icom
institute for competitiveness

SECURITY IN THE DIGITAL AGE

Europe at a crossroads

June 19, 7:40 – 9:30
Rond-Point Schuman 6 - 1040 Brussels

1. Cybersecurity in the digital age: a global overview

The digital revolution has transformed everyday life. Thanks to the Internet, connecting people across the world has never been as easy as it is today. Moreover, the IoT (Internet of Things) has led to the spread of a mass of smart devices for people and businesses. However, this relatively new way of living (always accessible, everywhere and at every moment) has brought to light many new problems in terms of security, specifically **cybersecurity**.

The digital environment is vast and, consequently, it is ideal ground for cyberattacks that can be either indiscriminate or targeted, aimed at large and small organizations in both the public and private sectors. Therefore, Internet usage and its connected devices offer new opportunities for people and companies but, at the same time, create new risks. **The range of potential attacks and attackers is wide and becoming more so by the day**. The new technologies, mobiles, smart devices connected to the Internet of Things and many artificial intelligence applications expose every organization to attackers, increasing the risks of, for example, shut downs or subversion of industrial control systems.

According to Kaspersky Lab[1], more than 40% of all industrial control system (ICS) computers were attacked by malicious software at least once during the first half of 2018. This is a continuation of a trend with the figure increasing from 36.61% in the first half of 2017 to 37.75% in the second half. Countries with the highest number of ICS computers attacks in 2018 were Vietnam (75.1%), Algeria (71.6%) and Morocco (64.8%). Countries with the lowest number of industrial attacks were Denmark (14%), followed by Ireland (14.4) and Switzerland (15.9%). The largest number of threats come from the Internet, which over the years has become the main source of infection for ICS with 27% of threats being received from the world wide web and removable storage media ranking second with 8.4%. Mail clients occupy third place in terms of volume representing 3.8% of threats.

[1] https://www.kaspersky.com/about/press-releases/2018_ics-computers-attacked-in-h1

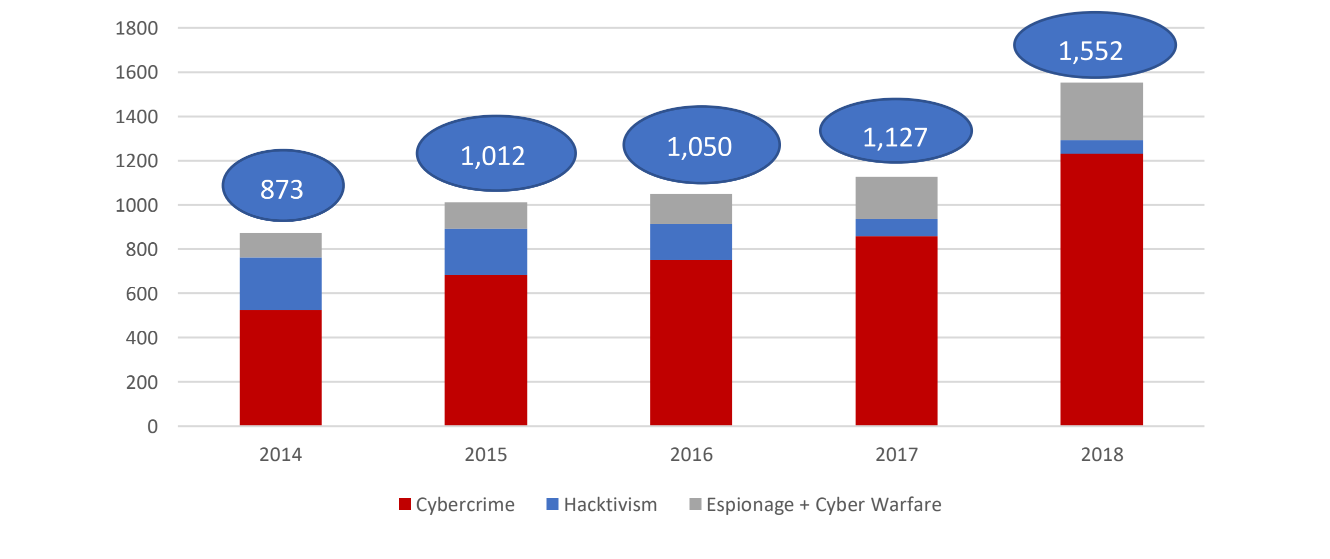
Threat can even be dangerous to human lives if you imagine an attacker being able to turn off life support systems in hospitals or take control of connected cars on the road.

