European Commission

CYBERSECURITY

OUR DIGITAL ANCHOR

A EUROPEAN PERSPECTIVE

EUR 30276 EN

Joint Research Centre

Manuscript completed in June 2020

Contact information
Igor Nai Fovino
European Commission, Joint Research Centre, Ispra - Italy
Email: *igor.nai-fovino@ec.europa.eu*
Tel: +39 0332785809

EU Science Hub
https://ec.europa.eu/jrc

JRC121051
EUR 30276 EN

PDF	ISBN 978-92-76-19957-1	ISSN 1831-9424	doi:10.2760/352218	KJ-NA-30276-EN-N
Print	ISBN 978-92-76-19958-8	ISSN 1018-5593	doi:10.2760/967437	KJ-NA-30276-EN-C

Luxembourg: Publications Office of the European Union, 2020

How to cite this report: Nai Fovino I., Barry G., Chaudron S., Coisel I., Dewar M., Junklewitz H., Kambourakis G., Kounelis I., Mortara B., Nordvik J.p., Sanchez I. (Eds.), Baldini G., Barrero J., Coisel I., Draper G., Duch-Brown N., Eulaerts O., Geneiatakis D., Joanny G., Kerckhof S., Lewis A., Martin T., Nativi S., Neisse R., Papameletiou D., Ramos J., Reina V., Ruzzante G., Sportiello L., Steri G., Tirendi S., *Cybersecurity, our digital anchor,* EUR 30276 EN, Publications Office of the European Union, Luxembourg, 2020, ISBN 978-92-76-19957-1, doi:10.2760/352218, JRC121051.

CYBERSECURITY

OUR DIGITAL ANCHOR

A EUROPEAN PERSPECTIVE

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The Report ***Cybersecurity – Our Digital Anchor*** brings together research from different disciplinary fields of the Joint Research Centre (JRC), the European Commission's science and knowledge service. It provides multidimensional insights into the growth of cybersecurity over the last 40 years, identifying weaknesses in the current digital evolution and their impacts on European citizens and industry. The report also sets out the elements that potentially could be used to shape a brighter and more secure future for Europe's digital society, taking into account the new cybersecurity challenges triggered by the COVID-19 crisis.

According to some projections, cybercrime will cost the world EUR 5.5 trillion by the end of 2020, up from EUR 2.7 trillion in 2015, due in part to the exploitation of the COVID-19 pandemic by cyber criminals. This figure represents the largest transfer of economic wealth in history, **more profitable than the global trade in all major illegal drugs combined,** putting at risk incentives for innovation and investment.

Furthermore, cyber threats have moved beyond cybercrime and have become a matter of national security. The report addresses relevant issues including:

- **Critical Infrastructures:** today, digital technologies are at the heart of all our critical infrastructures. Hence, their cybersecurity is already – and will become increasingly – a matter of critical infrastructure protection (see the cases of **Estonia** and **Ukraine**).

> Cybersecurity is no longer a technological 'option', but a societal need.

- **Magnitude of impact:** the number of citizens, organisations and businesses impacted simultaneously by a single attack can be huge.
- **Complexity and duration of attacks:** attacks are becoming more and more complex, demonstrating attackers' enhanced planning capabilities. Moreover, attacks are often only detected post-mortem[1].
- **Computational power:** the spread of malware also able to infect mobile and Internet of Things (IoT) devices (as in the case of Mirai botnet), hugely increases the distributed computational power of the attacks (especially in the case of denial of services (DoS)). The same phenomenon makes the eradication of an attack much more difficult.
- **Societal aspects:** cyber threats can have a potentially massive impact on society, up to the point of undermining the trust citizens have in digital services. As such services are intertwined with our daily life,

any successful cybersecurity strategy must take into consideration the human and, more generally, societal aspects.

This report shows how the evolution of cybersecurity has always been determined by a type of cause-and-effect trend: the rise in new digital technologies followed by the discovery of new vulnerabilities, for which new cybersecurity measures must be identified. However, the magnitude and impacts of today's cyber attacks are now so critical that the digital society must prepare itself before attacks happen. Cybersecurity resilience along with measures to deter attacks and new ways to avoid software vulnerabilities should be enhanced, developed and supported.

The 'leitmotiv' of this report is the need for a paradigm shift in the way cybersecurity is designed and deployed, to make it more proactive and better linked to societal needs.

Given that data flows and information are the lifeblood of today's digital society, cybersecurity is essential for ensuring that digital services work safely and securely while simultaneously guaranteeing citizens' privacy and data protection. **Thus, cybersecurity is evolving from a technological 'option' to a societal must.**

From big data to hyperconnectivity, from edge computing to the IoT, to artificial intelligence (AI), quantum computing and blockchain technologies, the 'nitty-gritty' details of cybersecurity implementation will always remain field-specific due to specific sectoral constraints. This brings with it inherent risks of a digital society with heterogeneous and inconsistent levels of security.

To counteract this, we argue for a **coherent, cross-sectoral and cross-societal cybersecurity strategy which can be implemented across all layers of European society.**

This strategy should cover not only the technological aspects but also the societal dimensions of 'behaving in a cyber secure way'. Consequently, the report concludes by presenting a series of possible actions instrumental to building a **European digital society secure by design.**

INTRODUCTION

We are living in an era of great opportunities enabled by digital technologies: access to information and knowledge has never been as easy as it is today. Global economic growth[2] and human well-being are becoming increasingly dependent on the adoption of digital technologies.

However, this intertwining of digital technologies in our daily lives brings with it heightened vulnerability to the deliberate exploitation of unsecure digital systems. This increases the potential impact of cyber attacks while reducing the advantages of the digitalisation of our society. To understand why cybersecurity is so central, we need look no further than the COVID-19 crisis which has triggered an increase in the cybersecurity risk facing European businesses, governments and citizens. Cyber attacks have become more frequent as the weaknesses resulting from the focus on fighting the pandemic have been exploited.

> Time is a crucial factor: we need to move quickly in an attempt to reduce the attacker's advantage.

> "Global economic growth and human well-being *are increasingly dependent upon the adoption of digital technologies.*"

Digital technologies are currently at the heart of all our critical infrastructures. Hence, their cybersecurity is already, and is becoming increasingly, a matter of **national security.** Therefore, cybersecurity is both costly and crucial.

The number of citizens impacted simultaneously by a single cyber incident can be huge as a consequence of the pervasiveness of connected devices: **3 billion** accounts in the attack on Yahoo in 2013, **77 million** users in the attack on Sony PS3 in 2011, **1.3 millio**n and **250 000** impacted citizens, respectively, in the attacks on Estonia and Ukraine in 2017, and 7 major security incidents in December 2019 alone (CSIS, 2020), just to cite a few examples.

At the same time, cyber attacks are also becoming more and more complex, demonstrating the attackers' enhanced planning capabilities and knowledge. An example of the growing complexity is the spread of malware able to infect both mobile and IoT devices, hugely amplifying the distributed computational power of cyber attacks while making it more difficult to effectively mitigate an attack.

> Contrary to common belief, cybersecurity *is not merely a matter of technologies.*

As cyber attackers operate outside the norms of regulation and law, this flexibility gives them a significant advantage over defenders who normally do not enjoy such freedom. The attackers have the crucial advantage of time which in cyberspace can be measured in milliseconds.

Contrary to popular belief, cybersecurity is not merely a matter of technologies. Rather, it has an impact on society and is influenced by the attitude of individuals while they are 'living their digital life'. Their preferences, desired digital services and the way in which they are used are the first considerations when trying to design a more secure cyberspace. Once again, the explosion of teleworking and online schooling during the first half of 2020 due to the COVID-19 crisis and, as a consequence, the higher number of cyber attacks show the extent to which our lives are intrinsically dependent on digital services and why we need urgently to increase their security. Cybersecurity is thus a very heterogeneous and multi-sectorial domain combining diverse needs, expertise and constraints.

Thus, the scope of this report is twofold:

- It gives the reader clear elements to reflect on the weaknesses of the digital evolution and the resulting impact on European society.
- It proposes the components which could potentially shape a new secure European society.

To achieve this scope, the report is organised as follows: *Chapter 1,* uses a brief historical excursion to provide the basic elements for understanding what cybersecurity is today. *Chapters 2, 3* and *4* analyse why the societal and technological transformations of our society require a more fit-for-purpose cybersecurity, while *Chapter 5* draws a picture of the evolution of cybersecurity threats and related risks. At the time of writing of this report the world is facing the COVID-19 pandemic. *Chapter 6* provides a snapshot of the cyber threats and challenges caused by this exceptional event, magnifying one more time how cybersecurity is today a cornerstone of our society, especially in times of crisis. On the basis of the evidence presented in the previous sections, *Chapter 7* suggests a number of possible strategies to mitigate cyber threats. The report concludes by identifying six possible policy intervention areas to foster a European digital society secure by design.

7 **Cybersecurity Risk Mitigation Strategies** p. 83

6 **Cyberthreats evolution at the time of COVID-19** p. 71

8 **Towards a more secure digital ecosystem** p. 95

> “Cyber attackers do not adhere to *regulations, ethical norms or cultural traditions.*”

SUMMARY

The development of the internet during the last decades didn't happen without events characterizing the vulnerability of the network. Over the years, a wide set of policy initiatives have been taken to ensure confidentiality, integrity and availability, of data and information. Increasing and emerging threats have always gone in parallel with new technologies and require therefore innovative mitigation measures. The cybersecurity concept must be extended to other disciplines and combined with the existing applications and technologies in the digital society. Investments are needed to strengthen security, but is it today possible to determine univocally the level of cybersecurity of our society?

CYBERSECURITY: EVOLUTION OF A MULTIFACETED DISCIPLINE

Today, cybersecurity plays a central role in guaranteeing the security of our society. However, cybersecurity is neither a term defined in a straightforward way nor simply a well-bound sub-domain of a single academic area. Over the years, it has become a highly cross-border and continuously evolving discipline, making it difficult to grasp its full extent at a single glance. A brief evolution of cybersecurity is provided here leading to a discussion on the situation today.

> This epochal shift is a journey, and like every journey, the road is paved by risks and threats.

1.1. 40 years of cybersecurity

This section highlights some insights into the joint evolution of digital technologies, cyber threats and cybersecurity.

1970s and 1980s – the early days

Cybersecurity's roots go back to the 1970s, the time of ARPANET, considered to be the precursor of the internet. The first early examples of malicious software and computer intrusions date back to that decade. In 1983, Fred Cohen presented a program capable of spreading itself from one machine to another, carried as a parasite in a legitimate application, and basically demonstrating the first computer malware (Cohen, 1984). In 1988, the first malware aimed at disrupting services was deployed causing a massive DoS in ARPANET by infecting 10 % of the computers connected to the network (Kienzle and Elder, 2003).

Consequently, policymakers took action: the US Administration released the Computer Fraud and Abuse Act in 1986 (Doyle, 2014), followed by the Computer Security Act of 1987 and, in 1990, by the Computer Misuse Act in the United Kingdom (Great Britain, 1990).

1990s – the birth and popularisation of the internet and World Wide Web

The 1990s were marked by the birth and subsequent popularisation of the World Wide Web (WWW) and internet. In this context, software and network security started to become seen as a key priority by industry and governmental

organisations. New standards providing additional security requirements on network protocols started to emerge along with good practices[3]. Inevitably, the growing popularisation of the internet led to an increase in the attack surface. Internet protocols were initially deployed with usability in mind but without any security considerations. Inner flaws started to be exploited to launch massive attacks, such as the Melissa worm (Kienzle and Elder, 2003), infecting thousands of computers worldwide and disrupting email services.

2000s – The modern digital era

The first decade of the millennium was marked by the birth of Web 2.0[4]. In 2000, the number of internet users exceeded 300 million, with 73 % of them in the top 10 richest countries (Pingdom, 2010). This massive adoption opened the door to a wider range of attacks, such as the 'ILOVEYOU' worm, which spread like wildfire in May 2000, infecting over 50 million systems worldwide during its first 10 days. In 2001, the Council of Europe proposed the Convention on Cybercrime, the first international treaty on crimes committed via the internet, which has been signed and ratified by more than 60 countries since then (Council of Europe, 2001). In 2002, the EU adopted the ePrivacy Directive (European Parliament and Council of the European Union, 2002) to safeguard the confidentiality of electronic communications in the EU; while in 2003, the US Department of Homeland Security launched its National Cyber Security Division.

> "'ILOVEYOU' worm spread like wildfire in May 2000, *infecting over 50 million systems worldwide during its first 10 days alone.*"

2010s – A race for digital transformation and cyber attacks

Throughout this decade, the number of cyber physical systems[5] continued to increase (a new generation of medical devices, industrial automation and control systems, etc.). This era was also characterised by the emergence of the big data phenomenon. These trends, paired with the greater hyperconnectivity of devices and the upsurge of AI, created new challenges for cybersecurity.

Cyber criminals also capitalised on the opportunities offered by these developments. In 2012, a wave of cyber attacks impacted millions of users worldwide who saw their personal data leaked online and their credit cards stolen[6]. This new generation of cyber attacks was characterised by their impact which, in many cases, went far beyond the economic dimension[7]. Massive ransomware campaigns and global botnets hit millions of users worldwide in industry, government, academia and households alike. These attacks took advantage of the proliferation of connected devices, through prominent examples such as the WannaCry ransomware global outbreak (Smart, 2018) and the Mirai botnet (Antonakakis et al., 2017).

Cybersecurity began to be placed at the centre of European policy initiatives[8], such as the General Data Protection Regulation (GDPR), the Network Information and Security (NIS) Directive and the European Cybersecurity Act.

The cybersecurity challenge ahead

Looking at the past 40 years, three trends emerge: (1) The circular sequence of 'new technology, new cybersecurity threats and vulnerabilities,

new mitigations'; (2) the constant increase over the years of the potential magnitude of attacks in term of size of targets and impact; and (3) a general increase in the attack surface. The last trend is due to a wide number of factors, including the pervasiveness of digital activity in daily life and the massive diffusion of IoT.

As a result, digital society can no longer afford to be reactive, remediating cyber threats once they have occurred. The magnitude and impacts of today's cyber attacks can be so devastating that our society needs to prepare for potential attacks. The targeting of hospitals and research centres by cyber criminals, including state-sponsored actors, during the COVID-19 pandemic has illustrated the current lack of globally agreed norms in cybersecurity and there is a growing realisation that some type of 'digital Geneva Convention' is required. Indeed, back in 2012, former US Defense Secretary, Leon Panetta, first alluded to the potential for a 'Cyber Pearl Harbor' attack against the critical infrastructures of any nation state as being just around the corner.

> "The potential for a 'Cyber Pearl Harbor' attack against *the critical infrastructures of any nation state is just around the corner.*"

To this end, elements of cybersecurity resilience along with measures to deter and novel ways to avoid software vulnerabilities should be enhanced, developed and supported.

1.2. Cybersecurity today

Cybersecurity has become a horizontal multi-domain discipline encompassing many fields and approaches. Indeed, due to the links between the manifold aspects of our digital and physical lives, the concept of cybersecurity involves knowledge coming from many different, and sometimes very distant scientific disciplines (European Commission and Directorate-General for Research and Innovation, 2017).

At the European level, cybersecurity is defined in Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 as 'the activities necessary to protect network and information systems, the users of such systems, and other persons affected by cyber threats'.

Thus, it is not only a matter of foundational research (e.g. in cryptography) but also a matter of technology, societal position, education, culture and, ultimately, policies.

Attempts to find a correct definition for and to standardise the term from a European perspective have been collected by the European Union Agency for Cybersecurity (ENISA) (ENISA, 2016a), including common definitions and official attempts by organisations. For the sake of completeness, a short glossary of the most relevant definitions linked to cybersecurity is included in this report. From this list, according to the most authoritative standard ISO/IEC 27032:2012: *'Cybersecurity' is defined as the 'preservation of confidentiality, integrity and availability of information in the cyberspace[9]'.*

> Cybersecurity began to be put at the centre of policy initiatives, *such as the General Data Protection Regulation, the NIS Directive and the European Cybersecurity Act.*

Confidentiality, integrity and availability are often identified as the key pillars of cybersecurity. As a very general definition (Bishop, 2003), we can say that:

- **Confidentiality** is the concealment of information or resources.
- **Integrity** refers to the trustworthiness of data or resources (and is intended as a set of mechanisms to prevent unauthorised or improper changes).
- **Availability** refers in general to the ability to legitimately use the information or resources (services) desired.

Unfortunately, for practical purposes, this definition does not provide a lot of information, as recognised by cybersecurity expert Matt Bishop (Bishop, 2003) who notes that the interpretation of these three aspects varies according to a given context.

For instance, it can be said that cybersecurity is not only about data/information protection but includes all 'things' which are vulnerable via information and communications technology (ICT) – i.e. information in any form, and including things like cars, traffic lights, IoT appliances and unmanned aerial vehicles, to name but a few. In other words, it is impossible to address cybersecurity in absolute terms. The most viable solution is to leave the definition somewhat open and connect the practical meaning of cybersecurity to its many sectorial applications and problems.

Nevertheless, understanding how exactly cybersecurity is connected to other technical disciplines and the technological areas which are its main drivers is a very important topic touching on many aspects of cybersecurity policymaking, such as:

- the skills of a cybersecurity expert to be considered in creating and fostering coherent curricula in education across Europe;
- the scientific domains to be boosted to enhance the advance of cybersecurity as a discipline;
- the market domains to be stimulated to create a healthier European cybersecurity industry.

