime and the risks for the economy and enterprises at the European Union and Italian levels



**Fancesca BOSCO**

*Associate Project Officer, UNICRI*

## Research Highlights and Overview of Guidelines for SMEs

The EU Institutions political agreement on the first EU wide cybersecurity Directive (Network and Information Security Directive<sup>1</sup>) brings the issue of cybersecurity to the forefront of European policymaking. Major aims of the directive include making sure that essential services are adequately protected to fend off cyber threats, and the new rules legally require companies in certain sectors to report security breaches, an action that businesses have often been reluctant to undertake in light of the negative ramifications for corporate reputation and investor confidence. While many experts might argue that these measures are not enough for ensuring cybersecurity across the EU, the directive underlines the need for more attention to be paid to cyber-related issues, particularly as they affect the private sector and customer data.

In relation to this topic, UNICRI has produced a comprehensive study concerning the economic risks associated with cybercrime at the EU and Italian levels, particularly as they affect small and medium enterprises (SMEs).

This research was subsequently followed up by the production of a set of guidelines for SMEs to be implemented in order to minimize cyber-related risk and protect vital company data. As SMEs represent an enormous sector of the European economy, these entities should be considered as a core element in any cybersecurity strategy enacted at the EU level. The following information serves to highlight the initial findings of UNICRI's 2014 research study, looking at Europe and particularly the Italian context, followed by an introduction to the guidelines produced with the aim of safeguarding SMEs from cyber attack.

## Initial Research Findings

Cybercrime is a multidimensional and complex phenomenon. It does not only target particular types of companies such as those in the Information Technology sector or those that produce highly specialized goods, but rather all types of companies.

Cybercrime is one of the most serious threats to the global economy, steadily growing over the past decade. The losses deriving from it are currently estimated to be between US\$375 and US\$575 billion per year<sup>2</sup>. However, Interpol has estimated that in Europe alone, the cost of cybercrime has apparently reached €750 billion annually<sup>3</sup>.

Cybercrime's impact on national economies is also huge. In addition to large companies, small and medium sized enterprises (SMEs) are increasingly affected by cybercrime attacks. The research study aims to provide a framework to assess the impact of cybercrime on the economy, and to evaluate the vulnerabilities of SMEs to cyber-attacks. SMEs represent a pillar of the European economic and social structure, as well as 99.9% of Italian

enterprises. The research focuses on the impact of cybercrime at the international, national (Italian) and local level. Targeted interviews and case study analysis have been conducted to provide an overview of the tools currently used by criminals, the most common reasons that lead to these criminal acts, and the major risks and vulnerabilities for businesses. Interviews with institutional players and companies have helped to clarify key problems and suggest a need for a coherent strategy for SMEs to defend themselves against cybercrime.

The main findings of our initial research report are as follows:

- All interviewees highlighted the need to invest in building capabilities through training programs as well as the need to remove cultural barriers that hamper awareness of the risks of cybercrime. One important concern which emerged is that vulnerabilities associated with people's lack of capabilities and knowledge are considered more dangerous than those related to technical issues. The human factor is, in fact, crucial in this type of crime, as cyber criminals often exploit human weaknesses for their own purposes.
- Crimes targeting specific organizations or individuals, such as spear phishing, have significantly increased in recent years.
- In order to implement countermeasures and concerted policies, it has been underlined that not only should IT managers be informed of the risks of cybercrime, but also administrators, business owners, and boards of directors.
- The research highlights a lack of information sharing and cooperation among companies and stresses the need to create networks between companies of the same sector or size in order to increase dialogue and the sharing of best practices.
- The investigative and judicial scenarios, as portrayed by the interviews, have shown that countering cybercrime is very difficult due to its transnational character. International cooperation between different actors therefore plays a crucial role in the investigation and prosecution of such crimes. In addition to strong legislative and law enforcement actions, the

<sup>2</sup> Net Losses: Estimating the Global Cost of Cybercrime Economic impact of cybercrime II Center for Strategic and International Studies June 2014, available <<http://www.mcafee.com/ca/resources/reports/rp-economic-impactcybercrime2.pdf>> (retrieved 10-12-2015).