Indeed, **the World Economic Forum has included cyber-attacks among the biggest problems of 2019**, along with natural disasters, biodiversity loss and ecosystem collapse and the spread of infectious diseases[2].

According to a 2019 Clusit study, out of a sample 8,417 serious attacks[3] occurring worldwide between 2014 and 2018, 1,552 were recorded during the last year (+77.8% compared to 2014 and +37.7% compared to 2017).

In recent years, Cybercrime, Cyber Espionage and Information Warfare have recorded a strong increase. Cybercrime rose by 43.8% in 2018 compared to 2017, while Cyber Espionage and Information Warfare increased by 35.6% in 2018 compared to 2017.

Fig. 1: Cyberattacks occurring worldwide (2014-2018)



Source: Clusit, 2019

Cybercrime is the first cause of serious cyber-attacks at a global level. It has gradually been increasing, from 60% of analyzed cases in 2014 to 79% in 2018, showing an unequivocal trend. Hacktivist attacks have progressively decreased, from 37% in 2014 to 4% in 2018. Instead, Cyber Espionage and Information Warfare grew from 13% of total attacks in 2014 to 17% in 2018.

[2] World Economic Forum, "The Global Risks Report", 2019.

[3] Serious attacks are thoseattacks with a significant impact on victims in terms of economic losses, damage to reputation, the dissemination of sensitive personal and non-personal data, or that herald particularly worrying scenarios.

In 2018, the most affected categories were Multiple Targets (304 attacks, +36.9% compared to 2017), government (252 attacks, +40.8%) and health (159 attacks, +98.8%).

Currently, **malware is the most widespread technique of attack, accounting for a total of over 800 million attacks in the third trimester of 2018**. According to McAfee[4], mining crypto-currency via malware is one of the big activities of 2018. Total "coin miner" malware has grown more than 4,000% in the past year.

Therefore, in an increasingly digitalized world, cybersecurity has jumped to the top of the company risk agenda after a number of high-profile data breaches, ransom demands, Distributed Denial of Service (DDoS) attacks and others over the last years.

Organizations are spending more on cybersecurity, allocating more resources to improving their defenses, and working harder to embed security-by-design. **However**, according to the EY Global Information Security Survey 2018 - 19[5], **more than three-quarters (87%) of organizations do not yet have a sufficient budget to provide the levels of cybersecurity and resilience they require**. Protection is patchy, and relatively few organizations are prioritizing advanced capabilities with, too often, cybersecurity remaining siloed or isolated. 39% of organizations said that less than 2% of their total IT headcount work solely in cybersecurity, however, cybersecurity budgets are on the rise.

Customer information, financial information and strategic plans make up the top three most valuable information areas that organizations would like to protect. For 17% of the organizations interviewed, the biggest fear is loss of customer information, followed by loss of financial information (12%) and strategic plan violations (12%). Moreover, 22% of organizations see phishing as the biggest threat, followed by malware and cyber-attacks.