On the basis of these considerations, in 2018, the European Commission published an overarching cybersecurity taxonomy (Nai Fovino et al., 2019), validated by key cybersecurity organisations and through a survey involving more than 700 European research centres (Lazari et al., 2018). This taxonomy offers a clear and precise indication of the areas of fundamental research and the relevant sectorial domains. By combining

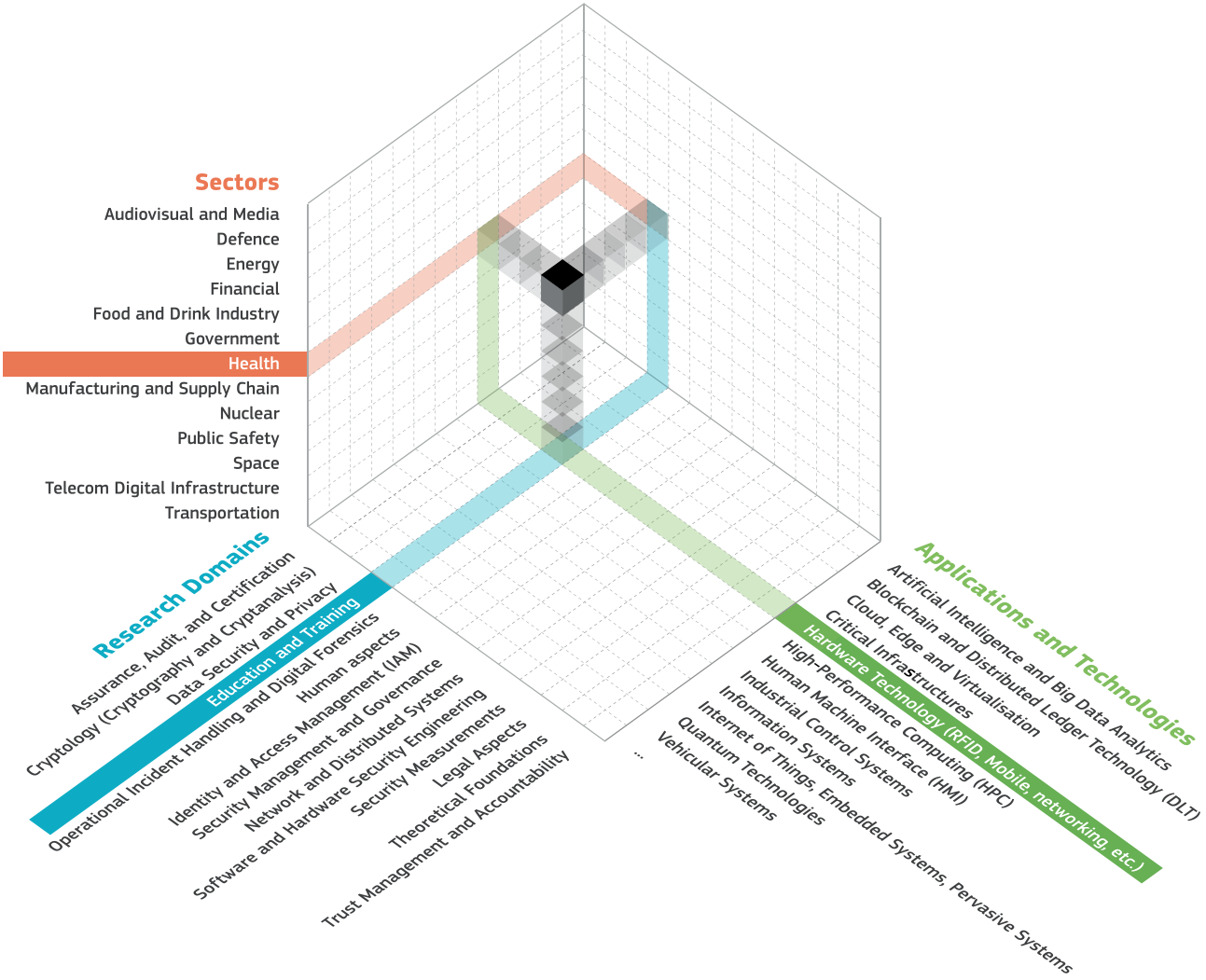


Figure 1: High-level view of the cybersecurity taxonomy

> Cybersecurity is not only about data/information protection, *but includes all 'things' such as cars, traffic lights, IoT appliances.*

both dimensions with existing applications and technologies in the digital society, a three-dimensional representation of the cybersecurity realm can be obtained, as depicted in *Figure 1.*

Cybersecurity is shown as a large, multifaceted discipline rather than a sub-area of computer science. While it is involved everywhere, each cell of this cube requires particular theoretical approaches and specific technical implementation and skills.

1.3. Can cybersecurity be measured?

While organisations invest a lot of money and human capital in enforcing and strengthening their cybersecurity, there is still no globally accepted and standardised way of measuring it. According to a 2019 Court of Auditors' report, this makes it difficult to decide which investments have resulted in a safer organisation. Although sporadic efforts have been made, including the Potomac Institute's Cyber Readiness Index 2.0 (The Potomac Institute for Policy Studies, 2016), there is no explicit system that can be used to quantify cybersecurity objectively. Organisations typically use qualitative measures of security rather than quantitative ones. In fact, according to a recent survey (Moore, Dynes and Chang, 2016) involving chief information security officers, industry best practices and frameworks were deemed to be the most important factors to access an organisation's cybersecurity position, while quantitative methods measuring the effectiveness of security controls were placed much lower down the list.

> "Cybersecurity is as a large, multifaceted discipline rather than a sub-area of computer science. *For that reason, there is still no globally accepted way of measuring it.*"

In response, the R Street Institute launched an initiative which resulted in a partially annotated bibliography entitled 'Resources for measuring cybersecurity' (Waldron, 2019). The authors indicate that a system of metrics is required which decision-makers can use and which need to be agreed and accepted within the relevant communities.

Their key findings are summarised as follows:

- Some measurement methodologies try to assess how changes in security measures will affect an organisation using forecasts rather than actual results, while others are basically reactive checking the effectiveness in terms of positive increase or harm done after a security measure has been implemented and deployed.
- A number of methodologies assess security by relying on frameworks and checklists of factors believed to strengthen security and by measuring compliance rates with a baseline set of best practices.
- A third set of methodologies focuses on resiliency rather than prevention, i.e. how quickly a system is restored after an attack.

SUMMARY

The rise in new disruptive digital technologies and their integration in our lives is generating and driving a profound transformation. In a new world where physical and digital blend together, the traditional measures to guarantee trust are no longer sufficient as they rely mainly on a societal model which has the material world as its centre of balance. Cybersecurity is an essential societal need, reinforcing the idea of a 'digital society secure by design'. It is also a value in which privacy, trust and data protection must converge in the building of trust. This chapter gathers together research from different sources and disciplinary fields, providing multidimensional insights into the evolution of cybersecurity from the advent of the digital era to the present day, and looking forward to the future needs of our society.

CYBERSECURITY AT THE HEART OF SOCIETAL TRANSFORMATION

What is new in the ongoing digital transformation is the speed and scale of its evolution, making it the first technological and societal revolution to affect almost all of mankind simultaneously. Our digital world is now much more complex and cumbersome to understand and therefore harder to protect as a whole. Cybersecurity is thus an essential element of our society.

The main factor that characterises this digital transformation is a novel technological paradigm of **datafication and thingification:** everything becomes a 'connected thing' able to produce data *(Figure 2).*

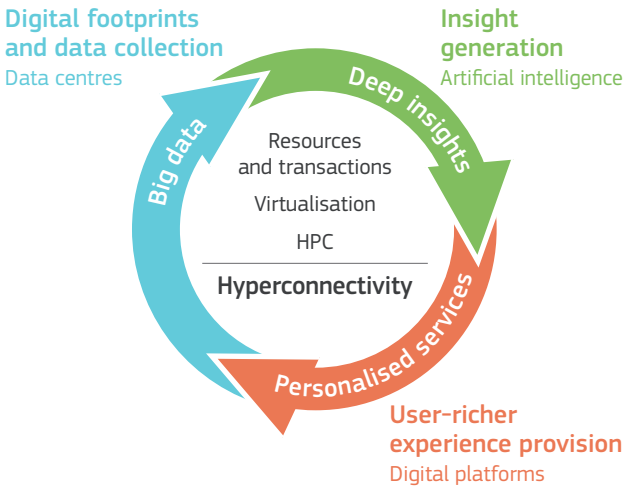


Figure 2: Simplified view of the datafication/ thingification paradigm processes

> Cybersecurity is becoming an essential element of the new digitally driven society.

These developments are directly connected to the ongoing explosion of connected humans and devices, where many of the latter are deployed in an 'install-and-forget' manner.

A direct consequence of this tight intertwining between things, humans, AI and data is that the more our world goes digital, the more its attack surface increases and the bigger the potential impact of cyber attacks on our society.

This would be sufficient already to highlight the centrality of cybersecurity in the technological evolution of digitalisation. Yet, there are more profound reasons why cybersecurity must be considered as a cornerstone of society today.

Traditionally, societal priorities have centred on the security and well-being of citizens and the stability of the economy, achieved through policy initiatives, industrial standardisation, certification processes, law enforcement and civic education. This 'magic square of enablers' is essential to ensure citizens' trust in governing institutions and the society in which they live.

Traditional measures to guarantee trust are no longer sufficient. In this context, cybersecurity becomes our digital anchor, enabling trust within society to be re-established and guaranteed. Cybersecurity should thus be considered as an essential societal need reinforcing the idea of a 'digital society secure by design'.

The rapid exploitation by cyber attackers on the COVID-19 pandemic to attack systems and individuals reinforces this need.

> *"Digital technologies have become the foundation of all modern innovative economic and social systems."*

2.1. Cybersecurity in the context of privacy, data protection and trust

If we think of digitalisation, immediately we think of 'online services', e-commerce, IoT, smart devices, etc. Their common denominator is the establishment of a minimum level of trust in the operations performed, in privacy and in data protection. Cybersecurity is the enforcer of these three dimensions, ensuring that trust is not misattributed, that digital processes maintain their integrity and availability, and that privacy and data protection are well preserved.

2.1.1 Privacy and cybersecurity

European citizens have the fundamental right to respect for their private life, home and communications[10].

The rise of AI and big data analytics pose new privacy challenges with implications for cybersecurity. For example, new techniques can be used to re-identify anonymised data by inferring from multiple and large databases.

Hence, there is an urgent need to rethink the way in which online services are designed, putting privacy and cybersecurity at the core of the design process from the outset.

Improving the level of transparency and usability of online services would facilitate this process. Transparency is about informing users on how their data is handled by digital services, including processing, storage and distribution to other parties. Only by understanding these data-handling aspects are users able to evaluate the privacy and cybersecurity risks. Therefore, cybersecurity is also a matter of awareness-raising and information.

Another important factor is the abundance of powerful anonymisation tools, including Tor, I2P, Freenet, Retroshare, and GNUnet. While they make a major contribution to the fight against censorship, the right to freedom of expression, and protection of the individual's privacy and anonymity, they constitute powerful attack vectors in the hand of aggressors wishing to conceal illicit activities and minimise their attack footprint.

2.1.2 Data protection and cybersecurity

In the EU, data protection is enshrined in Article 8 of the Charter of Fundamental Rights (European Union, 2012). In addition, the GDPR (European Parliament and Council of the European Union, 2016b), which entered into force in 2018, puts forward a set of rules designed to ensure the protection of citizens' personal data and strengthen their fundamental rights.

The GDPR acknowledges the importance of cybersecurity to protect personal data as a prerequisite for the collection and processing of personal data[11]. Experience shows that cybersecurity incidents due to the lack or ineffective implementation of proper cybersecurity mechanisms can lead to massive personal data breaches, affecting hundreds of millions of individuals and harming the reputation of the organisations involved.

Cyber attackers have started to recognise the value that the personal data of potential victims holds for them. Personal data breaches containing user passwords are regularly abused to conduct cyber attacks, namely impersonating users, bypassing authentication mechanisms, etc.

The GDPR introduces the principles of *data protection by design and by default;* the by design principle refers to the need to consider data protection requirements starting from the inception and design phases of a product or service, while the by default principle refers to the fact that even without explicit configuration by users, the product or service ensures a minimum level of data protection. Both principles are in line with the security by design and by default principles well established and adopted by the cybersecurity community.

Only effective integration and close cooperation between data protection and cybersecurity can ensure that personal data will be well protected and will not be misused and that citizens will ultimately be in control of their personal data.

2.1.3 Trust and cybersecurity

In today's hyperconnected digital world, trust is a necessary requirement to ensure stability and growth in the digital economy and foster digital transformation. In this context, cybersecurity and data protection are key enablers to delivering trust.

In the context of digital transformation, determining without doubt the identity of other interactors and getting a guarantee of the correctness and integrity of their actions are part of the process to correctly evaluate the level of trust/risk of a digital service.

However, trust should not be considered only in the context of digital interactions: if trust in digital is missing, the roll-out of big digital infrastructures, from energy smart grids to intelligent transport systems, e-government services, etc. would never take off. Obviously, there are also societal implications in this equation as trust is at the foundation of a secure society. Given the importance of trust, any element that strengthens its position is even more crucial.

Businesses, governments and citizens are becoming increasingly concerned by the potential impacts of cyber threats, such as massive personal data breaches, ransomware attacks, cyber extortion campaigns, cyber espionage or state-sponsored cyber attacks. As a result, users of digital products and services inevitably measure the benefits they can obtain against the potential cybersecurity and data protection threats they might have to face. The trade-off is obviously subjective and is linked to personal experience, interests, culture and age, among other factors. Thus, trust in digital services and products becomes intrinsically linked to the perception that individuals and organisations have of their reliability, security and safety.

Ensuring digital services work safely and securely, while guaranteeing citizens' privacy and data protection, illustrates that cybersecurity has evolved from a technological 'option' to a societal need.

2.2. The economics of cybersecurity

In most industries, **market forces** generate important incentives for companies to improve their products and services. However, the absence of effective competition in the digital sector means users can exert minimal influence on vendors to provide solutions to revealed vulnerabilities, resulting in the delayed release of solutions or poor-quality solutions (Jo, 2017).

When users have either the possibility or willingness to switch to competing products as a response to the emergence of vulnerabilities, vendors may face stronger incentives to create more-secure products. However, consumers often face high switching costs – i.e. they are not very likely to switch to a different provider in the case of known security weaknesses either concerning the software they use or in the software used by the vendors of the products and services they buy (Ablon et al., 2016).

Research has shown that firms' stock prices are negatively affected by announcements of cybersecurity breaches, although this effect only seems to apply in the short term (Kannan, Rees and Sridhar, 2007). In other words in the long run investors do not seem to care about reputational damage from cyber attacks. An important point here is that while small and medium-sized enterprises (SMEs) are the foundation of the EU economy (Hope et al., 2017), they are also more vulnerable to cyber attacks. Such vulnerabilities, which include a lack of formal cybersecurity policies, skills and expertise, shortage of financial resources, and incorrect attitudes towards risk management and cybersecurity, negatively influence their resilience to security threats.

Furthermore, **incentives** for different agents may not be aligned. For example, hospital managers and/or labs require medical records to improve service provision, financial management and possibly also research but these interests are not necessarily aligned with the patients' desire for

privacy. Misaligned incentives across network/service providers and other related parties also exist. For instance, while ingress packet filtering (BCP 38) was ratified almost 20 years ago, it has failed to solve the issue of source IP address spoofing due to fundamental **incentive misalignment.** Currently, a network provider which pays to adopt BCP 38 receives no direct benefit as any benefit goes to other networks and not the network provider itself. A more viable solution needs to provide value to the party investing in the solution rather than someone up- or downstream.

The design of information systems is characterised by an **efficiency-resilience trade-off.** Network convergence has allowed for the joint provision of several communication services by a single company. This represents enormous efficiencies as different applications can run on a common infrastructure. Business continuity now depends critically on the continued operation of the internet, and one single failure may have important spillover effects in many sectors. However, an individual company decision to improve efficiency by reducing operating costs does not take into account the implied increase in long-term/cascading vulnerabilities. Once again, incentives for short-term efficiency gains are not well aligned with incentives for reducing long-term vulnerability.

> *"The pace of innovation is surging and killer applications are emerging much more frequently than in the past."*

Several benefits can accrue from sharing cybersecurity information (Gal-Or and Ghose, 2005). However, the current industry context does not provide sufficient economic arguments to support cooperation and to justify the required investments for greater coordination. While public initiatives may create mechanisms enabling better access to information, effective voluntary initiatives among relevant stakeholders would also significantly improve coordination efforts.

Information asymmetries arise due to strong incentives to under-report incidents. When such asymmetries exist, society may fail to invest in appropriate defences. Poorly informed agents (consumers and firms) unable to accurately understand real threats and vulnerabilities will be inclined to rely on poor cybersecurity solutions. On the other hand, security providers will not be incentivised to bring better technologies to the market to help users protect themselves against the more serious threats.

On a positive note, bug bounty programs organised by numerous organisations and companies allow vulnerabilities to be detected and resolved before they are exploited by threat actors. This proactive practice can be further encouraged and fostered by governments by providing tax-relief programmes or other incentives to participating organisations.

One important characteristic of the information technology industry is the existence of different types of **externalities,** i.e. situations where individuals' actions have side effects on others. The three most relevant are network externalities, externalities of insecurity, and interdependent security. The software industry is highly concentrated, mainly due to the benefits of interoperability. This feature is also known as network externalities: the larger the network, the greater the value to each of its members (Duch-Brown, 2017).