<sup>3</sup> Opening Remarks by INTERPOL President Khoo Boon Hui at the 41st European Regional Conference (Tel Aviv, Israel, 8 May 2012), available at: <<http://www.interpol.int/content/download/14086/99246/version/1/file/41ERC-Khoo-Opening-Speech.pdf>> (retrieved 10-12-2015).

<sup>1</sup> European Commission - Press release- Commission welcomes agreement to make EU online environment more secure [http://europa.eu/rapid/press-release\\_IP-15-6270\\_en.htm](http://europa.eu/rapid/press-release_IP-15-6270_en.htm) (retrieved 10-12-2015).



fight against cybercrime requires appropriate tools and cooperation, as well as a particularly higher level of knowledge and awareness.

Cyber security is an added value, and the reliability of SMEs in this respect has to be considered as a crucial element for investors and clients.

Organizational culture is also an issue that needs to be addressed, and many preventative mechanisms can be implemented with limited costs. In addition to an internal security policy, it is necessary to encourage the sharing of information at multiple levels. Sharing best practices and information about threats internally and with supply chain companies, trade associations, and law enforcement agencies can help in preventing attacks and establishing initial countermeasures. At the operational level, during or after an attack: information sharing with other actors, such as law enforcement and financial institutions, can increase the resilience of production systems and mitigate economic and social damages.

The cross-border nature of cybercrime requires action at both the international and national level. In this regard, the European Union, in 2013, adopted its cyber strategy and invited Member States to do likewise. In 2014, Italy also published its National Strategic Framework for Cyberspace Security (*Quadro strategico nazionale per la sicurezza dello spazio cibernetico*).

To counter cybercrime, training and information sharing are crucial. The information collected in the research study allowed UNICRI to design and create a strategy based on the development of two complementary projects.

The first project aims to increase companies' knowledge and information exchange networks through the development of seminars, workshops and training courses tailored to non-technical decision makers, i.e. board of directors and business owners, and to IT staff.

The second project involves the organization of periodic roundtables among different actors, such as SME representatives, law enforcement, business associations, academic institutions, and advocacy and legal experts. The purpose of this project is not only to improve the sharing of information on emerging risks in cyberspace, but also to facilitate the creation of a leading cross-sectoral community in the fight against cybercrime.

The implementation of these two projects will allow for the creation of networks of experts to promote a culture of security, with the advantage of never becoming obsolete (a typical problem for classical best practices), and instead adapt themselves according to the evolution of the cybercrime phenomenon.

## Development of Guidelines for IT Security in SMEs

IT security for SMEs represents one of the most pressing challenges for both the economies of Italy and Europe. It is therefore necessary that a series of proactive measures be put into place with the aim of increasing awareness in this field.

SMEs make up 99.8% of European and 99.9% of Italian enterprises, respectively. In the European Union (EU), 86.8 million people are employed within this sector making SMEs the backbone of the Italian and European economies. While at the same time, they also represent a major point of weakness in terms of security.

Cyber crime provides a huge source of income for criminal organizations and is a key priority for the European Agenda on Security, alongside terrorism and organized crime<sup>4</sup>. The latest World Economic Forum (WEF) report<sup>5</sup> on global risks confirms that cyber attacks remain among the biggest threats to global security - both in terms of impact and likelihood of occurrence.

SMEs are a very attractive target for cyber criminals; nevertheless, decision makers working in these enterprises still often underestimate the threat posed by cybercrime. No matter the nature of an SME's business, every company is seen as a lucrative target. Various types of information, be it intellectual property, commercial data and contact lists, personal data, account credentials, and more can be sold on the black market to individuals intent on committing fraud, spreading malware and facilitating other crimes.

At the corporate level, damage is not only caused via a simple, one-off or indiscriminate attack. Instead, many attacks have long-term consequences. We are now witnessing an increase in targeted attacks that have the aim of appropriating sensitive data, deleting data altogether, or stealing copyrighted material.

Cyber crime is of a stronger nature and more widespread than one might imagine. In fact, most cyber attacks are still not being detected and/or reported. Losses due to cyber

crime for an individual company can reach up to several million euros.

Due to large-scale cyber attacks in 2014, approximately one billion records<sup>6</sup> were compromised – affecting, on average, one in every three Internet users. Many of these records were totally unencrypted, and thus easy to exploit.