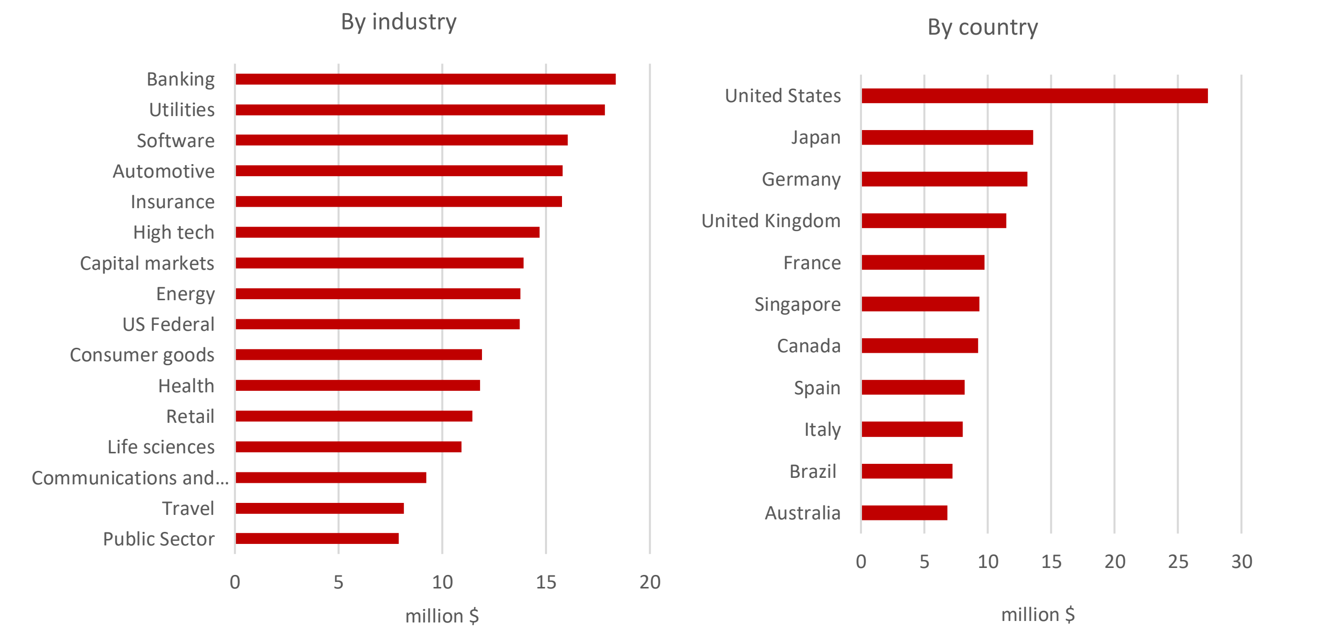
Attackers frequently use very simple tools and tactics, such as emails, heavily impacting and damaging companies. Nowadays, emails are not only a communication tool but also one of the prime sources of threat for users and organizations. This threat can range from unwanted emails in the form of spam to more dangerous types, such as the propagation of ransomware or targeted spear-phishing campaigns. According to the Internet Security Threat Report 2019 published by Symantec, **some industry sectors receive more spam than others. The spam rate varied from 52.6% for Wholesale Trade to 58.3% for the mining sector**. A growing proportion of spam now contains malware. **In 2018, agriculture, forestry and fishing, together with the retail trade, were the sectors most hit by email containing malware**. In these sectors, the percentage of email classified as malware made up 11% of total emails. **As regards phishing, the trend dropped from 1 in 2,995 emails in 2017, to 1 in 3,207 in 2018 with** agriculture being the most affected sector in 2018.

[4] McAfee Labs Threats Report, december 2018

[5] The 21st edition of EY Global Information Security Survey captures the responses of over 1,400 C-suite leaders and information security and IT executives/managers, representing many of the world's largest and most recognized global organizations.

Cyberattacks are having a significant and growing financial impact on businesses worldwide. According to the Cost of Cyber Crime Study published by Accenture and the Ponemon Institute (2019)[6], **the global average cost of cybercrime**, which includes the total of costs incurred to detect, recover, investigate and manage the response to cyberattacks, **climbed to $13 million in 2018, with an increase of 12% from $11.7 million reported in 2017, and 72% in the last five years**. **Malware is the most expensive attack type for organizations**, followed by Web-based attacks, however, **the cost of ransomware and malicious insider attack types has grown the fastest over the last year (**21% and 15%, respectively). Analyses show that **banking and utilities industries continue to incurred the highest costs for cybercrime** with an increase of 11% and 18%, respectively. The energy sector remained fairly level over the year with a small increase of 4%, and the Health industry experienced a slight drop in cybercrime costs of 8%.

Fig. 2: Cost of cybercrime (2018)



Source: Accenture and Ponemon Institute, 2019

In comparing different countries, **US companies incurred the highest total average cost at $ 27.4 million, increasing by 29% in 2018 compared to 2017**. **But the highest increase of 31% was experienced**

[6] The Cost of Cyber Crime Study surveyed 2,647 security and IT professionals in 355 companies in 11 countries: Australia, Brazil, Canada, France, Germany, Italy, Japan, Singapore, Spain, the United Kingdom and the United States.

by organizations in the United Kingdom growing to $ 11.5 million, **closely followed by Japan** increasing by 30 % in 2018, reaching $13.6 million on average for each organization.

Finally, the main and most costly impacts on organizations that suffered a cyberattacks are loss of information, business disruption, loss of revenue and damage to equipment.

2. Experience and awareness of cybersecurity in Europe

Europeans feel increasingly exposed to the risk of falling victim to cybercrime. According to a 2017 Eurostat survey[7], 87% of respondents saw cybercrime as an important challenge to EU security. Over half (56%) saw it as a very important problem, while just under a third (31%) viewed it as a fairly important problem. There are significant country-level differences in the number of respondents who think that cybercrime is a very important security issue, ranging from 76% in Cyprus, and 75% in the Netherlands to only 39% in Sweden and 26% in Estonia.

Moreover, Europeans are most worried about the potential misuse of their personal data and the security of online payments. In 2017, 45% of people interviewed by Eurostat were concerned about the possibility that their data might be misused by a third party, while 42% were concerned about the security of online payments.