The choice of an operating system is determined not only on quality and price but also on the number of other users who have adopted it. This helps to explain one of the basic weaknesses of security: as platforms exploit network externalities to build their privileged market position, they must attract suppliers of complementary products as well as direct users/customers. Given that it is more difficult to develop applications for more-secure software or systems, security is not considered properly until dominance has been achieved and sometimes not even then.

By definition, the lack of cybersecurity creates negative externalities: a compromised computer can harm more computers and/or systems than the host itself. In these cases, the societal costs derived from cyber attacks are greater than the financial loss to an individual or a company in monetary terms.

Interdependent security is another type of externality related to cybersecurity. Security investment by an individual creates positive externalities for others who may no longer have incentives to pursue their own investments (Kunreuther and Heal, 2003). The result of this process is free riding: agents will not bother to invest in security when they know that other players will not invest, leaving them vulnerable in any case (Varian, 2004).

This also impacts on another aspect of the cybersecurity economy: the difficulties faced by the few European cybersecurity suppliers (typically SMEs operating in niche cybersecurity market segments) in a global market dominated by non-EU suppliers.

Improving the competitiveness of Europe's cybersecurity industry is indeed paramount to ensure the security of critical digital assets and, in general, to improve European autonomy in the digital world. A key role will be played in this area by the Horizon Europe and Digital Europe funding programmes.

2.3. The cybersecurity policy landscape

Cybersecurity goes hand in hand with the development of technology and the ensuing digital transformation of society. Today, digitisation, digital identity, privacy, data protection and, crucially, shifting challenges in the safety and security of our societies are all of major importance in policymaking, and all connect to cybersecurity.

Arguably, the most significant actors in the cybersecurity arena are the states *per se*. That is, everything starts with a country's short- or mid-term strategic vision and plan and related actions to achieve it[12]. With this in mind, a basic priority for governments should be the shaping of a comprehensive cybersecurity strategy – accompanied by the appropriate resources to fund initiatives – that stipulates a competent authority in charge of the country's national cybersecurity position. For instance, some Member States have as strategic goal to increase the share of gross domestic product due to the digital economy, acknowledging that their future development and growth relies on their capacity to safeguard their digital economy. This requires investing appropriately and undertaking structural reforms.

Given that the digital transformation knows no borders, cybersecurity has become internationalised. Challenges facing the international community include future international collaboration on cybersecurity regulations, standardisation, cross-border prosecution of cybercrime and international law, and how to react to an increasing theatre of hybrid threats.

The following subsections outline the most significant efforts to date by countries, unions of states, academia, agencies for cybersecurity, and think-tanks to mould and develop cybersecurity and strategic risk management plans and frameworks.

2.3.1 The EU landscape

In February 2020, the Commission issued its ideas and actions for a digital transformation that works for all, reflecting the best of Europe: open, fair, diverse, democratic and confident. It proposes a European society powered by digital solutions that put people first, opens up new opportunities for businesses, and boosts the development of **trustworthy technology** to foster an open and democratic society and a vibrant and sustainable economy. Three strategic documents were issued, namely:

- a Communication on Shaping Europe's digital future (European Commission, 2020c), which sees cybersecurity as a principal ingredient in a successful digital transformation where European citizens and businesses trust that their applications and products are secure;
- a White Paper on Artificial Intelligence (European Commission, 2020b);
- a European Strategy for Data (European Commission, 2020a).

Cybersecurity is a transversal dimension underpinning this Commission's priority to build 'a Europe fit for a digital age'.

Over the last decade, the EU has addressed a wide range of cybersecurity measures, further details of which are provided in *Table 1.* Since 2016, in particular, the emphasis on cybersecurity has increased significantly with the adoption of the NIS Directive which pushes industry and relevant players to reduce vulnerabilities and to strengthen resilience. This has been complemented by the signature between the EU and the European Cyber Security Organisation (ECSO) of a public-private partnership to support all types of projects and initiatives to develop cybersecurity within the EU.

Table 1: Summary of EU initiatives relevant to cybersecurity

Date	EU initiative	Reference
19/02/2020	Shaping Europe's Digital Future White Paper on Artificial Intelligence A European Data Strategy (European Commission, 2020a)	 COM(2020) 65 final COM(2020) 66 final
26/03/2019	Cybersecurity of 5G Networks (European Commission, 2019)	C(2019) 2335 final
12/09/2018	Proposal for a Regulation of the European Parliament and of the Council establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres (European Commission, 2018c)	COM(2018) 630 final
13/06/2018	Joint Communication to the European Parliament and the Council – Increasing resilience and bolstering capabilities to address hybrid threats (European Commission, 2018b)	JOIN/2018/16 final
13/09/2017	Joint Communication to the European Parliament and the Council – Resilience, Deterrence and Defence: Building strong cybersecurity for the EU (European Commission, 2017b)	JOIN/2017/0450 final

Date	EU initiative	Reference
13/09/2017	European Commission, Regulation of the European Parliament and of the Council on ENISA, the 'EU Cybersecurity Agency', and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification ('Cybersecurity Act') (European Commission, 2017d)	COM(2017) 477 final
13/09/2017	'Commission Recommendation 2017/1584 on coordinated response to large-scale cybersecurity incidents and crises' (European Commission, 2017a)	C/2017/6100
07/06/2017	Draft Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ('Cyber Diplomacy Toolbox') – Adoption	9916/17
March 2017	Report of the High-Level Advisory Group of the EC Scientific Advisory *Mechanism Cybersecurity in the European digital single market.* 2017 (European Commission and Directorate-General for Research and Innovation, 2017)	
06/07/2016	Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (European Parliament and Council of the European Union, 2016a)	EU Directive 2016/1148
15/07/2016	European Cyber Security Organisation (ECSO), 'Cyber Security contractual Public-Private Partnership,' ECSO – European Cyber Security Organisation (ECSO, 2019)	
27/04/2016	European Parliament and Council of the European Union, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)	Regulation (EU)2016/679
06/04/2016	'Joint Communication to the European Parliament and the Council - Joint Framework on countering hybrid threats a European Union response' (European Commission, 2016b)	JOIN(2016) 18
28/04/2015	Communication from the 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, 2015)	COM/2015/0185
07/02/2013	Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Cybersecurity Strategy of the European Union: 'An Open, Safe and Secure Cyberspace' (European Parliament et al., 2013)	JOIN/2013/01

The 2017 Joint Communication on Cybersecurity (European Commission, 2017b) represents the most comprehensive piece of EU policymaking regarding cybersecurity, grouping measures into three pillars of European cybersecurity policy: resilience, deterrence and defence.

The 'Cybersecurity Act' (European Commission, 2017d) focuses on the definition of cybersecurity certification processes and standards for ICT products and gives a permanent mandate to ENISA, the EU Agency for Cybersecurity. As far as hybrid (cyber) threats are concerned, there have been Joint Communications to the European Parliament and the Council entitled 'Joint Framework on countering hybrid threats' (European Commission, 2016b) in April 2016, and 'Increasing resilience and bolstering capabilities to address hybrid threats' in June 2018 (European Commission, 2018b).

Likewise, the 'Cyber Diplomacy Toolbox' will provide the means for coordinating a response by EU Member States to malicious cyber activities at the EU level. Other complementary measures include the 'blueprint', a recommendation on addressing severe, large-scale cybersecurity incidents, the creation of a European Cybersecurity Competence Centre to coordinate a network of cybersecurity competence centres, and specific guidance on how to address cybersecurity measures in 5G networks.

At every stage, the development of a European cybersecurity policy is strongly guided by the special character of the EU whereby it has to provide a common link between Member States' national security agendas while guided by European core values and fundamental rights.

2.3.2 Academia, agencies for cybersecurity, and think-tanks

Academia, think-tanks, and relevant communities have also started compiling methodologies to assist countries and organisations in their cyber preparedness. The Potomac Institute's Cyber Readiness Index 2.0 (CRI) offers an experience-based methodological framework for assessing a country's cyber readiness. In addition, the Oxford Cybersecurity Capacity Maturity Model (CMM) sketches different levels of countries' cybersecurity maturity based on five pillars: (a) cybersecurity policy and strategy; (b) cyber culture and society; (c) cybersecurity, education, training and skills; (d) legal and regulatory frameworks; and (e) standards, organisations and technologies, and can be used toward diagnosing cyber preparedness. The e-Governance Academy in Estonia developed a multi-region National Cyber Security Index (NCSI) (Estonia's e-Governance Academy, 2019) which measures countries' readiness level on cybersecurity, and tracks down the major priorities that need to be addressed per country to prevent and fight against cyber attacks and crimes.

ENISA has published a report on risk assessment on cloud-computing business models and technologies, entitled 'Benefits, risks and recommendations for information security' (ENISA, 2009) in the context of the Emerging and Future Risk Framework project. Several other reports, also published in 2019, are worth mentioning. 'Good practices in innovation on cybersecurity under the National Cyber Security Strategies (NCSS)' addresses three aspects of innovation (ENISA, 2019f). 'Threat Landscape for 5G networks' focuses on the pertinent issue of 5G roll-out, and includes a threat taxonomy map and inter-relating risk scenarios to cyber threats (ENISA, 2019b). Further reports include 'EU Member States incident response development status report' (ENISA, 2019d), the 'ENISA good practices for security of Smart Cars' (ENISA, 2019a), 'Port Cybersecurity – Good practices for cybersecurity in the maritime sector' (ENISA, 2019g), and 'Good Practices for Security of IoT – Secure Software Development Life Cycle' (ENISA, 2019e). Finally, ENISA maintains an interactive map containing the NCSS per EU Member State along with their guidelines on implementation and information sharing (ENISA, 2020b).

> The more our world goes digital, *the more its attack surface increases.*

In 2013, Europol set up the European Cybercrime Centre (EC3) to strengthen the law enforcement response to cybercrime in the EU and thus to help protect European citizens, businesses and governments from online crime. EC3 has been involved in tens of high-profile operations and hundreds of on-the-spot operational-support deployments resulting in hundreds of arrests, and has analysed hundreds of thousands of files, the vast majority of which have proven to be malicious.

Each year, EC3 publishes the Internet Organised Crime Threat Assessment (IOCTA), its flagship strategic report on key findings and emerging threats and developments in cybercrime. The IOCTA demonstrates the wide and varied nature of cybercrime.

2.3.3 The international landscape

This section covers approaches to cybersecurity in the United States (US), China, Russia, Australia and relevant international organisations. In particular, since 2017, a number of regulations have been passed.

The US 2018 National Cyber Strategy (US Government, 2018) adopts a more assertive position compared to its 2015 predecessor, reflecting the growth in cyber threats. These include the Russian campaign against the 2016 US election, the proliferation of ransomware attacks on critical infrastructure, and the mass exploitation of US intellectual property. It is closely aligned with the US Department of Defense (DoD) 2018 Cyber Strategy (US Department of Defense, 2018) which marks out the military's role in relation to cyberspace and also adopts a much more aggressive stance. One of the key concepts within this strategy is that of 'defending forward' with the mission to 'disrupt or halt malicious cyber activity at its source, including activity that falls below the level of armed conflict'.

Since 2014, the National Institute of Standards and Technology (NIST) has published a number of guidance documents related to cybersecurity (Matthew P. Barrett, 2018). In 2018, NIST updated its special publication on 'Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy' (Ronald S. Ross, 2018). This voluntary framework includes standards, guidelines and best practices to manage cybersecurity risk.

China, on the other hand, has followed a similar approach to the EU by embedding elements of the NIS Directive into its 2017 national cybersecurity law (Asiapedia, 2019). This law

makes explicit the responsibilities of relevant government agencies, internet service providers, and end-users. Relevant organisations, which include any network or service provider and, in particular, any critical information infrastructure operator that would endanger national security if compromised, must establish stringent technical or other necessary measures. For example, these may include establishing a specialised security management body, carrying out disaster recovery back-ups, etc. to ensure the internet is safe and available, dealing with cybersecurity incidents adequately, deterring and preventing cyber criminal activities, and preserving the integrity, secrecy and usability of internet data.

In 2017, Russia adopted Federal law No. 187-FZ addressing the security of critical information infrastructures. Under this law, facilities must enforce sufficient protection measures and register with the Federal Service for Technical and Export Control (FSTEK). To cope with the risks related to the illicit use and potential abuse of information systems, any software produced abroad, especially that related to ICT security, like firewalls, antivirus applications, or any software using encryption, is subject to review by certified Russian agencies. This means that before a piece of software is imported and sold in Russia, its source code may be examined to ensure it is backdoor-free.

In addition, the 2019 Federal law No. 90-FZ provides the basis for isolating the Russian segment of the internet from the rest of the WWW – allegedly with the use of a parallel 'national DNS infrastructure' – therefore the so-called 'Runet' will still remain operational in the advent of a foreign cyber attack. As regards this latter point, the debate about 'sovereignty in cyberspace' is ongoing and at its core is the problem of misalignment. A key question arises here in relation to whether sovereignty in cyberspace can exist hand in hand with globalised connectivity, and whether national borders in cyberspace will eventually lower risks and strengthen security and order.

In 2020, the Australian Cyber Security Centre published the 'Australian Government Information Security Manual' (Australian Cyber Security Centre, 2020). It provides strategic guidance and a cybersecurity framework 'that organisations can apply, using their risk management framework, to protect their information and systems from cyber threats'. It offers cybersecurity principles grouped into key activities, namely: govern, protect, detect and respond. In addition, the Australian Government has developed a 'Protective Security Policy Framework' (Australian Government, 2020) with the aim of helping 'entities to protect their people, information and assets, at home and overseas'.

As regards international measures, these have come mainly from the International Telecommunications Union (ITU) and the World Economic Forum (WEF). The ITU has developed the National Cybersecurity Guide and a Global Cybersecurity Index to help countries to evaluate their cybersecurity strategies and programmes against those implemented by other countries. In the same context, in 2018, the WEF published its Cyber Resilience Playbook for Public-Private Collaboration (WEF, 2018). Its goal is to steer public-private collaboration in cybersecurity policy development. It also highlights the need for a clear national cyber governance framework, including unambiguous roles and responsibilities.

SUMMARY

Research activities represent a solid indicator of the growth and maturity of a given field. In this chapter, we analyse EU cybersecurity research-related activities and compare them with other countries on a global scale. We examine publications, patents, and the collaboration between public and private organisations in order to compile our observations, whilst also looking into more specific cybersecurity domains. From the results, it appears that even if the EU is one of the strong players in cybersecurity research, when looking at the national level, the more influential institutions are concentrated in only a few Member States. In order to further improve the situation in the EU, greater collaboration and cooperation are needed at both the national and international level.

EUROPEAN RESEARCH IN CYBERSECURITY

Research and development are primary indicators of the liveliness and competitiveness of a sector and its capacity to stay abreast of a given field. This chapter gives an indication of the cybersecurity research landscape across the EU and draws on a large mapping exercise conducted by the JRC. Results from participation in H2020 projects, scientific publications and patents are also described.

3.1. Mapping the cybersecurity research landscape

As seen above, the Commission intends to create a network of cybersecurity competence centres across the EU to stimulate the development and deployment of technology in cybersecurity. In support of this initiative, the JRC undertook a comprehensive exercise to plot existing European centres, typically university departments or research centres. The data collected provides a screenshot of the landscape, which is described in more detail below and will be covered more fully in the forthcoming publication of a dedicated 'Cybersecurity Atlas'. Some 725 organisations participated in this exercise, a summary of which is provided below. The mapping covers all the EU Member States plus additional countries participating in the Horizon 2020 research programme (H2020), as seen in *Figure 3.*

> Although cybersecurity research in the EU is both robust and dynamic, there is room for better collaboration and coordination.

Figure 4, which summarises the clustering per country, shows that the majority of research activities are mainly performed by higher education organisations (universities). *Figure 5* shows the distribution per country and per type of 'legal status' of the research institutions (public, private or public-private partnerships). It is interesting to note that, with a few exceptions, there is a certain balance between public and private organisations. Furthermore, despite being a relatively new instrument, public-private partnerships on cybersecurity research exist in the majority of European countries.