Additionally, ransomware is not showing any signs of decreasing in activity. The number of this type of attack more than doubled in 2014 – rising from an estimated 4.1 million attacks in 2013, to 8.8 million in 2014. From a psychological point of view, ransomware represents a very profitable form of attack because if a victim has not performed regular backups of their data, they are normally willing to pay the ransom in order to be allowed to retrieve it.

Alcatel-Lucent's Motive Security Labs<sup>7</sup> has estimated that more than 16 million mobile devices around the world have been infected with malware for the purpose of carrying out industrial and personnel espionage, to steal information and to attack companies, private, banks and government. In 2014 alone, mobile device infections increased by 25% (an increase of 5% compared to 2013).

Phishing is still one of the most common methods of attack. Despite possibly being the most well-known cyber-attack technique, the percentage of users who click on phishing e-mails is still very high, even today. The 80,000 security incidents analyzed in the Verizon Data Breach Investigation Report<sup>8</sup> have led to economic damage and data loss of more than \$400 million for the companies involved. The Verizon study therefore shows how highly profitable it is for a cyber criminal to use phishing techniques. Based on the data analyzed, for every ten phishing e-mails sent out, there was a more than 90% chance that at least one user would fall victim to an attack.

Considering the growing trend regarding this type of threat, it is more important than ever to develop efficient preventative security systems.

4 Communication from the EU Commission to the European Parliament, The Council, The European Economic and Social Committee and the Committee of the Regions, The European Agenda on Security, European Commission, Strasbourg, 28-04-2015, in <[http://ec.europa.eu/dgs/home-affairs/e-library/documents/basic-documents/docs/eu\\_agenda\\_on\\_security\\_en.pdf](http://ec.europa.eu/dgs/home-affairs/e-library/documents/basic-documents/docs/eu_agenda_on_security_en.pdf)> (retrieved 09-06-2015)

5 The Global Risks 2015 10th Edition, World Economic Forum, in <[http://www3.weforum.org/docs/WEF\\_Global\\_Risks\\_2015\\_Report15.pdf](http://www3.weforum.org/docs/WEF_Global_Risks_2015_Report15.pdf)> (retrieved 06-05-2015)

6 Why SMEs are an attractive target for cyber criminals and what they can do about it, by Neil Ford, 02-03-2015, in <<http://www.itgovernance.co.uk/blog/why-smes-are-an-attractive-target-for-cyber-criminals-and-what-they-can-do-about-it/>> (retrieved 21-05-2015)

7 Motive Security Labs malware report – H2 2014, Alcatel-Lucent's Motive Security Labs, in <<https://resources.alcatel-lucent.com/asset/184652>> (retrieved 23-03-2015)

8 2015 Data Breach Investigations Report, Verizon, in <<http://www.verizonenterprise.com/DBIR/2015/>> (retrieved 25-05-2015)

# Cybersecurity for a resilient European infrastructure



**Hans TEN BERGE**

*Secretary General of Eurelectric*

Expanding and improving Europe's energy networks is vital for Europe's transition towards a low-carbon economy. Europe needs smarter distribution grids to integrate increasing decentralised generation and electric vehicles into the network and to encourage consumers to manage their energy demand. To establish an interactive infrastructure with new energy management capabilities, smart grids must integrate high-speed and two-way communication technologies into power equipment. However, growing dependency on Information and Communication Technology (ICT) might give rise to smart grid vulnerability. Potential network intrusion and customer information leakage could lead to brownouts or blackouts and the destruction of infrastructure, thus compromising reliable and secure power system operation. As a result, cyber security issues in smart grids are of critical importance in today's energy world.

## Why is cybersecurity of critical importance?

A large-scale cyber-attack could generate substantial damage and give rise to very high costs for the electricity system. It could trigger power outages and disruption in communications, affecting critical sectors of society. Although incidents do occur in EU distribution grids, Europe does not know yet what a major cybersecurity attack could look like.

With smart meters being rolled out, the European Union might face vast security and reliability challenges. The transition from analogue to digital controls creates new potential pathways into utility systems. Currently, most power failures relate to technical issues, severe weather conditions and human error. However, merging communication technologies into power generation, distribution, load balancing and meter reading can potentially set off an increase in cyberattacks or other hacking episodes.