For this reason, a lot of Internet users in European countries use identification procedures for online services. **The use of the tools to ensure secure access to online services and to carry out electronic transactions in a safer way is growing rapidly**.

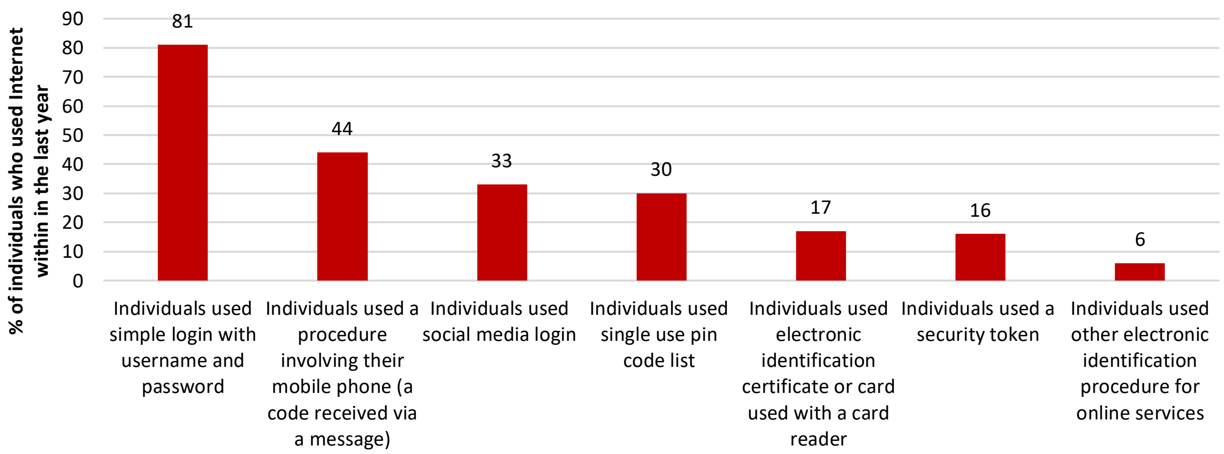
According to Eurostat data, in 2018, **over 80% of Internet users in the European Union logged in to online services using their username and password. Other popular identification procedures were by receiving a code by text message on their mobile phone, which was used by 44% of the EU's Internet users. Using social media logins to access other online services (33%) and logging in with a single-use PIN code list (30%) were also popular**.

For example, text messages with a code are a powerful tool in verifying the identity of individuals. In the EU, most Internet users in the Czech Republic (75%), the Netherlands (72%), the United Kingdom (61%) and Denmark (60%) logged in to online services using a procedure involving their mobile phone where a code is received through a text message. In contrast, the lowest percentage for this type of login procedure were recorded in Croatia (4%), Bulgaria and Romania (both 5%)[8].

[7] Special Eurobarometer 464°, Europeans' attitudes towards cyber security, 2017.

[8] https://ec.europa.eu/eurostat/web/products-eurostat-news/-/EDN-20190205-1

Fig. 3: Identification procedures used for online services in the EU (2018)



Source: Eurostat, 2019

Use of smartphones to access the Internet has significantly increased and consequently many users are experiencing some security issues, such as viruses affecting devices, abuse of personal information, financial losses, and, therefore, they try to restrict access to their data. **According to Eurostat data, in 2018, 58% of individuals at least once were restricted or refused access to personal data, when using or installing an app on their smartphone, while 28% were never restricted or refused access to personal data. Moreover, 7% of individuals did not know it was possible to restrict or refuse access to personal data, when using or installing an app on their smartphone**.

Europe plays an increasingly active role in addressing the multiple cyber threats and holds a leading position in the global context.

According to the Global Cybersecurity Index 2018 (a composite index combining 25 indicators into one benchmark to monitor and compare the level of the cybersecurity commitment of Member States for the five pillars[9] of the Global Cybersecurity Agenda) published by the International Telecommunication Union (ITU), the UN Agency that deals with TLC and network policies, **European countries have improved their rankings due to initiatives such as the EU certification framework for ICT security products, the implementation of the General Data Protection Regulation (GDPR) and the Directive on security of network and information systems (NIS Directive)**. In 2018, six European countries with the

[9] The five pillars are: 1. Legal Measures based on the existence of legal institutions and frameworks dealing with cybersecurity and cybercrime; 2. Technical Measures based on the existence of technical institutions and frameworks dealing with cybersecurity; 3. Organizational Measures based on the existence of policy coordination institutions and strategies for cybersecurity development at the national level; 4. Capacity-building Measures based on the existence of research and development, education and training programs, certified professionals and public sector agencies fostering capacity building; 5. Cooperation Measures based on the existence of partnerships, cooperative frameworks and information sharing networks.

highest level of commitment to cybersecurity were in the top ten most committed countries globally. The **United Kingdom dominated the global ranking, followed by France in third position, Lithuania (4th), Estonia (5th), Spain (7th) and Norway (9th)**.