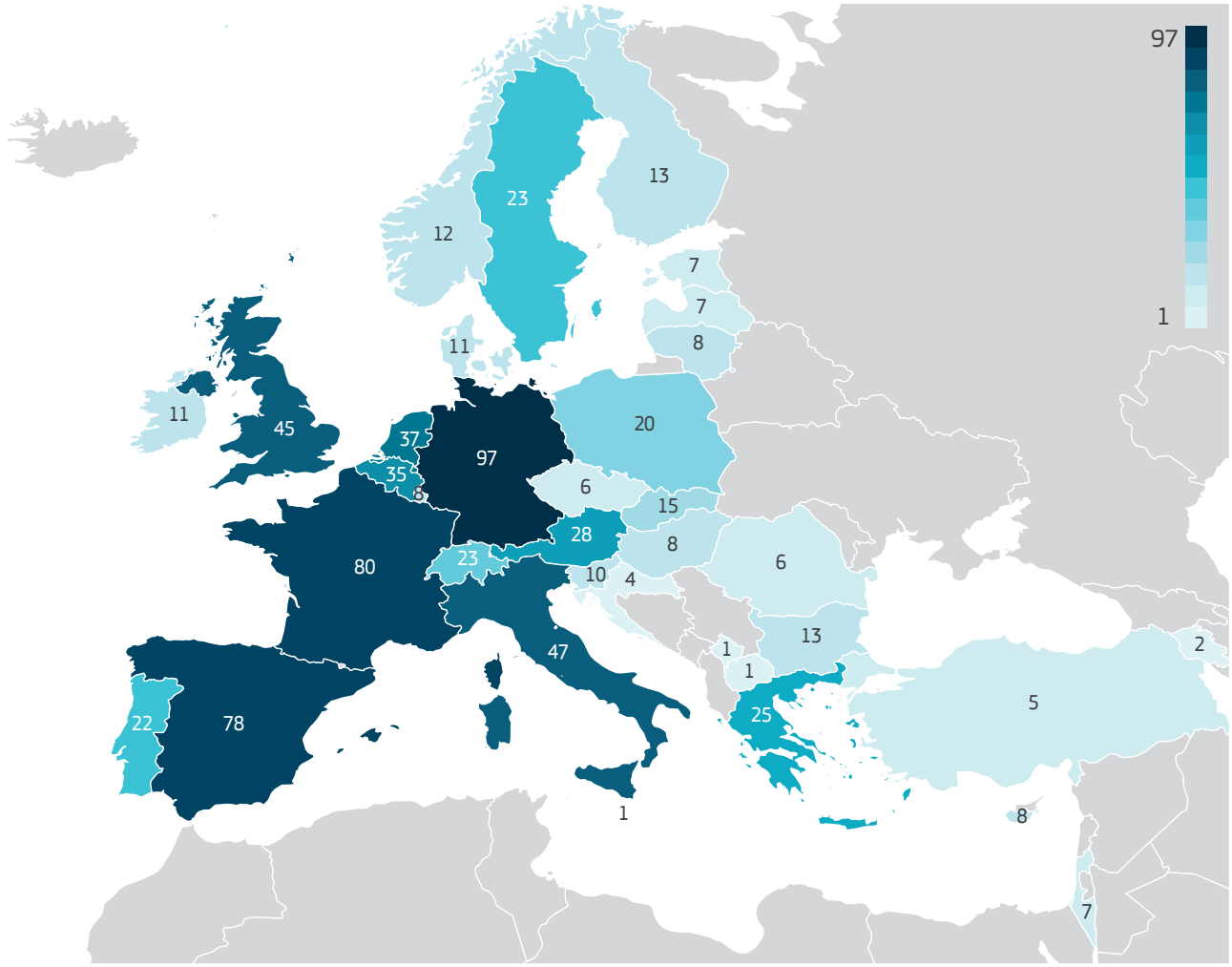


Figure 3: Mapping coverage

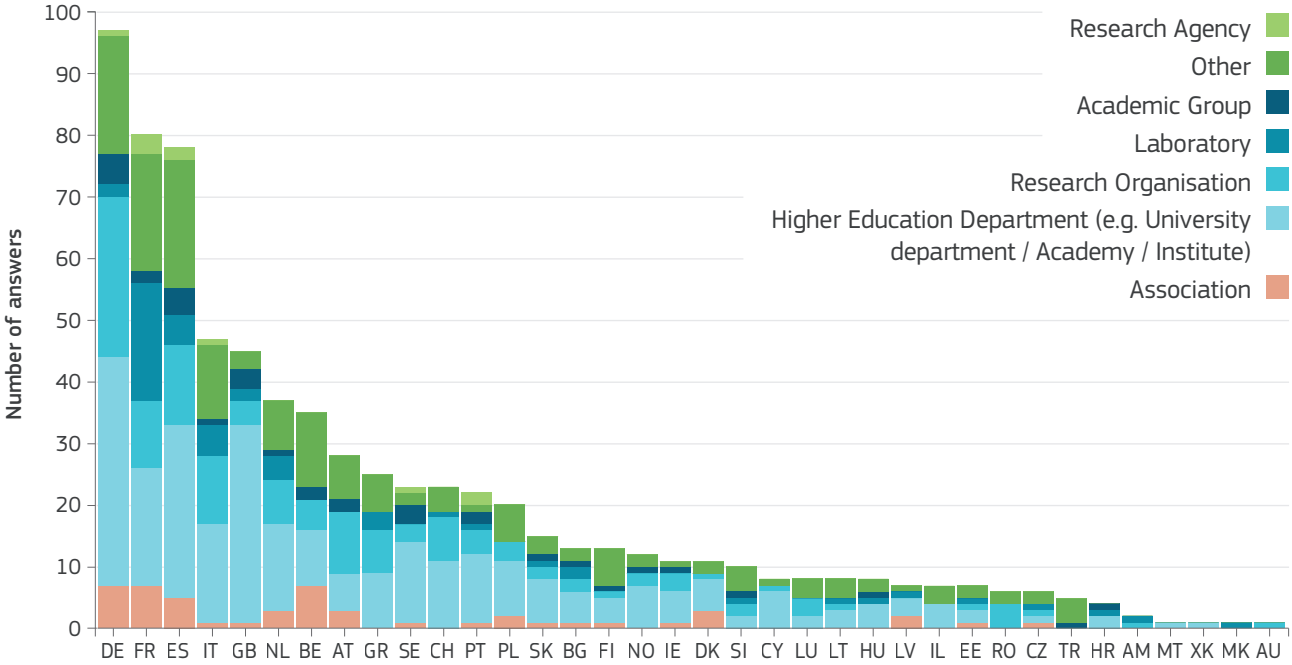


Figure 4: Clustering per type of institution

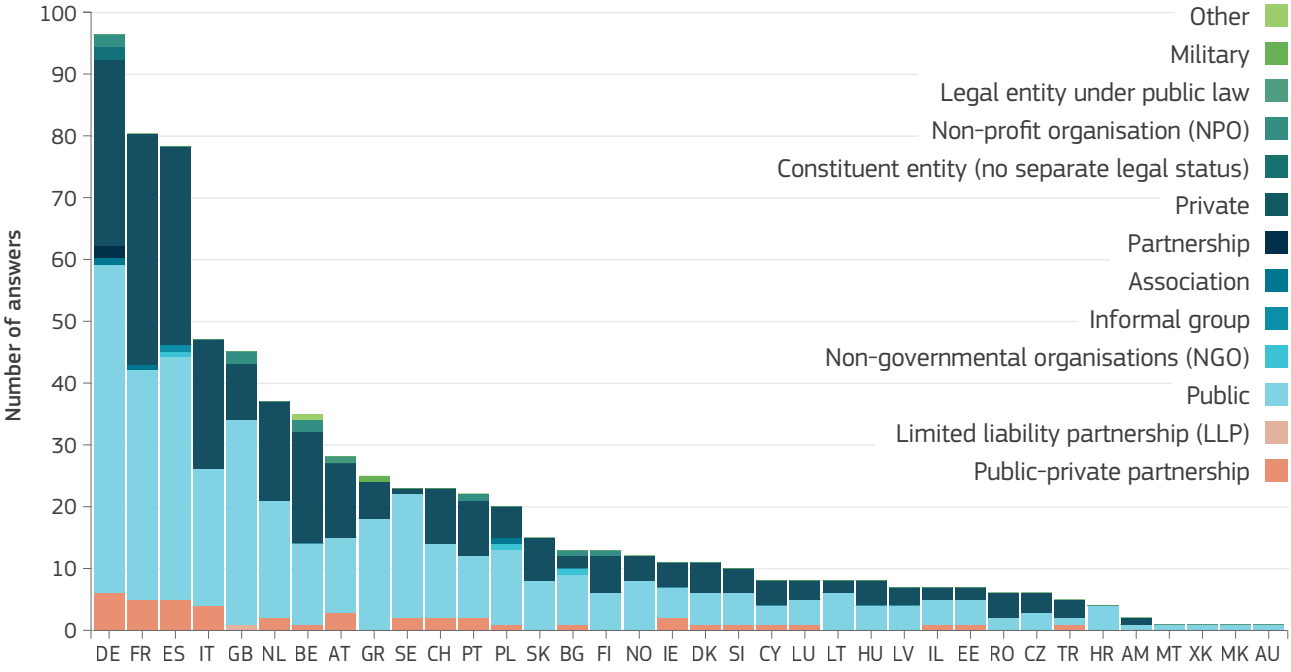


Figure 5: Legal status

3.2 Cybersecurity research domain mapping

While all research domains are covered, a deeper analysis shows that there are several sub-domains, such as post-quantum cryptography, which are poorly investigated. Similarly, the initial data show that 50 institutions claim to cover all cybersecurity domains, with 200 claiming to cover at least 75 % of the domains. While this appears positive in terms of geographical coverage, further analysis of the scientific literature and participation levels in H2020 cybersecurity-related projects reveals that a few research institutions dominate the field. The most plausible reasons for this are the dispersion of resources and the lack of overall coordination and collaboration.

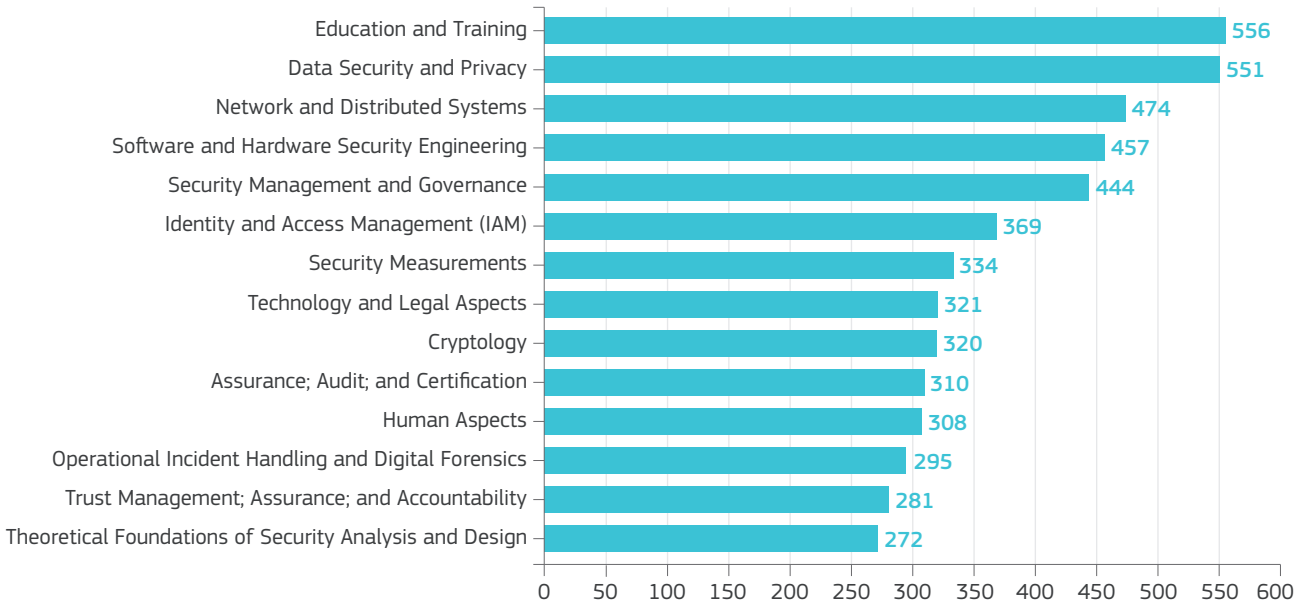


Figure 6: Domain coverage

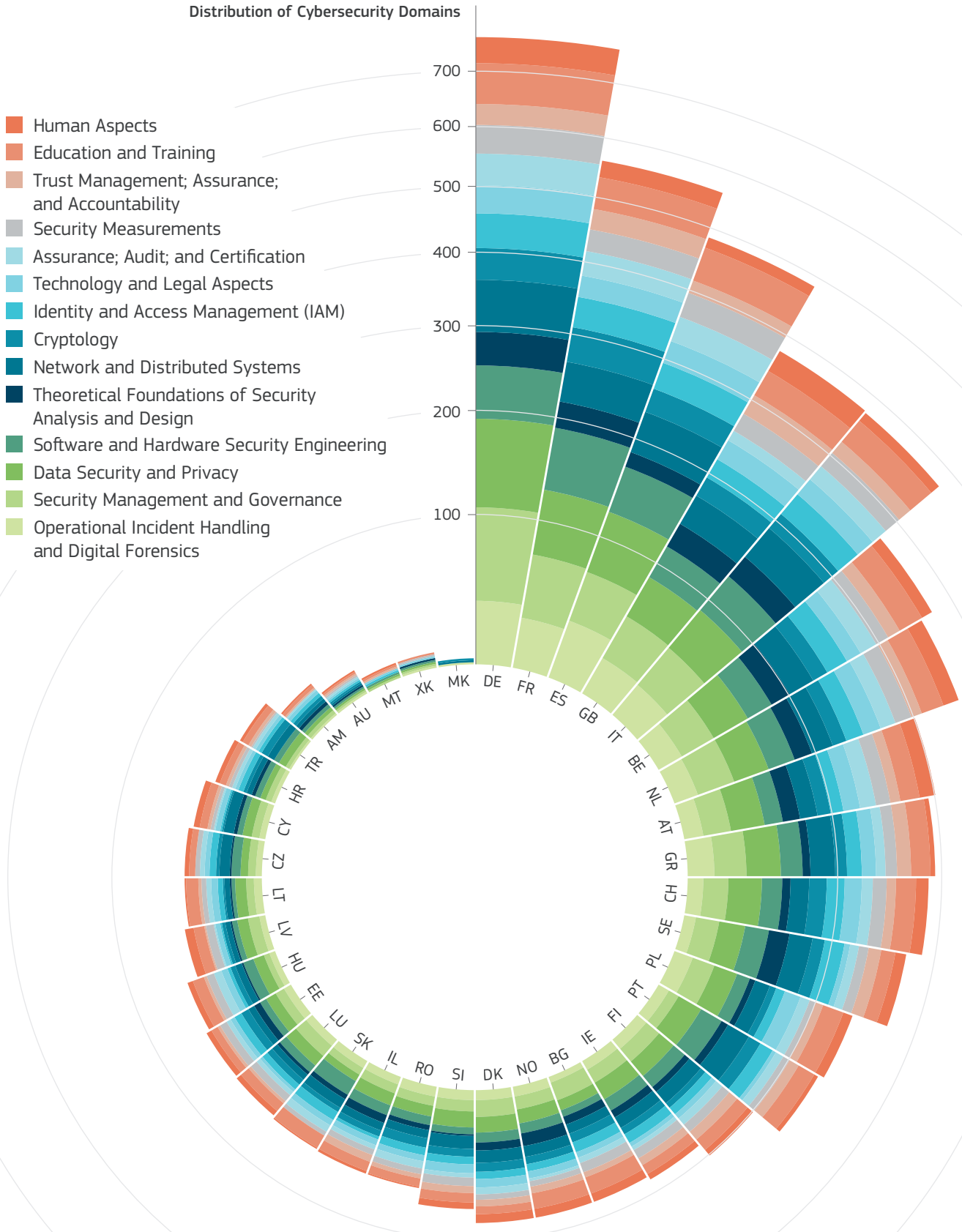


Figure 7: Domain coverage per country

Analysis of the sectors covered by the research centres further validates this reasoning. It is evident, for example, that the sectors and applications where costly facilities are needed to perform cybersecurity research, in fields such as energy, space and defence, are well covered only by those countries which traditionally have more resources available to invest in big facilities or where there is a strong industrial player in the specific sector.

This is confirmed by analysing the field of applications *(Figure 10)* where those that require more investment, such as high-performance computing, AI and quantum, are well covered only in those countries which traditionally can afford to invest in such areas.