Since the level of cybersecurity vigilance varies across utilities, common protocols for interconnected grids are difficult to find. Moreover, energy regulators are not usually empowered with cybersecurity mandates, which currently make it harder to *strengthen cybersecurity regulations*.

## Practices and solutions for the EU

The cyber-risk management capabilities of companies and national regulatory authorities (NRAs) are at a nascent or developing stage.

They also differ between Member States. As a result, several European projects have been investigating new cybersecurity methods for electricity grids. For example, SEGRID (Security for Smart Electricity GRIDS) a collaborative project, funded by the EU under the FP7 programme (2014-2017), is researching into the enhancement of vulnerability assessment techniques. Its objective is to improve the protection of smart grids against cyber-attacks by applying a risk management analysis approach to a number of smart grid use cases. This will define security requirements and determine gaps in current security technologies, standards and regulations. The project will also develop a realistic testing environment (Security Integration Test Environment) to assess and verify new security methods.

PREEMPTIVE is another project receiving funding from the EU's FP7 programme (2014-2017) that is worth mentioning. It provides solutions for enhancing procedures to prevent cyber-attacks targeting utility companies. This piece of research aims to implement detection tools based on a dual approach comprising



direct detection (i.e. network traffic and system calls) and process misbehaviour detection (i.e. automatic industrial or business processes). The existing methodological security and prevention frameworks will be enhanced to harmonise risk and vulnerability assessment methods, standard policies and procedures. Prevention and detection tools will be designed.

### Building blocks to strengthen cybersecurity

Although there is a will to create a more reliable and secure power system operation, it remains difficult to protect the electricity grid from all cyber-attacks because of their unpredictable nature. Therefore, industry and regulators need to consider how to prioritise actions and minimise the risk of cyber-attacks and their impact.

Currently, the EU's main piece of legislation in this area is the EU Cybersecurity Strategy, adopted in 2013. The European Commission also made a proposal for a directive on

Network and Information Security (NIS), which aims to make the EU's online environment the most secure in the world. Moreover, the Commission is putting together an Expert Group dealing with Energy Strategy on Cybersecurity to provide advice in terms of policy and regulatory directions at European level.

However, there is still a great need for better harmonisation across the EU to develop and deploy good practices if faced with a major power supply disruption. Both the EU and individual NRAs should raise awareness and enable cooperation on this matter. Considering that cybersecurity is not only technical, but also operational and organisational, a governance model is required in all Member States. This model should empower energy regulators with a cybersecurity mandate and include smart grids in cybersecurity strategies. Moreover, organisations need to evaluate their own vulnerabilities to correct them.

Cybersecurity needs a long-term vision that includes standards, best practices, protocols to respond to cyber-attacks, and funding to

reinforce the grid. Industry and regulators should work together and come up with baseline security measures. The EU considers that national risk assessment could help evaluate and improve national cybersecurity strategies.

Usually, transmission system operators (TSOs) do not consider smart grid security as their problem, because security issues are usually found in distribution grids. However, cooperation between TSOs and DSOs will facilitate the secure exchange of data across grids and ensure data privacy.

As the electricity sector is increasingly dependent on information and telecommunication technologies, cybersecurity remains an important area to consider for the future of smart grids. In order to keep Europe's infrastructure resilient, industry and regulators have to speed up the process and provide Europe with a clear and consistent view on how to tackle cyber risks and increase the resilience of the energy system.





# Cyber-security and hybrid codes



**Zbigniew SAGAN**

Chief Technology Officer, Advanced Track & Trace, member of ITSA Board of Directors\*

## Digital and physical exchanges, mobilities and interconnections: What Security systems?

In a global context, more and more dependent on digital technologies and confronted with the appearance of new risks, all sorts of links are formed between real entities (persons, objects, companies, institutions, etc.) and virtual entities (their representation or virtual information).

With the multiplication of exchanges and communications, the relationships of these entities, the relationships with individuals and their environment, are constantly changing. The traceability of these entities, whether physical or virtual, the traceability of their actions and of their interactions is at the core of a sequence of needs which evolve and appear in order to provide more security, under the best conditions, for the circulation and the life of these entities: identification, authentication, legitimacy, attributes, integrity, eligibility, inspection, localisation, etc... The association and the combination of some or all of these elements, allows more and more precise traceability solutions to be established such as described in numerous works and standards.