The United Kingdom ranked first with the highest score in the legal pillar and the organizational pillar, with a number of legal instruments to fight cybercrime, including the Computer Misuse Act.

France, in third place globally, for the second time running was ranked in second place in Europe, scoring 100 per cent in the legal and organizational pillars. France is collaborating with institutional partners (ministries, national authorities, private sector and non-profit organizations) and, under the European Cybersecurity Month, is using various means to raise cybersecurity awareness.

Lithuania has the highest score in both the legal pillar and the organizational pillar. The Lithuanian Law on Cybersecurity lays down provisions enabling competent authorities to take action against public electronic communication infrastructures participating in malicious online activity (e.g. participating in a botnet). The State Data Protection Inspectorate can publish cybersecurity incidents involving personal data breaches.

Finally, **Europe stands out as having the highest number of Member States with national strategies** with, out of a total of 45 European states, as many as 39 having a National Cybersecurity Strategy.

3. The European Regulatory Framework

Cybersecurity is one of the most important priorities for European institutions.

Since the adoption of the EU Cybersecurity Strategy in 2013, the European Commission has planned actions to better protect Europeans online. The **EU Cybersecurity Strategy** launched in 2013, established 5 priorities that involved increasing cyber resilience, drastically reducing cybercrime, developing an EU cyber defense policy and the industrial and technological resources for cybersecurity and establishing a coherent international cyberspace policy for the EU.

In 2015, the European Agenda on Security was launched by the European Commission, setting 3 priorities - terrorism, organized crime and cybercrime – and proposing, for the latter, the following actions:

- placing renewed emphasis on the implementation of existing policies on cybersecurity, attacks against information systems, and fighting child sexual exploitation;
- reviewing and possibly extending legislation on fighting fraud and counterfeiting of non-cash means of payments to take account of newer forms of financial tool crime and counterfeiting;
- reviewing obstacles to criminal investigations on cybercrime, notably on issues of competent jurisdiction and rules on access to evidence and information;
- enhancing cyber capacity-building actions under external assistance tools.

The **Regulation on Electronic Identification Authentication and Signature (EIDAS)** entered into force on September 17, 2014 and became applicable from July 2016, in the field of electronic identification and trust services for electronic transactions in the Internal market, and representing another important measure to increase security in the European Union. This regulation provides for a predictable legal framework for individuals, companies (in particular, SMEs) and public administrations to safely access services and carry out transactions online and across borders.

It defines a predictable regulatory environment to enable secure and seamless electronic interactions between businesses, citizens and public authorities. More specifically, it ensures that people and businesses can use their own national electronic identification schemes (eIDs) to access public services in other EU countries where eIDs are available and creates a European internal market for eTS - namely electronic signatures, electronic seals, time stamps, electronic delivery services and website authentication - by ensuring that they will work across borders with the same legal status as traditional paper-based processes. Only by providing certainty on the legal validity of all these services, will businesses and citizens begin using the digital interactions as their natural way of interaction.

On July 6, 2016, **Directive 2016/1148** (c.d. **NIS Directive**) was adopted, setting measures for a common high-level security for networks and information systems in the Union. This is of extreme importance as, for the first time, the cybersecurity challenge has been tackled, revolutionizing cybersecurity in Europe. The Directive recognizes that network and information system security is essential for economic and social activities and, above all, for the functioning of the Internal market.

To this end, the Directive: 1) has prescribed Member States to adopt a national strategy on network security and information systems; and 2) has established a cooperation group to support and facilitate strategic cooperation and information exchanges among Member States and to build trust among them - this group is made up of representatives from the Member States, the Commission and ENISA and carries out its activities on the basis of two-year work programs; 3) creates a network of cybersecurity action teams in the event of an accident to contribute to the development of trust among Member States and to promote rapid and effective operational cooperation; 4) establishes security and notification obligations for operators of essential services and for digital service providers; 5) obliges Member States to identify competent national authorities, single contact points and CSIRTs with tasks related to network security and information systems.

The national strategy must regulate several aspects, in particular, the objectives and priorities, a governance framework to achieve the objectives and priorities set, the identification of preparedness, response and recovery measures, including collaboration between the public sector and the private sector, the indication of training, awareness and education programs, research and development plans and a risk assessment plan (Article 7).