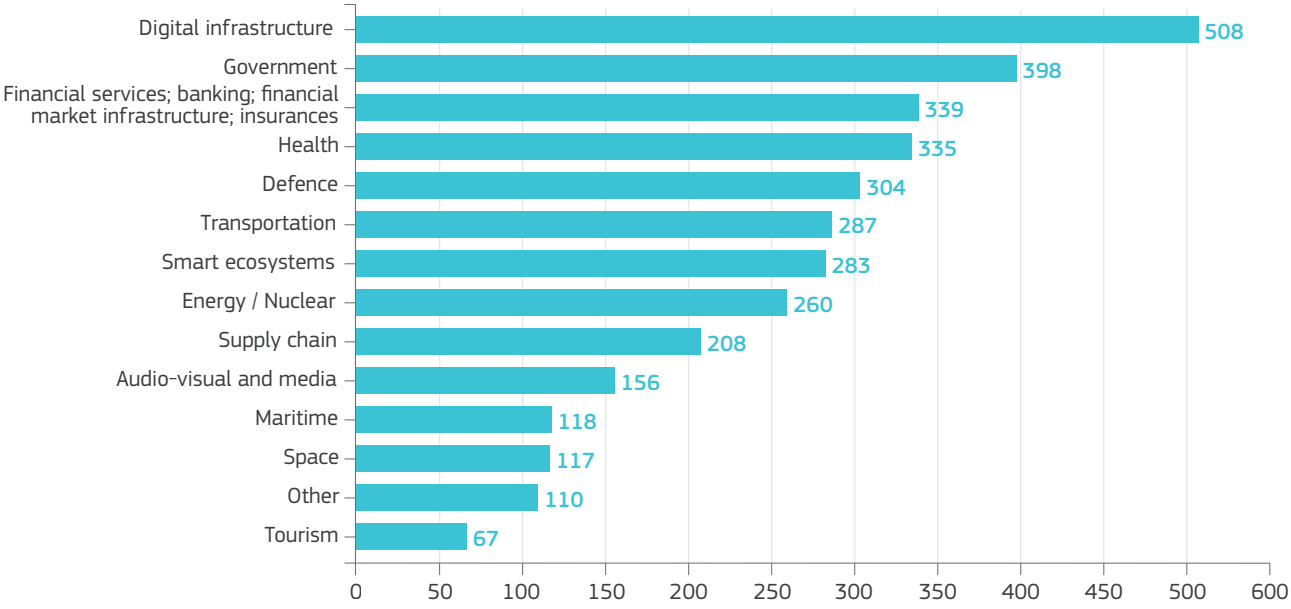


Figure 8: Sector coverage

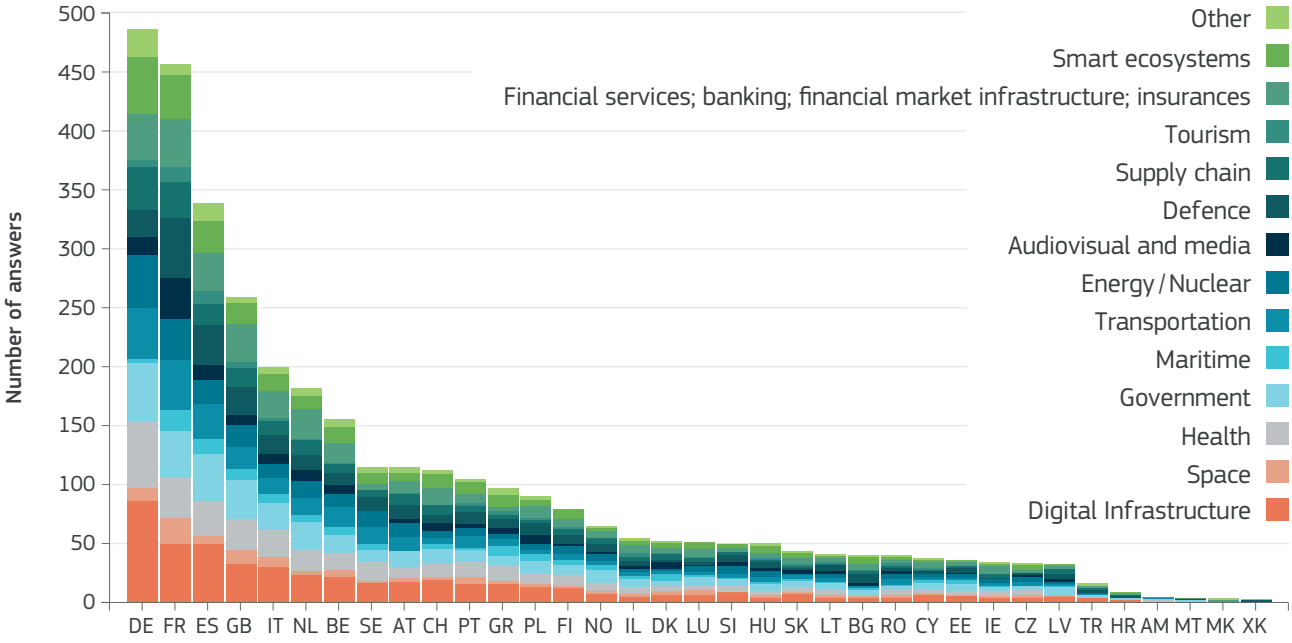


Figure 9: Sector coverage by country

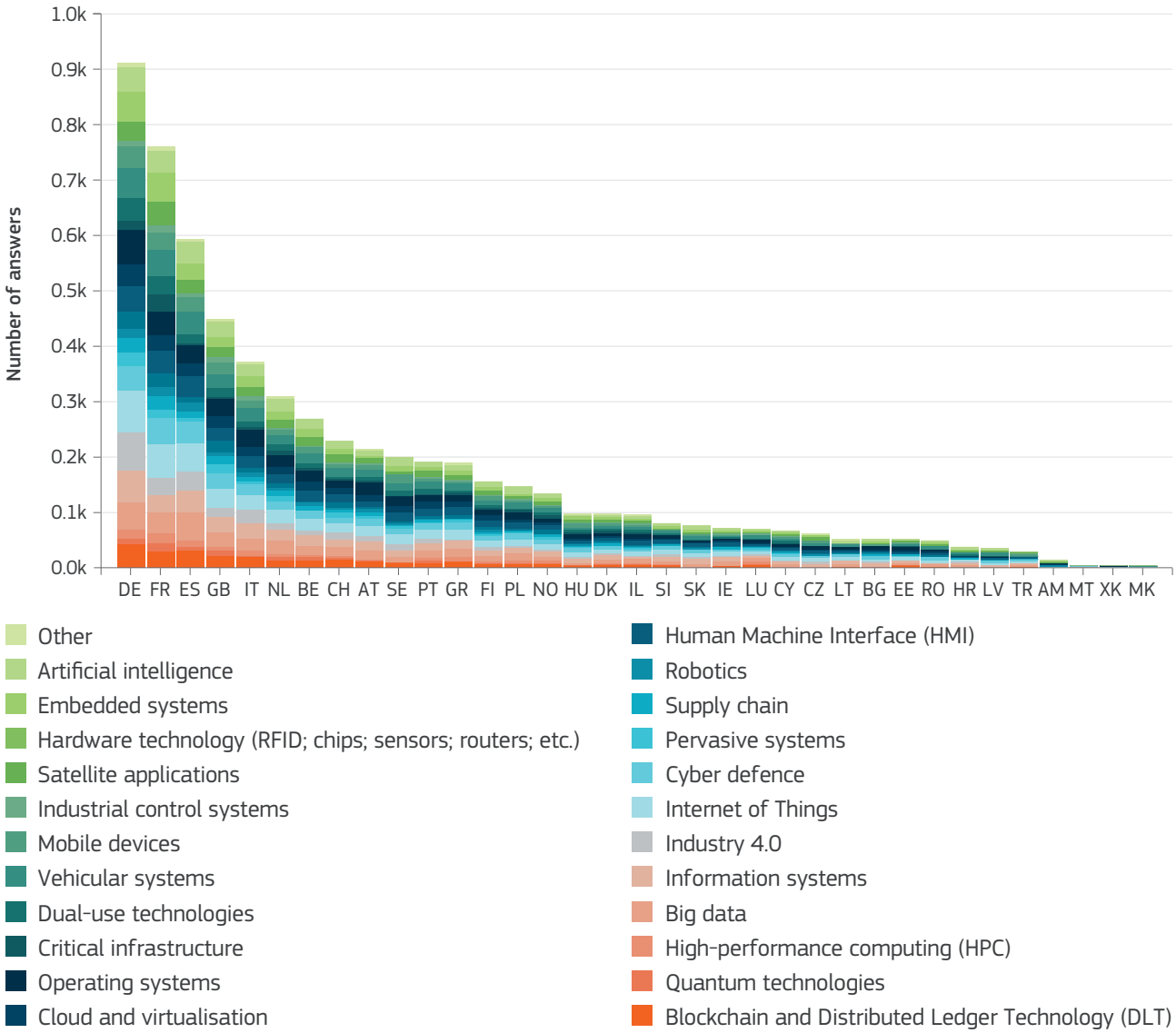


Figure 10: Fields of application

3.3 Scientific and technological development analysis

The number of publications, participation in H2020 projects and analysis of patents also help to build a picture of scientific and technological development in this domain.

3.3.1 Analysis of publications

Analysis of the cybersecurity scientific literature indicates that the USA leads scientific research in cybersecurity with half the number of publications. The EU is in second place with a quarter of the total number of publications, while the remaining quarter aggregates the scientific production of all the remaining non-EU countries (dominated by China, Canada and Japan), as shown in *Figure 11.*

The majority of publications are concentrated in the following domains:

- Security management,
- Network security,
- Data security and privacy,
- Cryptology.

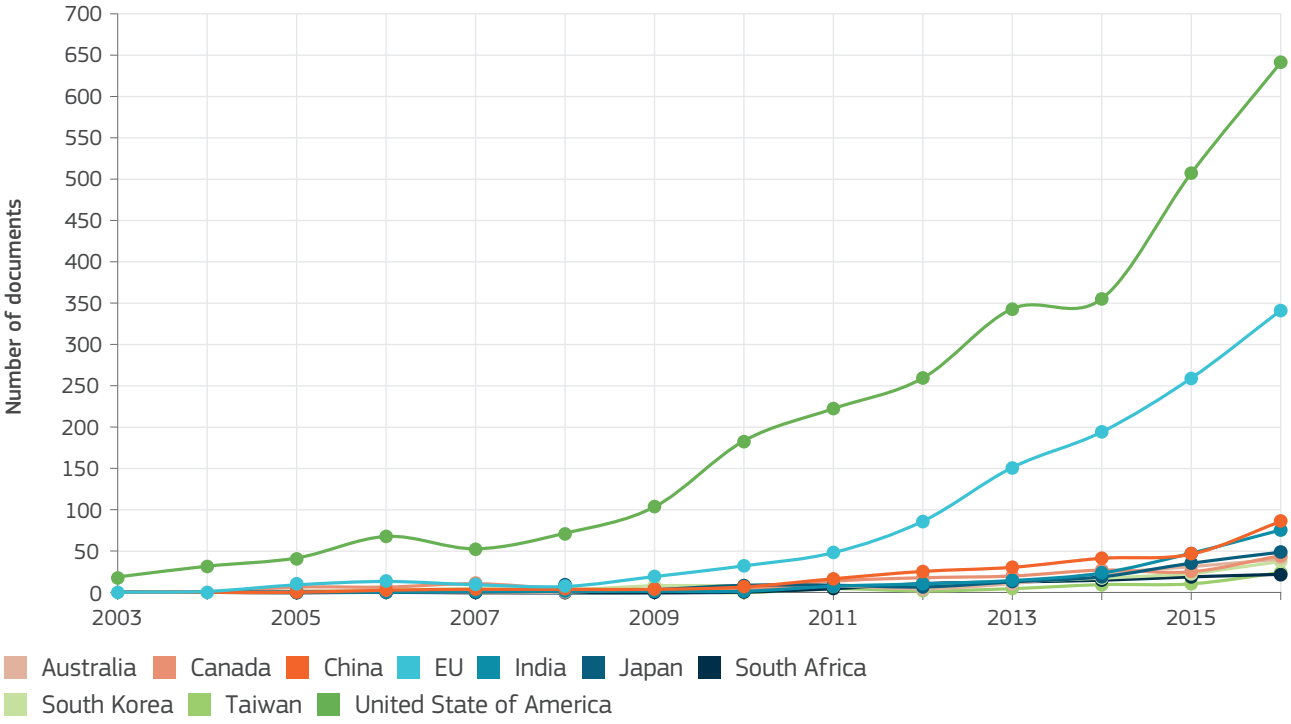


Figure 11: Scientific publications in cybersecurity per country

It is interesting to note that these domains match the domain ranking which emerged from the analysis of the surveys.

> "The USA is the EU's strongest partner *regarding the overall scientific production in cybersecurity, followed by Switzerland and Israel.*"

As regards this analysis, it is important to underline how the preliminary analysis was quantitative, i.e. the relevance of a publication was not weighted (a publication for a conference was counted as a publication in an international journal). Moreover, even if the four domains mentioned above dominate the others in terms of scientific production, the results are underdeveloped in several of their sub-domains. One example is in the field of cryptology which ranks fourth in terms of the total number of papers published but where there is limited publication in the post-quantum sub-domain. This is also confirmed by the results of the mapping.

An analysis of the collaboration networks *(see Figure 12)* shows how the USA is the EU's strongest partner as regards its overall scientific production in cybersecurity, followed by Switzerland and Israel.

Distribution of the scientific production among European institutions reveals an anomaly with respect to the survey results. While more than

> In Europe, a few institutions polarise scientific production *and can aggregate critical mass, enabling them to be influential in the domain.*

200 institutions claim to cover at least three quarters of the cybersecurity research domains, an analysis of the scientific literature by domain shows that each domain is dominated by a limited number of institutions in terms of the number of publications. Furthermore, the numerical difference between the top 10 in each domain and the rest of the institutions publishing in that domain is not negligible. In other words, the picture obtained from the analysis of scientific publications combined with the results provided by the survey shows a Europe where scientific production is polarised in a few institutions which are able to make a difference in the domain.

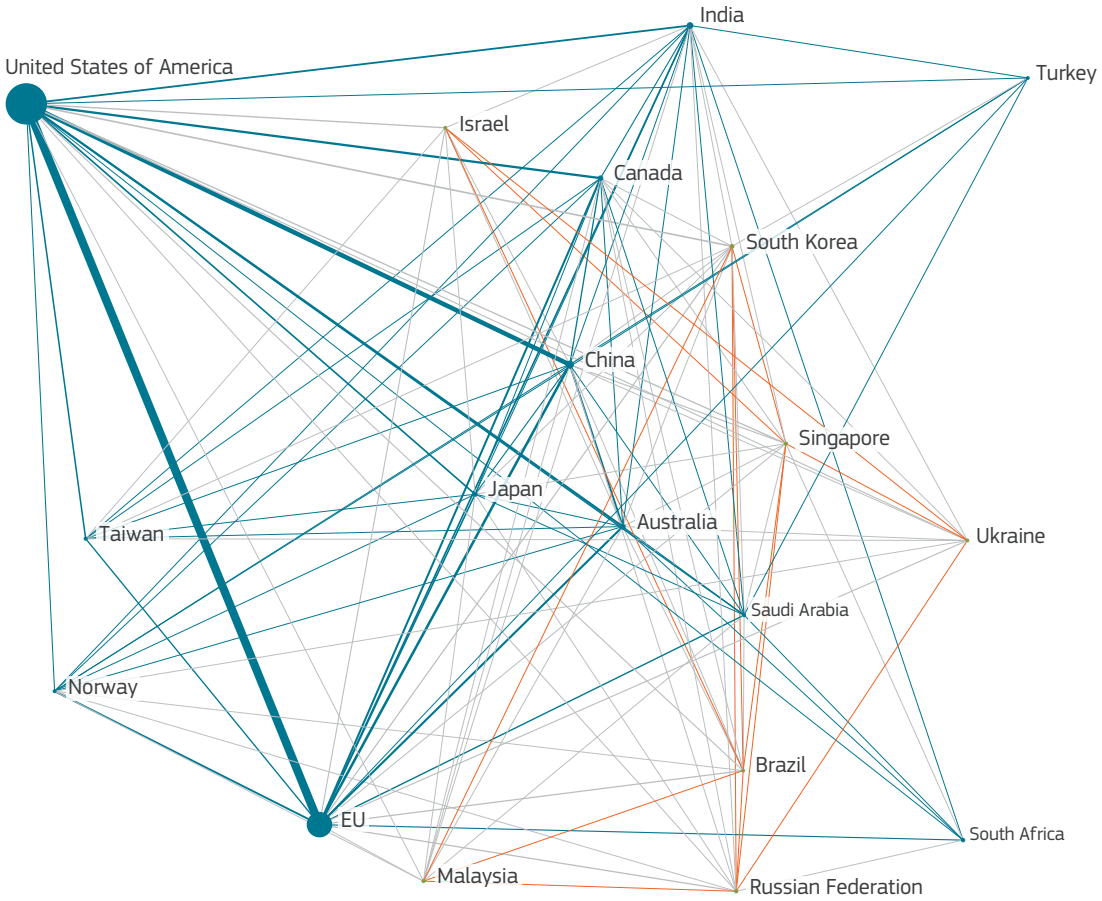


Figure 12: Size of node = country share of scientific publications in cybersecurity (size of nodes = number of projects, edge between nodes = project(s) in common, colours identify communities of countries collaborating more often)

3.3.2 Horizon 2020 projects

This picture of a polarised Europe is confirmed to some extent by analysing the participation in cybersecurity H2020 projects, where this polarisation around a limited number of academic institutions is even more evident *(Figure 13)*.

It is worth noting that when considering the participation of private companies in H2020 cybersecurity-related projects, the weight of the different countries is quite similar.

On a qualitative note, a number of pilot research projects funded through H2020, including CONCORDIA, ECHO, SPARTA and CyberSec4Europe, are intended to advance and boost the EU's cybersecurity capacity and address forthcoming challenges towards a safer European digital single market. Last but not least, some other H2020-funded projects, such as EUNITY which focuses on improving the cybersecurity and privacy dialogue between Europe and Japan, are aimed at fuelling and ultimately developing the dialogue between Europe and third countries on cybersecurity and privacy research.

Figure 13: Participants in H2020 cybersecurity-related projects (academic partners)

3.3.3 Patent analysis

Figure 14 gives a picture of patents in the cybersecurity sector where patent filing is dominated by China, followed by the USA, while the EU does not have a prominent position.

A more-detailed analysis shows that, on average, the number of patents filed by a European entity on cybersecurity is around 5 %, with the exception of cryptology (21 %).