No field of human activity escapes these needs today.

If traceability, in all its forms, becomes more important and is more visible every day, it must also often comply with the notions of individual freedom and the protection of privacy.

The reinforced needs of security, the rapid development of "connected objects", social networks, Big Data and Cloud Computing put traceability even more at the heart of exchanges and needs, allowing heterogeneous entities to be linked with their acts, actions and interactions. It is essential therefore, to master systems, to set-up their links and their purposes.

## From identification to authentication

Persons, documents, objects, are the central participants of events in a sequence of traceability and it can be seen that the mechanisms and the techniques for recognizing the legitimacy of a participant, whether it be human or other, often share similar or even identical logic.

The principal goal to achieve is to provide the means necessary in order to ensure the security and the reliability of technical tools which allow citizens to be better protected (public safety and health) by detecting behaviours and illicit practices in different areas such as:

- counterfeiting and misappropriation of products
- management of critical components (aeronautics, software, ...)
- document fraud.

The link between technological means used and applied in the so-called "brand protection" area (counterfeit protection, unit traceability of products, secured traceability, etc.) and cyber-security solutions, is obvious. Numerous stakeholders have been successfully implementing hybrid solutions, for several years now.

In all cases, this is to ensure the **uniqueness of values** and to combine them with **unique identifiers encryption**, in order to mask and secure information content. Incidentally, the ex nihilo creation of values by fraudsters who might want to replace them by being presented as legitimate is not possible anymore.

With the ever increasing volume of products and objects having a unique identification number and information relating to their origin, their conditions of production, storage, transport, distribution, communication, ..., it becomes strategic to be able to perform verifications efficiently and at each step of the process, to have the certainty of being in the presence of the right entity, the right place, the right time. Indeed, it must be recognised, not only if the unique identification number is legitimate but also, if it is not a clone which could threaten a system. **This certainty is obtained by the legitimacy authentication of the object being checked.**

If there are numerous physical authentication solutions, the authentication system must be recognized and to have the means of inspection. It is also the reliability of the identification function at the source which is at stake, and if one considers, the diversity of multiple specific identification systems, often private, the task becomes complex with the need for interoperability.

## Standardisation and interoperability progresses

The interoperability question was identified by anti-counterfeit experts several years ago and the standard ISO 16678 "Guidelines for interoperable object identification and related authentication systems to deter counterfeiting and illicit trade" saw the light of day in 2014. This standard was developed in the framework of TC 247 "Fraud countermeasures and controls" before the re-grouping, decided upon by ISO, of all the projects related to security, within a single technical committee, the TC 292 "Security and Resilience" as of January 2015.

The question of interoperability is treated in the ongoing project ISO WD 20229 "Security and resilience - Guideline for establishing interoperability among object identification systems to deter counterfeiting and illicit trade" which follows the logic of the standard ISO 16678.

In France, this work is monitored in the framework of the national mirror committee TC 292 (AFNOR), by the CNPPC working group: Commission de Normalisation Performance des outils de Protection contre la Contrefaçon (Commission on the Performance

Standardisation of Tools for Protecting against Counterfeiting).

The desire of industrialists to develop an interoperability scheme in the area of counterfeiting, did not start today. Several initiatives have followed one another via experimental platforms but their deployment has not been widespread.

### Bearer codes: from digital to physically protected

The reflections are oriented to the possibility of getting over, or at least limiting the necessity of access to a specific Internet service of the "hub" type.

One of the approaches, already used, passes by the systematic use of a bearer code for an electronic signature. Whatever the technology of the information bearer (2D code, RFID, NFC, etc.), this approach allows information to be secured which bears a chosen code, -data container-, and thus to direct the monitoring entity to the reliable information source: directly to the eligible service or to a third-party, certified Internet service.

In this context, the management of electronic signatures must be treated classically, identically to its use in the context of the digital economy where it must respond to certain criteria, such as eIDAS in Europe, in a logic of "identity - authentication - trusted service".