The NIS Directive also requires states to designate one or more competent authorities to control the application of the directive at national level. A single point of contact should be designated by each

Member State, to ensure international cooperation and connection with other states through the cooperation mechanisms identified in the directive itself.

Finally, each state must designate one or more Computer Security Incident Response Teams (CSIRTs) responsible for monitoring incidents at the national level, providing timely alerts and announcements with the aim of disseminating information on risks and incidents.

Cooperation among institutions of the individual Member States is a crucial part of the NIS directive. To this end, a cooperation group consisting of representatives of the Member States, the Commission and ENISA was set up with four areas of work - planning, guiding, reporting and sharing.

The last of the main points of the directive concerns operators of essential services for the nation and providers of digital services. In particular, public or private companies operating in energy, transport, banking and healthcare, in financial market infrastructures, in the supply and distribution of drinking water and in the digital infrastructures must adopt security measures able to prevent risk, guarantee the security of systems, networks and information and manage accidents.

As well, digital service providers – that is the digital services online market, online search engines and cloud services (cloud computing) - will be required, according to the NIS directive, to implement appropriate security measures and to notify relevant incidents. In addition to the measures already envisaged for operators of essential services, the NIS Directive prescribes other specific security measures for digital service providers, such as the security of systems and installations, the management of business continuity, monitoring and testing, and compliance with international standards. The transposition process had to be completed in each Member State by May 9, 2018.

In September 2017, the Commission launched the **Strategic Plan for Cybersecurity**. The Plan aims to increase defense, deterrence and the resilience of information systems, based on three fundamental pillars: 1) building a resilient European system increasing the level of cybersecurity in the European Union; 2) creating an effective and univocal response to computer crimes, adapting penalties to the seriousness of the criminal action; and 3) encouraging international collaboration.

One of the most important aspects of the proposal concerned the creation of a **European Agency on Cybersecurity** - the result of the strengthening of the already existing European Information Security Agency and of the Networks (ENISA) – with a full and permanent mandate, with more tools and targets, to come into effect by 2020, when the current Agency mandate will expire. Ongoing training in security systems tops the objectives. The Agency will simulate computer attacks to allow Member States, in coordination with the European institutions and their agencies, to prepare forms of response to potential attacks, improving information and intervention times, thanks also to the creation, by 2018, of a platform for training.

The EU plan also aims to create a single system certification of cybersecurity to overcome the fragmentation currently existing in the presence of 4 main certifications (CPA, CSPN, BSPA, SOG-ISMRA) and to increase reliability, in terms of security, of purchased products.

On this topic, the Commission identified three priority areas - security in critical or high-risk applications, cybersecurity in widely-deployed digital products, networks, systems and services used by private and public sector alike to defend against attacks and apply regulatory obligations and the use of **"security by design" methods** in low-cost, digital, interconnected mass consumer devices which make up the Internet of Things. At the same time, the Commission underlined the specific issues of specific sectors and so, the necessity to encourage the development of their own approach and the definition of sector-specific cybersecurity strategies in areas such as financial services, energy, transport and health.

The Commission also focused on the importance of **skills**. In fact, effective cybersecurity relies heavily on the skills of the people concerned so it is necessary to develop cybersecurity education at all levels, starting from regular training of a cyber workforce, additional cybersecurity training for all ICT specialists and new specific cybersecurity curricula.

To promote cyber hygiene and awareness the Commission encourages Member States to maximize the availability of cybersecurity tools for businesses and individuals, accelerate the use of more cyber-secure tools in the development of e-government and also draw full benefit from the competence network, and make cyber-awareness a priority in awareness campaigns.

Last, but certainly not least, the carrying out of effective investigation and prosecution of cyber-enabled crime and a review of the criminal policy in the Member States. Here, the Commission encourages greater uniformity in the penalties applied in the Member States and the affirmation of the right of access to information by the victims of such crimes. It offers an adequate and simple assistance system and the creation of a close collaboration within the Union's judicial system, through strengthening existing structures and local Contact Points.

On 8 March 2019, the Commission and the High Representative proposed the establishment of a **horizontal sanctions regime to counter cyber-attacks**. The proposed regime has worldwide coverage and will enable a flexible EU response irrespective of the location from which cyber-attacks are launched and regardless of whether they are carried out by state or non-state actors.

In the same period (12 March 2019), the "***EU-China – A strategic outlook***" identified some actions to be endorsed by the European Council underlining the importance to safeguard against potential serious security implications for critical digital infrastructure and to detect and raise awareness of security risks posed by foreign investment in critical assets, technologies and infrastructure.