As regards the ratio between scientific publications and patents, it seems evident that the relatively high scientific production does not automatically correspond with to an equal 'innovation' push. Several reasons might explain this phenomenon:

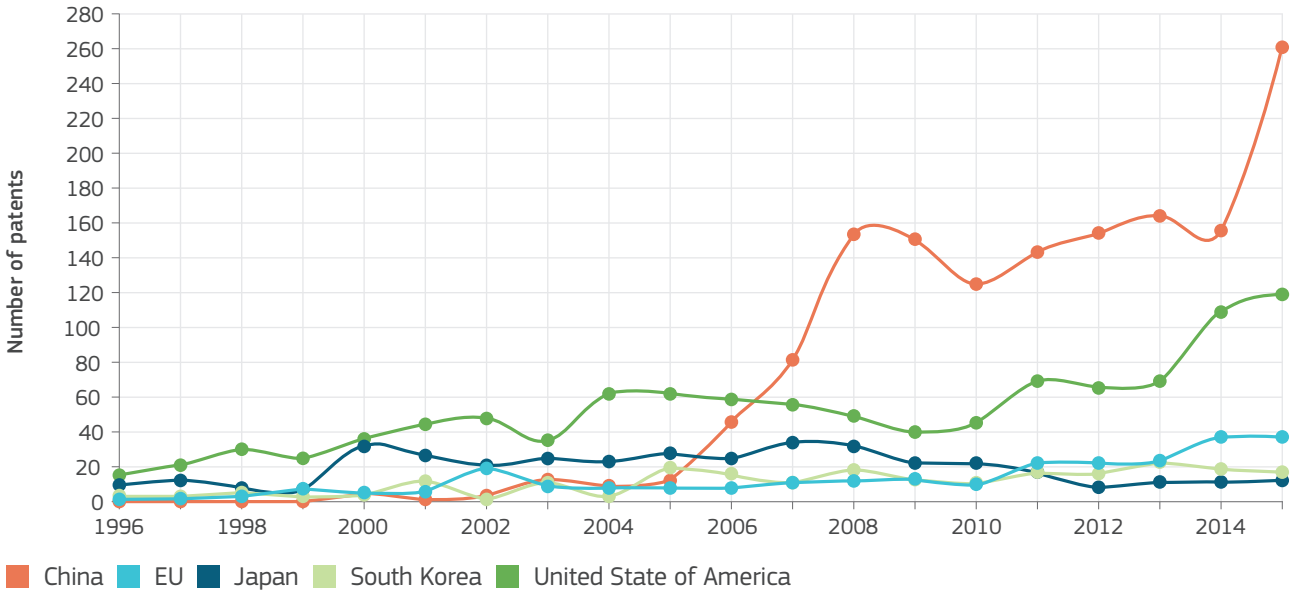


Figure 14: Patents in cybersecurity per country

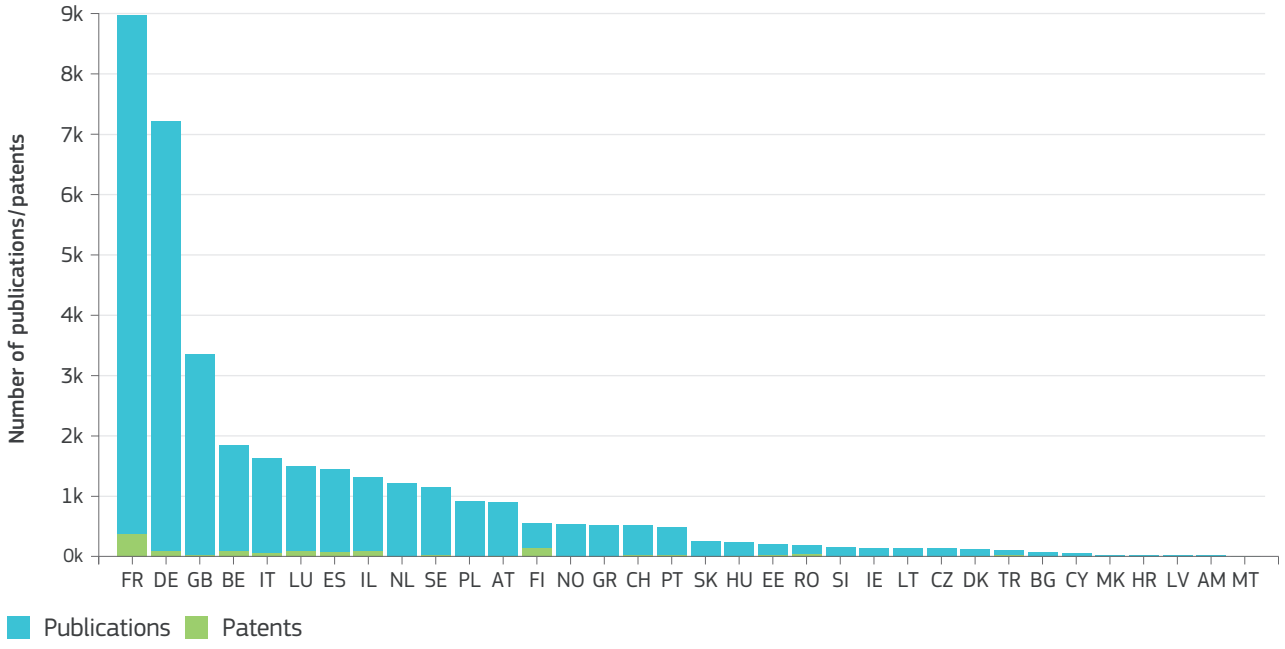


Figure 15: Cybersecurity publications/patent ratio per country

- Patent filing is a costly and complex process.
- Collaboration between industry and academia is limited, or 'consultancy oriented' (i.e. one-shot collaborations without a multi-annual collaboration and development plan).
- The patent analysis is unable to completely capture the innovation chain.

The last point is certainly true for ICT and cybersecurity as patent analysis does not allow the capture, for example, of the phenomenon of software development and licensing for which, unfortunately, it is not easy to provide a projection. However, even considering the fact that a relevant element of the picture is missing, it is still true that other countries patent much more in cybersecurity than Europe.

3.4 European cybersecurity research ecosystem

The analyses of the mapping results and the desktop research provide a complex picture of the situation of cybersecurity research in Europe. Along with the USA, the EU is one of the two main actors in cybersecurity scientific production.

While there is complete coverage of the research domains at EU level, it is noticeable that scientific results in some relevant sub-domains are limited. At country level, all Member States have cybersecurity capabilities covering the majority of research domains. However, their capacity to impact on the scientific and technological production is heterogeneous, with the more-influential institutions concentrated in a few Member States. The same trend is confirmed when looking at the sectors and fields of application covered, with those requiring the availability of costly facilities only explored in-depth by a limited number of institutions in a few countries.

As regards the collaboration between industry and academia, the H2020 programme has contributed to strengthening relations between the two. However, not all the institutions proved to be equally capable of successfully and continuously accessing H2020 funds.

An analysis of patents in the field indicates low European interest in patenting cybersecurity solutions. This could be seen as a weakness in the collaboration between industry and academy, although it is also true that patents cover only one aspect of the cybersecurity value chain with software licensing occupying the other half. China's dominance in patenting could be linked to its pursuit of cybersecurity sovereignty. Unfortunately, no data are available to estimate the size and 'value' of the licensing phenomenon.

The overall picture provided by this analysis is positive as the European cybersecurity research landscape is vibrant, productive and recognised at the global level. However, it could be improved by:

- Strengthening and enlarging the collaboration of cybersecurity research organisations across Member States.
- Streamlining and stabilising the R&D cooperation between industry and academia.
- Better coordinating research funding across the EU.
- Co-designing research plans between funding bodies and recipients.
- Supporting the sharing of highly expensive infrastructures (in an Open Laboratory Initiative approach).

The Commission's proposal to set up a European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres (COM(2018)630) is moving directly in this direction, aiming to create a more collaborative and synergetic European cybersecurity competence ecosystem.

SUMMARY

The vulnerabilities of IoT devices and big data are the new frontier for cyber attacks while, at the same time, providing the main sources of information, insights and analytics that can be used to detect cybersecurity threats. Furthermore, vulnerabilities and threats in mobile applications, which are often written by hobbyists, might put citizens' lives in danger. At a different level, although network availability is taken for granted, realistically, the absence of connectivity in interdependent networks may occur and create an immediate impact in terms of our society's safety. On a different scale and level of maturity, AI, blockchain and quantum technologies can be turning points in cybersecurity.

CYBERSECURITY AT THE HEART OF DIGITAL TECHNOLOGICAL DEVELOPMENT

The previous section presented societal aspects in the interplay of cybersecurity and digital transformation. The scope of this section will illustrate the emerging technical challenges that cybersecurity has to overcome.

4.1. Big data

Worldwide, citizens, public administrations and private companies generate and store a vast volume of data every day. A driving factor is certainly greater internet connectivity, illustrated by the following 2019 statistics:

- Today, there are more than 1 billion websites (Netcraft, 2020), targeted by over 6 billion Google queries each day (Internet Live Stats, 2020).
- In 2018, there were over 2.3 billion Facebook (Facebook, 2019) and 321 million Twitter (Twitter Investor Relations, 2019) active users.
- Every day, around 4 billion videos are viewed on YouTube (MerchDope, 2020), and 95 million photos and videos are shared on Instagram (Instagram, 2020).

> The consequences of malicious attacks on cyber physical systems could have severe impact on human lives and the environment.

In the digital transformation age, the internet went through its second (r)evolution by connecting 'everything', known as the 'Internet of Everything' (IoE). It is estimated that, by 2025, each connected person will have at least one data interaction every 18 seconds (Reinsel, Gantz and Rydning, 2018). Many of these interactions are triggered

by IoT devices that will increasingly enable digital technologies to embed themselves in all aspects of our economy and society.

The scenario magnifies some key issues to which cybersecurity needs to find the appropriate answers:

- The big-data paradigm relies on the quality of the collected data to extrapolate new results, evidence and services. The injection of fake data is now the new frontier of cyber attacks. In the big-data era, cybersecurity must provide a means to guarantee the provenance and integrity of information used by big-data applications.

- IoT and wearables are increasing our vulnerability 24 hours a day to cyber threats. Even worse, instead of following a life-cycle approach whereby amendments are done over time to strengthen security, a plethora of these 'things' are deployed in a 'set and forget' fashion.

- The exponential growth of the number of potential targets reachable online increases the complexity of cyber threats and attacks detection.

> "In the digital transformation age, the internet has undergone *a second (r)evolution to connect 'everything' – the 'Internet of Everything'.*"

Reflection is needed on how to tailor cybersecurity approaches and solutions to cover the need for security in the big-data context, to streamline cybersecurity mechanisms at IoT level, and to leverage AI to enable a more accurate and distributed monitoring of cybersecurity across all elements of the big-data value chain.

4.2. Cybersecurity and hyperconnectivity

The big-data paradigm implies a high availability of connectivity: many connected devices require the transmission of huge amounts of data in the cloud to be stored and/or processed. The advent of the 5G-based services network will dramatically increase this demand in the coming years – in particular for real-time processing services. The bandwidth, low latency and ubiquity of 5G will not only boost the hyperconnectivity of connected devices but will also enable new use cases, such as remote real-time surgery, smarter and self-driving vehicles, drone control and a higher degree of industry automation.

Critical applications using connected devices (for example, in sectors like health, energy or automotive) will depend on the reliability of communication networks. Today's digital services are developed in a 'composition fashion' whereby different components are deployed in geographically sparse systems and put together thanks to the availability of hyperconnectivity.

In a sense, the problem is that network availability is taken for granted today. However, in reality, recent episodes show that attacks against what can currently be considered as the cornerstone of the digital revolution are feasible, and their impact can be immense in terms of the safety of our society.

The challenge here is that the internet backbone does not have centralised governance, which means

> Critical applications using distributed connected devices *will depend on the reliability of communication networks.*

its security cannot be enforced homogeneously. Furthermore, this existing trend in greater dependency on internet connectivity in all kinds of services and products is leading to unforeseen impacts due to the complex interdependencies created among heterogeneous digital services. A cybersecurity attack that results in the unavailability of a certain cloud service can initiate a cascading effect with adverse consequences for those systems that depend on it.

4.3. Cybersecurity, mobile devices and the IoT

In an effort to reduce network congestion, low-level latency and lower the dependence on continuous connectivity, novel data-computing architectures were introduced, of note, edge and fog computing *(see Figure 16).* Edge computing attempts to perform data processing/filtering on the device close to the sensor (the edge) whereas fog computing processes data in intermediate nodes within the local network itself.

Mobile devices are good examples of the edge-computing paradigm as they currently have sufficient computational power to perform a plethora of tasks locally, while IoT, together with mobile devices and gateways, could be seen as the key interface between fog computing and the real world.

Despite being conceived for completely different reasons, both IoT and mobile devices are expected to have a huge impact on the way cybersecurity is delivered. Smartphones have now reached the majority of the global population (Internet World Stats, 2017) and mobile internet traffic today exceeds landline traffic (Cimpanu, 2016) as shown in *Figure 17.*

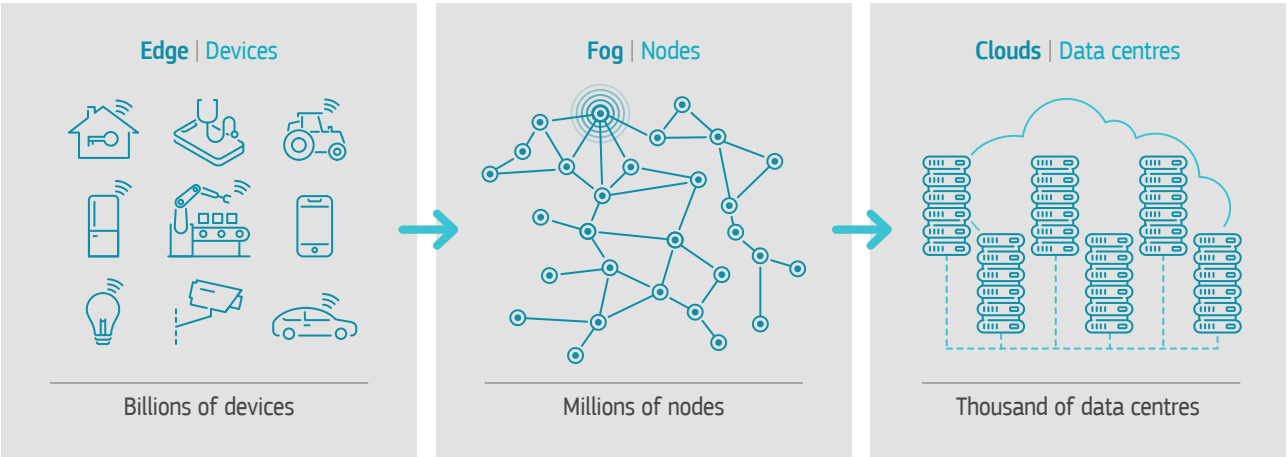


Figure 16: The continuous space of cloud computing

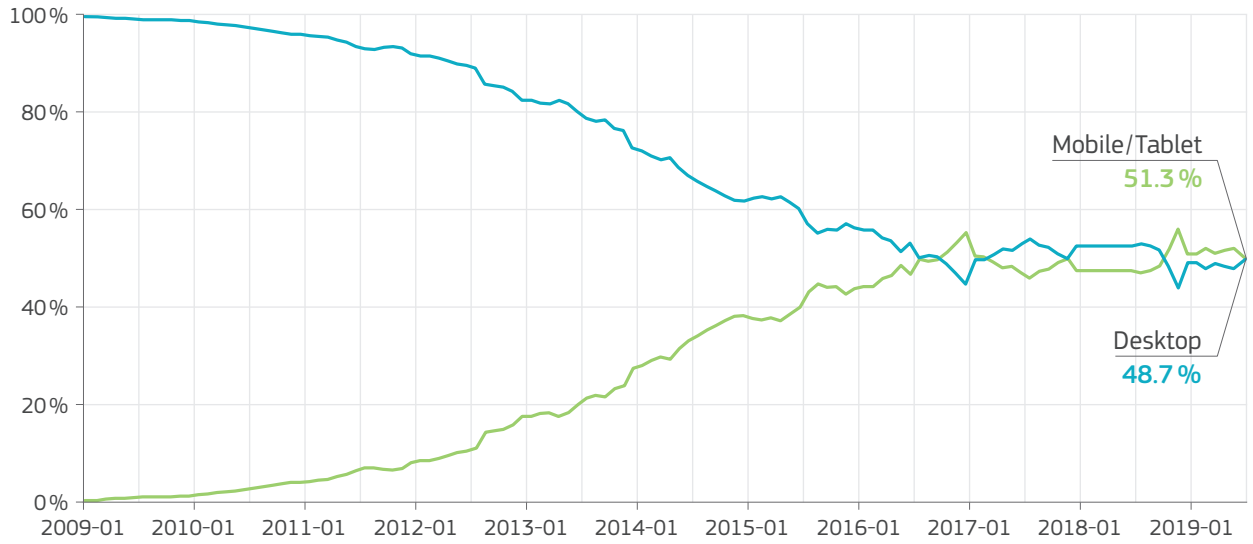


Figure 17: Internet usage worldwide for the period 2009-2018 (StatCounter, 2020)

> In 2018, there were 17 billion connected devices, *7 billion of which were IoT devices.*

In 2018, there were 17 billion connected devices, 7 billion of which were IoT devices (Knud Lasse Lueth, 2018). This number is expected to grow to more than 13 billion in 2022, thereby overtaking the number of non-IoT connected devices worldwide. Similar predictions are also reported by Gartner (Omale, 2018), with an estimated 25 billion connected things by 2021.

Many IoT and mobile app vulnerabilities are rooted in their design, implementation, and deployment. For example, in several cases, mobile apps are written by hobbyists or by professionals without any cybersecurity background and awareness. The same can also be said about the average IoT device, which is quite often designed with only the target functionality to be provided in mind, and with a limited budget (IoT and apps must be cheap to take off in the market), hence without any attention to cybersecurity issues.

This lack or deficiency of proper cybersecurity mechanisms in IoT devices could have direct safety implications for the citizen. Medical devices and applications, smart-house automation systems, and connected cars are just a few items which, if hacked, could endanger life (see the follow *Box 1* for an example).