### Identification and authentication: all in the code, nothing in the Cloud

Advanced Track & Trace follows this approach entirely by applying the principle of "security by design". Its technologies are based on physical codes mainly but also **physical / digital hybrids**. These authentication and traceability codes integrate, as of their conception, the notion of intrinsic security, not based upon a secret other than the encrypting key related to the management of rights.

These functions are valid whether for a simple unique identification number or for a private logo which acts as a 2D public code, pointing to a specific service, as for a data container code bearing biometric data.

Hence, were elaborated the data container codes SealCrypt® and BioSeal® whose design has been guided by the preoccupation, amongst other things, for the respect for privacy. The ability of these codes is to include simultaneously, in the same symbol, private data and the electronic signature, rendering its use possible locally, without remote access to a server or other service and in the absence of any communications network.

In addition, the data contained in these codes can be divided into categories and classified into, for example, public or private data, the public data being kept in clear and the private data being encrypted.

If security constraints require it, the interpretation of private data is assured by the reader terminal which could be a simple smartphone: it is a **"match on secure device"** by analogy with "match on card".

The establishment of an eco-system without databases, nominative or sensitive with respect to privacy protection, becomes simple to produce, under particularly competitive economic conditions.

### From digital to physical: securing data whatever the state

The procedures for processing information and data never cease to evolve with successive passages from digital (creation) to physical (printing) and coming back to digital (scan, pdf, etc.). This process of **document hybridisation** and of the mixing of the physical and digital worlds, requires specific and appropriate solutions which will allow documents to keep their **original value** and be able to **guarantee their integrity**.

This is what the new container codes, developed by Advanced Track & Trace, allow, which support the migration of documents from physical to digital form with their content and their integrity intact and are able to supply irrefutable proof of their integrity, locally, without need for access to a database.

Advanced Track & Trace follows this logic and makes available for cyber-security stakeholders solutions like SealCrypt®, SealStamp® and BioSeal®. They allow the integrity check of a document edited, scanned and transformed into pdf format (for example), then re-printed to be certified and this, without accessing the original information system. SealCrypt® can allow an electronic signature to be affixed to a physical or digital document, making it hybrid and bringing guarantees of integrity and security to the electronic signature. The SealCrypt® code can be read and authenticated using a standard smartphone, PC or other, without need for a connection.

The proof of integrity accompanies the documents and the data, throughout their life-cycle whatever the state through which they pass.

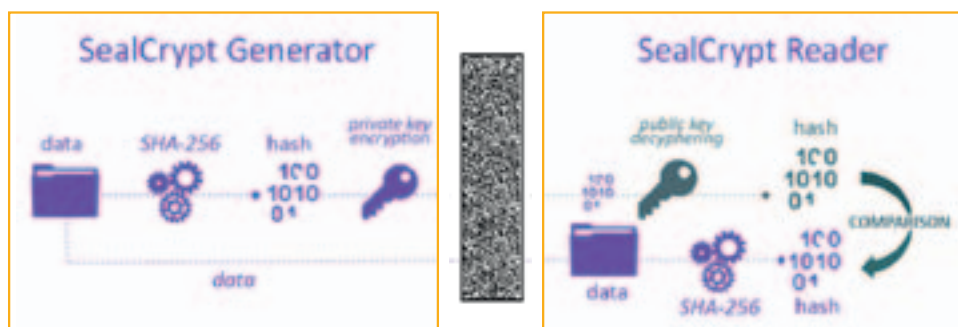
In conclusion, securing products, objects, communicating objects, documents and providing a reliable link with eligible persons and entities, all in heterogeneous and sometimes hostile environments, under economically acceptable conditions, is a sizeable challenge.

The appearance of new technologies and solutions allows appropriate, reliable, economic answers to be provided, coming from new ways of thinking, and which comply with the requirements of modern governments concerning the respect for privacy and individual liberties.

\*\*\*

*Advanced Track & Trace is a driven leader in digital security applied to unitary traceability, documents security, banknotes and Brands protection against illicit trades.*

*Zbigniew Sagan: Zbigniew studied Biomedical Engineering at Warsaw Technical University. He joined Advanced Track & Trace team in 2003 as Chief Technology Officer. He holds several patents in the field of document security, ID and brand protection. He is an active member of ISO Technical Committee 292 "Security and Resilience" and a member of Board of Directors of International Tax Stamp Association (ITSA).*



Data securing process applying asymmetrical encryption scheme

# Threat Intelligence



**Filip CHYTRÝ**

Security Researcher, Avast Software s.r.o.