Regulation n. 2019/452 of 19 March 2019 (applicable from 11 October 2020) **establishing a framework for the screening of foreign direct investments in the Union,** provides a powerful instrument to detect and raise awareness of foreign investment in critical assets, technologies and infrastructure. It will further allow for identifying collectively and addressing security and public order threats posed by acquisitions in sensitive sectors.

Considering the importance and the impact of 5G networks and the critical issues on security, on 26 March 2019, the European Commission recommended a set of operational steps and measures to ensure a high level of **cybersecurity of 5G networks** across the EU. The Recommendation sets out a series of operational measures, encouraging Member States to conclude a national risk assessment of 5G network infrastructures by the end of June 2019 (considering various risk factors, such as technical risks and risks linked to the behavior of suppliers or operators, including those from third countries), underlining that EU Member States exclude companies from their markets for national security reasons, if they do not comply with the country's standards and legal framework, supporting exchange of information and the activity of the Commission and the European Agency for Cybersecurity (ENISA), also completing a coordinated risk assessment by 1 October 2019. In the field of cybersecurity, considering that the future European cybersecurity certification framework for digital products, processes and services foreseen in the Cybersecurity Act (which will be discussed later in the analysis) should provide an essential supporting tool to promote consistent levels of security, the Recommendation encourages Member States to immediately and actively engage with all other involved stakeholders in the development of dedicated EU-wide certification schemes related to 5G. In the field of telecoms, it underlines the necessity for Member States to ensure that the integrity and security of public communications networks are maintained, with obligations to ensure that operators take technical and organizational measures to appropriately manage the risks posed to security of networks and services. ENISA will complete a 5G threat landscape that will support Member States in the delivery by 1 October 2019 of the EU-wide risk assessment and by 31 December 2019, the NIS Cooperation Group should agree on mitigating measures to address the cybersecurity risks identified at national and EU levels.

On 7 June 2019, **Regulation n. 2019/881** of 17 April 2019 on ENISA and on information and communications technology cybersecurity certification, and repealing Regulation n. 526/2013 (**Cybersecurity Act**), was published in the Official Journal of the European Union. It will enter into force on 27 June 2019 (with the sole exception of a few articles - 58, 60, 61, 63, 64 and 65 - which relate to the national cybersecurity certification authorities, to the conformity assessment bodies and to the establishment of the European Group for the certification of cybersecurity (ECCG), which will enter into force on 28 June 2021).

It gives ENISA, the European Union Agency for Cybersecurity, a permanent mandate strengthening its role (art. 1-45) and defines an EU framework for cybersecurity certification, boosting the cybersecurity of digital products and services in Europe (art. 46-65).

The Cybersecurity Act aims to strengthen **the role of ENISA** setting a permanent mandate and allowing it to perform not only technical consultancy tasks, as it has done until now, but also activities to support the operational management of IT incidents by Member States. In this way, ENISA will be able to guarantee more concrete support, also regarding the implementation of the NIS Directive. The Regulation attributes specific powers and competences to ENISA to develop and implement Union policy and law, encourage operational cooperation at Union level, knowledge and information, public awareness of cybersecurity risks and education, international cooperation, research and innovation and defines the organization of ENISA in also setting specific rules on its budget.

ENISA will also support and promote the development and implementation of Union policy on **cybersecurity certification of ICT products, ICT services and ICT processes**, having a leading role in managing the certification system introduced by the Cybersecurity Act. ENISA will prepare a candidate scheme after consulting all relevant stakeholders by means of a formal, open, transparent and inclusive consultation process and maintain a dedicated website providing information on, and publicizing, European cybersecurity certification schemes, European cybersecurity certificates and EU statements of conformity. The Regulation fixes security objectives of **European cybersecurity certification schemes**, namely: a) to protect stored, transmitted or otherwise processed data against accidental or unauthorized storage, processing, access or disclosure during the entire life cycle of the ICT product, ICT service or ICT process; b) to protect stored, transmitted or otherwise processed data against accidental or unauthorized destruction, loss or alteration or lack of availability during the entire life cycle of the ICT product, ICT service or ICT process; c) to ensure that only authorized persons, programs or machines are able to access the data, services or functions to which their access rights refer; d) to identify and document known dependencies and vulnerabilities; e) to record which data, services or functions have been accessed, used or otherwise processed, at what times and by whom; f) to make it possible to check which data, services or functions have been accessed, used or otherwise processed, at what times and by whom; g) to verify that ICT products, ICT services and ICT processes do not contain known vulnerabilities; h) to restore the availability and access to data, services and functions in a timely manner in the event of a physical or technical incident; i) to ensure that ICT products, ICT services and ICT processes are secure by default and by design; j) to ensure that ICT products, ICT services and ICT processes are provided with up-to-date software and hardware that do not contain publicly known vulnerabilities, and are provided with mechanisms for secure updates.