Their criticality, the completely distributed nature of such devices, the inability to make assumptions on the environment surrounding them, and the impossibility of attributing a guaranteed level of trust is currently forcing cybersecurity to switch from a centralised *segregate and defend approach* to a *collaborative and distributed device by device defence.* This means that each element of the technology value chain must be conceived with embedded cybersecurity principles, including the entire life cycle, from its design to its governance.

BOX 1. Cybersecurity challenges for connected medical devices

The future of healthcare will revolve around big data and smart medical devices which are increasingly connected to the internet, thereby making cybersecurity imperative. Science, IoT, AI, and data will contribute to the detection of disease much earlier and enable disease prevention and personalised treatment. Such innovation may be called IoMT, which stands for the **Internet of Medical Things.** New actors, such as 'remote healthcare services', are already emerging across the entire 'healthcare supply chain', and the overall trend will be characterised by a shift from 'hospital care' towards 'home care', as illustrated in *Figure 18* below.

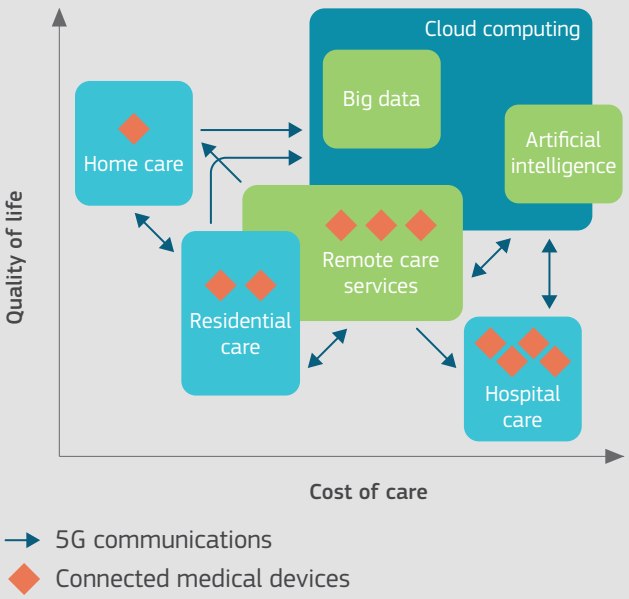


Figure 18: Cost of care – connected healthcare provision model based on connected medical devices; adapted from (Landers et al., 2016)

People will be equipped with smart devices continuously monitoring key health data, such as heart rate, blood pressure, electromyography, electrocardiogram, nasal airflow, glucose levels, weight, activity levels, etc. The data in the IoMT era will be transmitted around the clock to remote care centres, where algorithms will process them to detect early signs of disease. Depending on the diagnostic results, remote consultation with specialist physicians or physical visits may be arranged.

This new era of 'connected healthcare' is based on several novel technological developments, including 5G networks, big data, AI, cloud computing, and augmented reality, among others. Each one of these developments offers operational performance benefits and risks, most notably in the cybersecurity domain. In addition, the so-called 'legacy health systems' should be considered from the point of view of emerging cybersecurity risks.

At the EU scale, medical devices are regulated by Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017. Known as the MDR (Medical Devices Regulation), it came into force on 25 May 2020, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC. As a relatively recent issue, cybersecurity was barely covered by previous legislation. Hence, the task of the MDR to include cybersecurity specifications is a first of its kind in the EU. The JRC has been involved in a task force led by the European Commission's DG GROW which has developed guidance for manufacturers to implement the MDR's new essential safety and performance requirements related to cybersecurity.

> Disruptive technologies such as Artificial Intelligence, Blockchain and Quantum *will have an impact on the way cybersecurity will need to be achieved.*

4.4. Cybersecurity and blockchain

Blockchain can enable parties with no particular trust in each other to exchange digital data on a peer-to-peer basis with fewer or no third parties or intermediaries. Thanks to properties which include decentralisation, tamper-resistance, transparency, security and smart contracts, blockchain has been followed with interest by the cybersecurity community, given its potential to introduce new mechanisms to ensure trust and integrity in digital transactions.

The intrinsic nature of blockchain has some interesting advantages:

- It provides disintermediation and uses a model that does not require trusted parties.
- The parties have full guarantee that the transactions will be executed as expected.
- Being fully distributed, blockchain services and the underlying data are resilient to failures, DoS and, in general, make a well-designed system harder to attack. As a result, the transactions and data stored in the blockchain are themselves resilient to cyber attacks and remain under the control of the users' community.
- Blockchains are transparent and cannot be modified.

In addition, what makes blockchain appealing from a cybersecurity perspective is the concept of smart contracts, a computer program that is embedded in a blockchain which inherits the characteristics of blockchain and thus has no downtime, censorship or third-party interference. As a result, smart contracts cannot be altered, thereby covering another cybersecurity priority, i.e. ***process integrity.***

In other words, today, blockchain appears to be a promising option to be considered when it comes to enforcing trust, resilience to DoS, integrity and the authenticity of data and processes.

However, while blockchain holds potential benefits for cybersecurity, several challenges remain. From a development perspective, the main challenge is the lack of best practice and experience on how to develop professional services based on blockchain in a secure way. This also affects the deployment of smart contracts.

4.5. Cybersecurity and AI

In recent years, revolutionary technological developments have brought AI to the centre of digital transformation (Annoni et al., 2018; Villani, 2018).

It is not easy to define AI either as a specific scientific discipline or as some form of specific computer engineering. AI encompasses many disciplines and has itself been through many transformations (Stuart J. Russell and Norvig, 2016; Independent High-Level Expert Group on Artificial Intelligence, 2019) since it emerged in the 1950s (Moor, 2006). For the purposes of this report, we will adhere to the definition published by the European Commission's High-Level Expert Group on AI (HLEG) (Independent High-Level Expert Group on Artificial Intelligence, 2019). This definition is broad enough to encompass virtually all digital or robotic systems capable of some form of autonomous action or of adapting in some way to its environment or new data through some process of learning. Although the definition covers several sub-fields of AI, for many purposes, we refer to systems belonging to machine learning synonymously with AI, since they currently produce the most successful and important applications of AI.

The application of at least partly autonomous algorithms in cybersecurity is actually not a new development[13]. Cybersecurity controls capable of functioning autonomously in order to protect systems and services have existed at least since the 1990s, for instance, in early methods to detect network intrusion (Paxson, 1999).

However, cybersecurity is increasingly being affected by recent developments in AI (Brundage et al., 2018; Osoba and Welser, 2017), mainly since many parts of the digital sphere are being transformed by AI and because it empowers cybersecurity itself. The changes ahead for cybersecurity include greater capabilities for cyber defence, lawful prosecution and digital forensics, the introduction of completely new types of software vulnerabilities in AI systems, and the deliberate malicious use of AI (Brundage et al., 2018).

The well-recognised dual nature of AI systems (Brundage et al., 2018) obliges us to reflect on the possible malicious use of AI. As with any new technology, AI introduces its own limitations on robustness against deliberate attacks and those of inherent safety, requiring specific new developments in AI cybersecurity, regulations and standards. These considerations become especially relevant in the context of the rising deployment of vulnerable AI in cyber physical systems and critical infrastructure controls, where the potential impact of an AI-related cyber incident can have direct harsh consequences in the physical world.

The intersection of general AI research, AI safety and robustness, and cybersecurity is a topic of rapidly growing importance for researchers and policymakers (see, for example, European Commission, 2018a; Amodei et al., 2016; Barreno et al., 2006).

4.6. Cybersecurity and quantum technologies

New technologies, such as quantum computers or quantum communication applications, are still very experimental and probably quite far from widespread usability. However, their potentially transformative impact on cryptography and information security warrants their inclusion when considering the future of cybersecurity.

In quantum information science, communication and information processing are based on quantum physical laws and real quantum systems are used as information carriers[14] (Bennett and Shor, 2006). This opens up the possibility for the direct technological exploitation of hitherto unusable quantum effects for computation. At the intersection of physics and computer science, the field has steadily evolved in recent decades from a theoretical endeavour into high-tech engineering (Quantum Flagship, 2019b). Once fully developed, the resulting technologies, such as quantum computers or quantum communication channels, are very likely to have a significant impact on computing, telecommunication and applied sciences.

For cybersecurity, two developments are of particular relevance:

- The threat posed by *quantum computers* to modern cryptography: Quantum computers, when finally deployed, will be able to perform tasks which are impossible with a classical computer (Nielsen and Chuang, 2011). A direct consequence of this is that some current cryptographic algorithms, based on challenges that are not solvable by classical computers, could easily be broken by a future quantum computer (Shor, 1994). In particular, this would affect communication protocols based on public key cryptography and, thereby, unsettle the foundations of modern cybersecurity. To counterbalance this threat, cybersecurity will have to incorporate the developing field of *post-quantum cryptography,* the study of quantum-resistant cryptographical schemes to replace the old algorithms.

- The development of *quantum cryptography* techniques, using quantum physical effects to improve the security of systems and services: the most important applications to date are *quantum key distribution protocols,* promising novel ways to use quantum entanglement for initiating completely secure communication channels between partners. In this context, in June 2019, at the Digital Assembly in Bucharest, Romania, representatives of seven EU countries (Belgium, Germany, Italy, Luxembourg, Malta, the Netherlands and Spain) signed a declaration agreeing to explore together how to develop and deploy a quantum communication infrastructure (QCI) across the EU within the next 10 years.

It is still hard to predict when a functioning quantum computer will be available or when quantum cryptography techniques will be in widespread use. Nonetheless, there is a real possibility that this will happen sooner rather than later. Quantum computing experts who responded to a JRC survey (Travagnin et al., 2018) gave a median estimate of

> “It is still hard to predict when quantum cryptography techniques *may become widespread in their use.*”

2032 ± 11.5 years for when current cryptographic protocols might be broken. Quantum key distribution is available commercially for certain niche use-cases and there have been several dozen medium to large scale publicly-funded trial deployments worldwide (Travagnin and Lewis, 2019). It is also the subject of much ongoing research see, for example, the European Commission-funded Quantum Flagship projects CIVIQ, QIA, QRANGE and UNIQORN, and the OpenQKD testbed (Quantum Flagship, 2019a).

In light of these uncertain predictions, any discussions on cybersecurity should already consider new quantum technologies.

SUMMARY

Cyber attacks continue to evolve and become more complex, taking advantage of technological evolutions. Although the main goal behind such attacks is usually financial gain, other motives may also be present, such as ideals. Attacks will always be feasible as no system is absolutely secure – it will always come down to correctly identifying the risks and the potential impact of an attack and thus protecting against it. Moreover, as the number of devices and technologies used continues to increase, so does the attack surface and the ways in which a system may be compromised. Although the vulnerabilities related to such attacks can vary, the human factor remains a constant weakness.

EVOLUTION OF CYBERSECURITY RISKS

This chapter explores in detail the potential effects of digital transformation and technological development increasing the risks associated with cyber attacks.

As shown in *Figure 19,* the number of cyber attacks has grown constantly over the years, with a corresponding growth in the resulting financial damage. For instance, the average cost of a data breach was estimated to be EUR 3.5 million in 2018, an increase of 6.4 % over the previous year (Ponemon Institute, 2018). More generally, it is foreseen that by 2021, cyber criminal activities will have an annual global cost of EUR 5.5 trillion (Cybersecurity Ventures, 2019).

> We must ensure that the positive effects of digital transformation in cybersecurity will outweigh the negative ones.

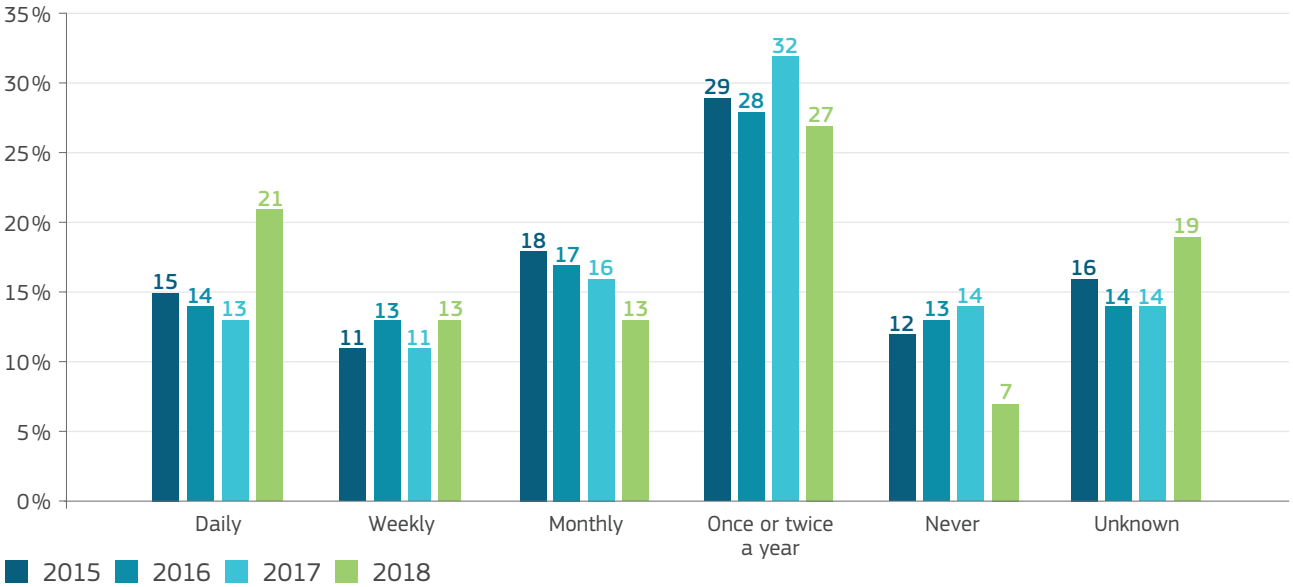


Figure 19: Increasing frequency of cyber attacks over the period 2015-2018 (percentages rounded to the nearest integer number) (Radware 2019)

> *The average cost of a data breach was estimated at EUR 3.27 million in 2018.*

To better understand how to counter this trend it is important to understand risk both in the cybersecurity context and in the evolution of the cyber threat landscape scenario, in terms of actors, motivations and targets. Only in this way will it be possible to identify and prioritise the correct mitigation actions and strategies.

5.1. A cybersecurity conceptual model

Cybersecurity risk, like any other type of risk, is the combination of two main factors: how likely a negative cyber event is to happen and the potential consequences of such an event. Even if an event is not likely but its impact is large, the resulting risk will still be very significant. For example, this is the case when the outcome of a cyber attack can put human lives at risk, albeit the chances of it occurring might be generally low. Therefore, even in very unlikely threat scenarios, the risk still needs to be properly addressed to prevent a potential disaster. An example of such a scenario could be a major terror cyber attack against some component of a country's nuclear plant installations.

The *likelihood* that a negative cyber event will take place depends on *who* might be motivated to conduct the attack and on *how* the attack could take place (Joint Task Force Transformation Initiative, 2012). The *impact* is the consequence of a successful attack on the target.

Cybersecurity risk is based precisely on these three main dimensions: *threat actors* (i.e. cyber attackers), *vulnerabilities* (i.e. systemic weaknesses) and *impacts* (i.e. adverse effects of successful cyber attacks, either intended or collateral). *Figure 20* puts these three dimensions of cybersecurity into context, showing their interconnection and their role in the composition of the cybersecurity risk.

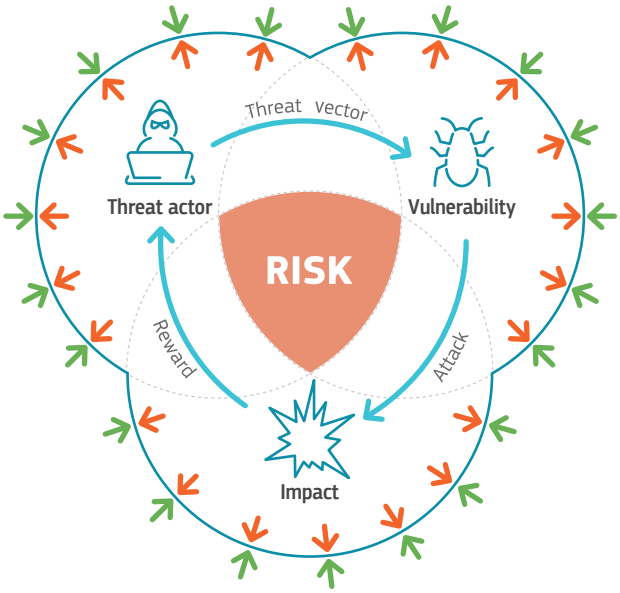


Figure 20: Conceptual model depicting the logical links between the different components of the cybersecurity risk in the context of the influence of digital transformation

There are clear interactions between all dimensions, depicted by the innermost clockwise circle of arrows.

- *Threat actors* refer to any actor or group with a motivation to carry out a cyber attack to secure a certain reward. This can include the full spectrum from mere cyber criminals who seek to make money, to activists following an ideology, or to state-sponsored attackers.

- *Threat vectors* are the means at the disposal of threat actors to exploit existing *vulnerabilities* by using a threat tool for a cyber attack, depicted by the first inner arrow. Threat tools are any form of malicious software, also known as *malware,* for instance a computer virus. Vulnerabilities can take on many specific forms, but mainly reflect security weaknesses in the design of software and computer code.