## Today's threat landscape is moving towards mobile

Throughout the last few years, online threats have been a prominent and growing issue. Within mobile cyberspace, the issue is unfortunately not much different. As most of us can't imagine going a day without using our smartphones, it's crucial that we come to understand what our devices are capable of and the consequences that could happen as a result of their mishandling.

Let's take a step back to several years ago – at that time, my device was operated by Android 1.6, Donut. It was a smooth, easy-to-use

platform with almost no apparent threat landscape present. Now, in 2016, I can confidently say that we can expect rapid growth of mobile-oriented threats within the next coming years. In the past two years we have already seen an exponential growth in terms of threats and these threats are becoming much more involved and aggressive.

## Which specific threats are we talking about?

The threats to be on the lookout for can be divided into multiple categories – some of them are already widespread, while others can be expected to make a bigger name for themselves in 2016.

## Adware / Malvertising

Malvertising is a common method used by hackers in order to sneak unwanted content onto a device. Often, hackers will build adware based on popular apps and games whose names are familiar to most users. This makes it easier for the fake, malicious versions of these apps to be located and downloaded by users. Hackers use social engineering techniques in order to frighten victims into falling for malvertising scams. As we move forward in 2016, the techniques used by hackers will only become smarter and more complex.

## SMS Payments

Simply put, SMS payments are an easy way to obtain money from a user. Malicious SMS messages can go hand in hand with

malvertisement, serving as a result of adware that has been downloaded onto a device. The messages are automatically sent to a paid number, which in turn costs the user a small amount of money to send. While SMS payments have begun to become less of a popular method in European countries, they still exist as a problem within Eastern Asia.

## Fake Apps

What could be easier than downloading a popular, legitimate app and packing it with unwanted content? This is what many cybercriminals do in order to distribute fake, compromised apps within app stores. Many users continue to be scammed by this method, since the illegitimate versions of apps are usually free of charge to download and use. As fake apps most often occur within untrusted, third-party apps stores, the chance of encountering them can be significantly reduced by only downloading apps from trusted sources.

## Advanced Persistent Threats

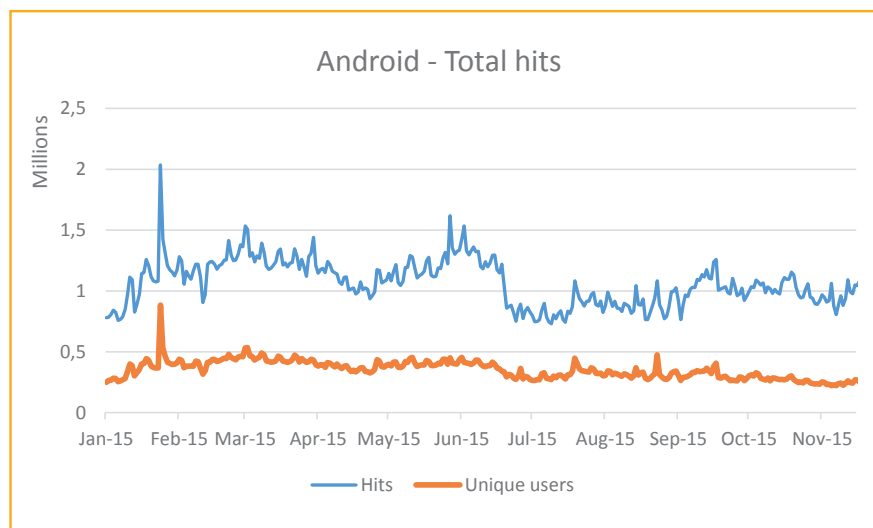
If you are being targeted by an Advanced Persistent Threat (APT) you most likely don't know someone is on your network spying on you. This year, we have seen remote access tools, such as OmniRAT, in the wild targeting mobile devices. Remote access tools (RAT) are typically spread via social engineering and are a tool to execute advanced persistent threats. If you fall for social engineering and download a RAT an attacker can gain full access and control of your mobile device.