The Regulation also identifies powers and structure of the **European Cybersecurity Certification Group** (art. 62).

4. Power breakfast main highlights

Cultivating capability: European competence center

Today, there is a profoundly fragmented cybersecurity approach between EU Member States. This fragmentation results from a lack of expertise, staff, and integrated national systems. This is particularly troubling because Member States with less advanced capabilities are a “backdoor entrance” into the EU digital market and present security risks for Europe as a whole. The clear vulnerability resulting from this degree of fragmentation makes the proposal for a European competence center paramount. The proposed center would be supported by every Cybersecurity Centre of Excellence in Europe –

representing 600+ public and private firms across the EU. Further, the proposal calls for a national coordination center in every Member State and that these national centers will report directly to the European competence center.

The central goal of a European competence center would be to better coordinate European cyber practices by increasing the capacity of all Member States to monitor, prevent, and respond to cybercrime. However, Europe must also address the overall lack of skills that have warranted the need for a center in the first place. Europe's struggle to recruit and maintain young talent has been troublesome. The prospect of leaving Europe for better opportunity in Silicon Valley or shifting from employment in the public sector to private sector is driving this problem. Plans to incentivize educated youth labor to stay in Europe must be developed to ensure a necessary labor force to protect Europe's cyber landscape. One approach should include investment in start-ups, to allow for the burgeoning of new technologies, practices, and European-based companies. Additional lessons may be drawn from the city of Be'er Sheva, Israel. Here, relationships between universities, companies, and state government have produced an environment highly conducive to recruiting and maintaining an ample supply of youth skill.

European certification framework

The framework for European cybersecurity certification, born with the passage of the Cybersecurity Act, is the EU's primary vehicle for enhancing the security of connected devices. Still in its early stages, the framework provides schemes that apply to three levels of security assurance (basic, medium, high). The framework, operated by the European Union Agency for Network and Information Security (ENISA), convenes an expert group and considers input from a range of stakeholders to advise the design of each certification scheme. In effect, the framework has perspectives from a diversity of backgrounds and expertise influence the design of certification schemes. As of now, the system is voluntary but there is discussion in the Member States about whether it should become compulsory.

The current certification framework is facing an uphill battle, as there is a gap of expertise and lack of clear, Union-wide standards and measurements. Facing these handicaps, it is clear not everything can be certified. This reality has stressed the need to pursue a strategic approach guided by sectoral emphasis. Sectoral emphasis is highly warranted for certification schemes affecting providers of essential services - transport, energy, digital, or water infrastructures. Providers of essential services are currently lacking clear standards from ENISA and are subject to varying requirements in each Member State. Due to the critical importance of this industry, comprehensive European cooperation is greatly needed.

Further, certification schemes require further development for sensitive technologies, such as medical devices, smart grids, and smart vehicles. These devices, incredibly reliant on IoT connection, are engaged in complex supply chains and, subsequently, face particular security challenges. These challenges beg the question of where certification is needed for which components of the supply chain.

The role of strategy in defensive and offensive practice

In the absence of wide-reaching EU cybersecurity policy, Europe has a limited capacity to defend its cybersecurity interests. However, orienting coordinated responses around strategic considerations can morph limited capacity into a substantial defensive force to protect Europe’s most vulnerable industries - banking, utilities, software, and automotive. When considering future joint efforts, it is imperative that data drives assessment of security priorities. These priorities should dictate the amount of time and resources that are invested into industry-specific responses, in order to best protect consumers, businesses, and the functioning of the single market.

However, the notion of effective defensive forces may be inextricably tethered to offensive forces. When looking to the international community, Israel stands out as a valuable example. Israel Defense Forces (IDF) personnel note that a lack of offensive capability limits the efficacy of defensive capability, as most cybercrime is organized by states and well-funded organizations. As the IDF is a global leader in cyber capabilities and sophistication, developing offensive strategy should be entertained by Europe. Additionally, the concept of marrying cybersecurity to artificial intelligence (AI) is gaining momentum, as AI has emerged as a primary way of attacking systems. Nevertheless, establishing synergy and linkage between civilian and military projects in Europe has proven extremely difficult. A lack of proposals stemming from the European Defense Fund (EDF) and worries from the Member States of encroaching on national sovereignty have limited offensive cyber developments.