## Ransomware

Ransomware attempts to lock users' data and demands a specified amount of money to unlock it. We saw many cases of ransomware take place in 2014 and 2015, but now, the stakes are even higher. Attackers are now starting to use asynchronous encryption, a tool that makes it next to impossible for your data to be restored once it's been locked by ransomware.

## Vulnerabilities

Today, many software companies have bug bounty programs available where people can report vulnerabilities in exchange for a monetary reward. Unfortunately, cybercriminals on the black market pay more for the same vulnerabilities, which they then sell



Number of users protected daily by Avast Mobile Security during 2015.



## Obfuscation

The screenshot shows the 'Блокировщик рекламы' (Ad Blocker) application in its 'Device administrator' mode. The interface is in Russian. At the top, the status bar shows various icons and the time 11:34. Below the title bar, the app icon is a red octagon with 'ABP' in white. The text 'Администратор активен. Это позволяет Блокировщик рекламы выполнять следующие операции.' (Administrator active. This allows Ad Blocker to perform the following operations.) is displayed. A list of five operations is shown: 'Erase all data', 'Change the screen-unlock password', 'Set password rules', 'Monitor screen-unlock attempts', and 'Lock the screen'. At the bottom are 'Cancel' and 'Deactivate' buttons.

```
String str2 = onCreate("學習口.");
Class[] arrayOfClass2 = new Class[3];
arrayOfClass2[0] = B.class;
arrayOfClass2[1] = Integer.TYPE;
arrayOfClass2[2] = Integer.TYPE;
Method localMethod2 = localClass4.getMethod(str2, arrayOfClass2);
localMethod2.invoke(localObject5, arrayOfObject5);
```



```
localClass4.getMethod(onCreate("창륙櫛",
new Class[0]).invoke(localObject5, new Object[0]);
Method localMethod3 = localClass2.getMethod(
onCreate("창뤼櫛, 憩捡·霰뵐·塋·彬-"),
new Class[0]);
Class localClass5 = Class.forName(
onCreate("8뤼櫛, 愔挠·露뤼·塹·146廁更櫛"));
String str3 = onCreate("뵐櫛·憊捶");
```

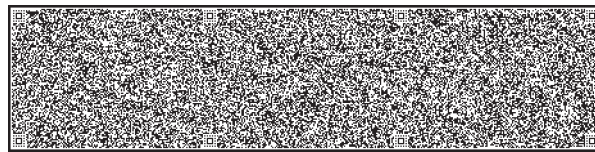
Overall, people still underestimate risks. I'm trying to be really careful personally, but even my credit card information has been stolen twice in 2015. Credit cards are a good example of a risk people underestimate, because your device does not have to be compromised - instead your cards can be compromised when you swipe or enter your details into a third party device.

when you use a mobile payment method and that third party can be just about anyone.

Looking back on the mobile threats that dominated 2015, we can bet that vulnerabilities, malvertisement, data collecting and spying will continue to develop and spread, as more and more people use smartphones. At Avast, we currently have about 2 million mobile samples in our database that are potentially unwanted or malicious. If we also take web threats into consideration, we are looking at millions of threats targeting mobile users.









## SEALCRYPT® IS

- ☐ A BIOMETRIC PASSPORT
- ☐ A VISA
- ☐ AN ELECTRONIC SIGNATURE
- ☐ CONFIDENTIAL DATA
- ☐ AN ACCESS BADGE
- ☐ A DOCUMENT OF PROBATIVE VALUE
- ☐ AN ID PHOTO

☒ ALL OF THEM. AND MUCH MORE...



Scan to download the SealCrypt® app  &   
or visit <https://sealcrypt.att-fr.com>  
Visa: sealcrypt  
Password: sealcrypt

  
Advanced  
Track&Trace  
[www.att-fr.com](http://www.att-fr.com)





8<sup>TH</sup>

# INTERNATIONAL CYBERSECURITY FORUM



DATA SECURITY & PRIVACY

**25<sup>TH</sup> & 26<sup>TH</sup>**  
OF JANUARY 2016

**LILLE**  
GRAND PALAIS

THE EUROPEAN CYBERSECURITY EVENT

➔ [www.forum-fic.com](http://www.forum-fic.com)



An event co-financed by the Nord-Pas de Calais-Picardie regional Council and organized by