- *Threat actors* seek to *receive a reward* from their attack, ultimately causing the *impact.* An impact of a cyber attack is usually caused by a combination of rewards intentionally sought by the perpetrator – for instance, the money stolen by a banking Trojan – and collateral damage of the attack – for example, a ransomware attack that results in the disruption of systems and communication networks.

The area within the three overlapping circles in *Figure 20* represents the effective cybersecurity risk. In theory, no risk exists if one of the three key elements is absent. Likewise, the risk is greatest if all three factors are high simultaneously. In the real world, vulnerabilities always exist as no ICT system is perfectly secure, nothing is without impact and there will always be some motivation for threat actors to attack a system. Thus, the goal of a cybersecurity risk assessment is always to determine the magnitude of risk, not whether it is present or not. If the estimated risk warrants action, taking into account the limited resources, *mitigation strategies* (controls) need to be devised to reduce that risk to an acceptable level, i.e. 'residual risk'.

Cybersecurity risk can either be mitigated by deploying mechanisms aimed at reducing the cyber threats (e.g. deterrent actions, such as cybercrime prosecution), or those to prevent vulnerabilities (e.g. identification of vulnerabilities and software patching to correct them) or mechanisms to mitigate the effect of impacts (i.e. increased resilience). The level of risk acceptance is often combined with another aspect of risk management, the transferral – i.e. the contractual shifting of a risk from one part to another through insurance.

Digital transformation constantly creates new digital assets, which can be *vulnerable* to cyber attacks, thereby increasing rewards and motivations for threat actors. This enlarges the so-called *attack surface*[15], ultimately leading to higher potential *impacts* of cyber attacks.

However, cybersecurity risk can also be contained by putting in place the right countermeasures at the technical, organisational and societal levels. Such strategies can positively influence these forces by supporting and helping to better counteract threats, vulnerabilities and impacts.

> "Digital transformation constantly creates new digital assets. *This enlarges the so-called attack surface, ultimately leading to higher potential impacts of cyber attacks.*"

Thus, the basic challenge ahead for cybersecurity lies in ensuring that the positive effects of digital transformation will outweigh the negative.

5.2. Evolution of the cyber threat landscape

To better understand how the landscape of cyber threat actors is evolving, it is important to start by detailing the possible profiles of those behind a cyber attack before clearly analysing their motivations.

5.2.1 Threat actors

Here is a typical classification of threat actors grouped by their motivation (ENISA, 2019c; CSAN, 2018):

- **Cyber criminals.** Professional criminals mainly motivated by financial gain and the most active group in the threat landscape.
- **Insiders.** Personnel (current or former) within targeted organisations, such as employers and contractors. They can cause security incidents intentionally or unintentionally. Intentional attacks usually have a financial motivation.
- **State-sponsored.** Government-funded actors, highly skilled and traditionally seen as the threat actor with the most resources and capabilities. They are motivated by political and geopolitical agendas.
- **Hacktivists.** Individuals motivated by social or political movements, without links to governments or private corporations.
- **Cyber terrorists.** Individuals motivated by political or religious extremist beliefs and ideology.
- **Script kiddies.** Typically people with limited knowledge of hacking, relying on publicly available third-party tools to conduct their attacks. Their lack of knowledge limits their awareness of the consequences of their actions. Their main motivations are mischief, ego, curiosity and thrill-seeking.

Although there is a clear distinction in the motivations among threat actors, in recent years, the differences in terms of skills and resources have diminished (ENISA, 2019c; CSAN, 2018). Moreover, threat actors can act on behalf of more than one category. Cyber criminals, for example, may offer their services to third parties like hacktivists or state-sponsored groups, whereas an individual working in a state-sponsored group could end up becoming a hacktivist or an insider. In terms of resources, in the past, state-sponsored actors were considered more capable, but nowadays trends show that groups like cyber criminals are comparable in terms of skills and resources. Quite often, top-tier criminal syndicates as well as state-sponsored groups are referred to as advanced persistent threats (APTs).

This reduction in the capability gap among the various groups of threat actors is due to several circumstances. In this era of digital information, the knowledge to conduct cyber

> “Launching a distributed denial of service attack nowadays *is as simple as subscribing to a mobile provider.*”

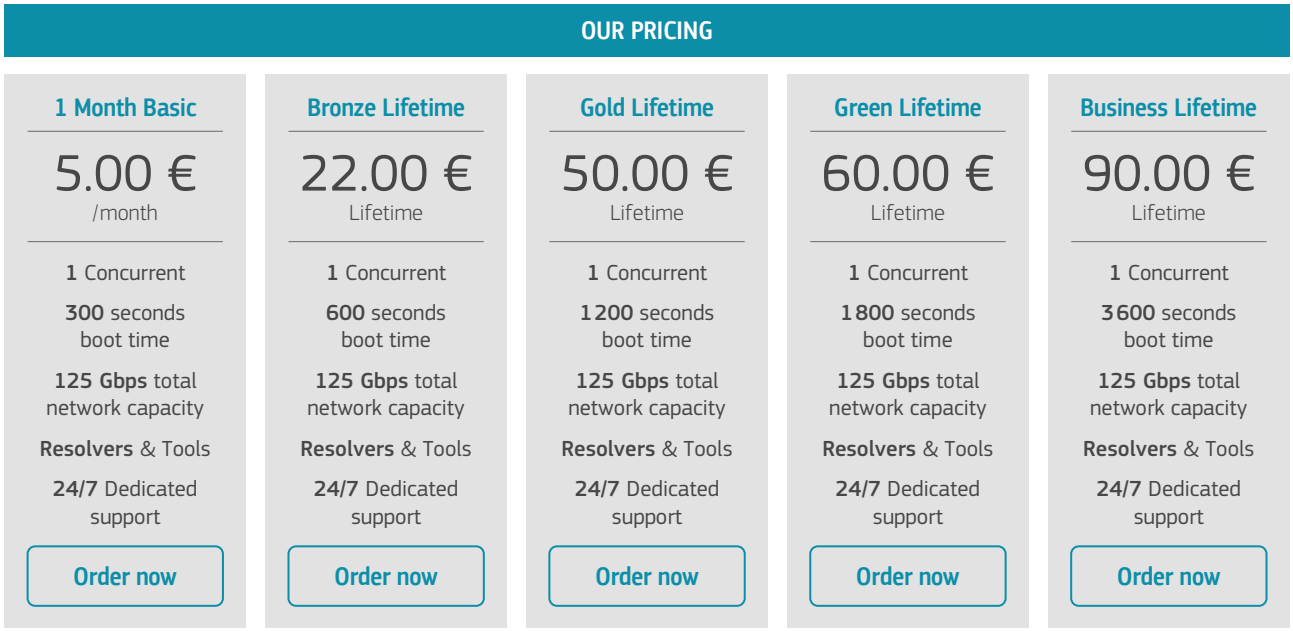


Figure 21: Price list of a service offering DDoS attacks (Makrushin, 2017)

attacks can usually be acquired very cheaply or even for free. In addition, the proliferation of the cyber criminal market reduces the cost of launching cyber attacks. Crime-as-a-Service (CaaS) has proven to be a lucrative business, thanks in part to the myriad of devices that came online with the digital revolution. For example, launching a DDoS attack nowadays is as simple as subscribing to a mobile company as criminal services are offered on the dark web to anyone without requiring any specific knowledge or resources, as depicted in *Figure 21.*

Hence, cybersecurity experts are increasingly being faced with the problem of clearly categorising hypothetical threat actors and their resources. This trend is reflected in aggregated data on threat-actor motivations, where it can be clearly seen how non-attributable motives are becoming increasingly significant *(see Figure 22).*

In this new context, the best way forward is to move away from an approach whereby cybersecurity measures are identified and applied after the IT system has been designed and eventually breached to a model of security-by-design in which cybersecurity is an integral part of products and services.

Another complex problem is how to identify threat actors and attribute a cyber attack to its original set of perpetrators in the context of their motivation. First, threat actors are making greater use of technology to cover their tracks: for instance, by using specific network protocols or email as their attack vectors. Second, threat actors deliberately obfuscate their real motivations by pretending to conduct another type of attack. And lastly, due to the virtual borderless nature of the internet and the relative ease of making use of threat tools or CaaS, single actors now have the possibility of simultaneously targeting thousands, or even millions of citizens and infrastructure targets.

The same – possibly single individual threat actor – who impacts millions of targets on one side of the globe, can physically reside in a different country, i.e. outside the jurisdiction of the country where the damage has been caused. This problem is crucial for lawful prosecution efforts as well as for issues of national security and defence. For a general overview, *Figure 22* illustrates the motivation behind cyber incidents in recent years (Radware, 2019).

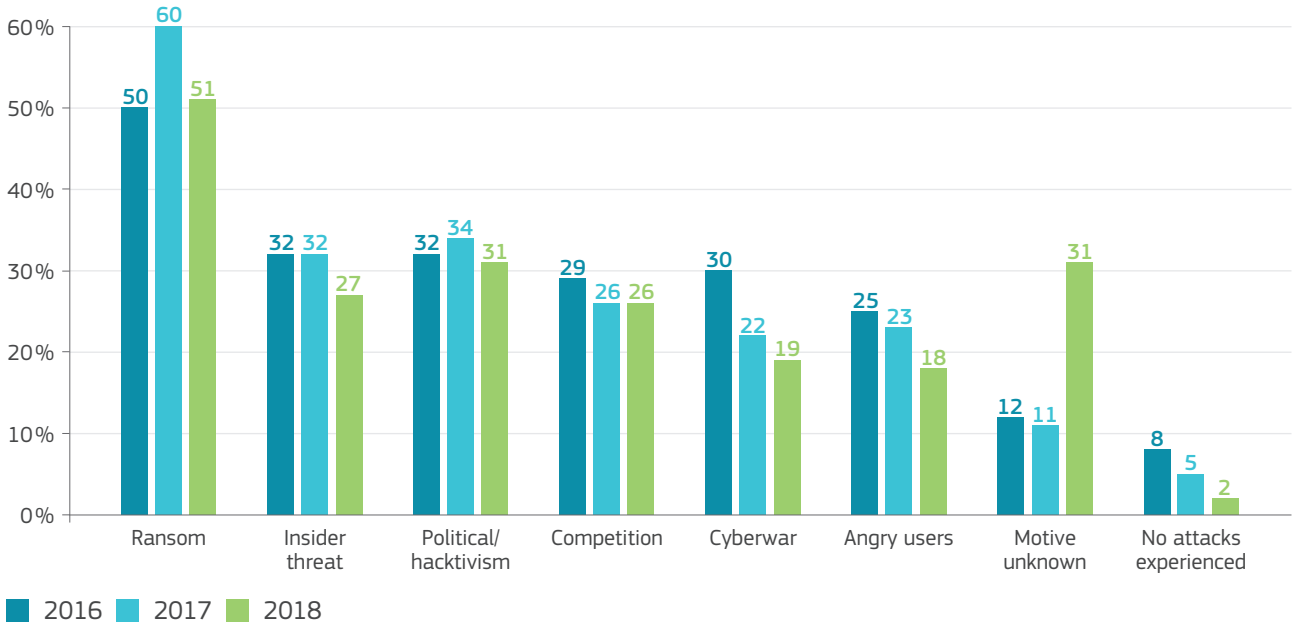


Figure 22: Overview of the motivations identified behind cyber attacks. The data come from an annual survey by Radware of 790 organisations of various types. The percentage indicates the share of respondents who were victims of a cyber attack.

5.2.2 Financial motivations behind cybercrime

Cyber criminals have always found creative ways to 'monetise' their attacks. Thus, obvious targets for threat actors include all digital transactions and, more specifically, online banking. In 2016, the estimated fraud from online payments was EUR 1.8 billion, 35 % more than in 2012 (European Central Bank, 2018). In recent years, there has been an increase in incidents directly targeting banks rather than end-users, such as the attack against the Bangladesh Central Bank in 2016.

> "Cyber criminals will always take advantage of *new technological developments to find new ways to monetise cyber attacks.*"

Cyber criminals are also adapting their strategies in line with technological trends, such as the cryptocurrency boom. Drawing a parallel with 'traditional online banking', cyber attacks in the domain of cryptocurrencies are directed towards end-users – aiming to steal the content of cryptocurrencies wallets – or towards higher-profile targets, such as the attack against the MtGox cryptocurrency exchange in 2013 (Leyden, 2013). Mobile banking malware is another example of how criminals have adapted to the digital economy.

Threat actors have also been ingenious in designing new approaches to steal cryptocurrencies. Compromised machines, more traditionally used to conduct advanced attacks (e.g. DDoS, SPAM campaign, etc.), are now also being exploited for their computational performances to mine cryptocurrencies. Such a technique, called cryptojacking, is yet another use case of the well-known botnets, networks of compromised machines controlled by one or more central nodes.

BOX 2. SWIFT bank heist

In February 2016, a group of hackers infiltrated the Bangladesh Central Bank and stole EUR 74 million. The attackers managed to send 35 SWIFT instructions ordering the transfer of USD 1 billion (EUR 912 million) from the bank's account in the Federal Reserve Bank of New York. The first four transfers went through, but the fifth one was stopped due to a spelling mistake in the recipient's name (Serajul Quadir, 2016). The attack was attributed to a group suspected of ties to the North Korean government (the Lazarus Group) (Symantec, 2017; Corkery and Goldstein, 2017), although the authorities did not rule out the participation of an insider agent (Devlin Barrett and O'Keeffe, 2016).

Last but not least, the features offered by some cryptocurrencies in terms of flexibility, ubiquity and anonymity have been welcomed by cyber criminals. They are often the choice for the receipt of ransoms, a modern strategy employed by cyber criminals to access a more recent source or revenue (Europol, 2018). Typical examples of these attacks make use of ransomware, in which threat actors block access to data or resources until the ransom is paid.

The Ponemon Institute produces an annual report analysing the cost of data breaches (Ponemon Institute, 2018). According to their results, the average total cost of a single data breach in 2018 was EUR 3.6 million, representing an average cost per lost or stolen record of EUR 137. The number of known data breaches per year continues to increase globally, as illustrated in *Figure 23,* highlighting the importance of this topic.

While attacks may be motivated by financial gain, money is not the main driver behind the main risks society faces today.

5.2.3 Cyber warfare, hybrid threats and hacktivism

The range of impacts from attacks driven by ideologies or (political) agendas rather than money[16] is extensive. It includes targeted cyber espionage activities threatening companies' intellectual property, cyber attacks against critical infrastructure with potentially dramatic effects

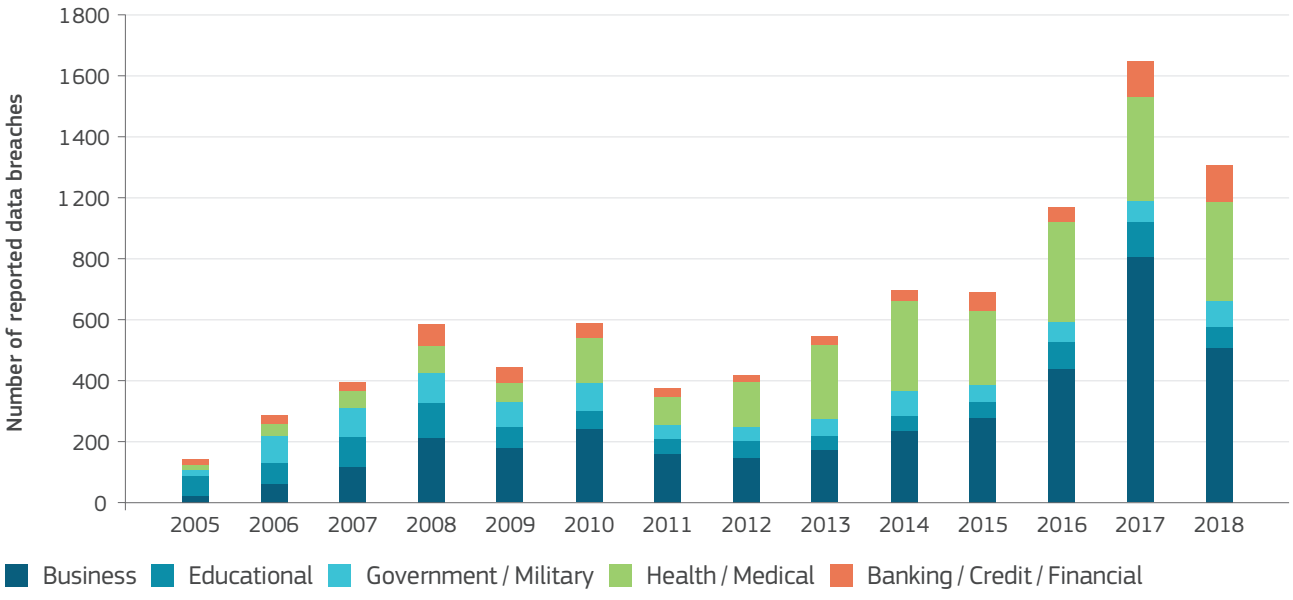


Figure 23: Number of data breaches in recent years

> *Today, the most common driver of malicious activities in the cyber world is money.*

on the physical world, disinformation campaigns aiming to provoke emotional and psychological effects within society, or even the deployment of cyber capabilities in a military conflict to support regular warfare. One such example of a hybrid attack is that against Ukraine's electricity infrastructure which temporarily disrupted electricity supply to over 225 000 consumers in December 2015 (Styczynski, Beach-Westmoreland and Stables, 2016).

The common reason behind these attacks is their strategic reach, potentially weakening national security. This probably explains the steep increase in state-sponsored cyber incidents (Council on Foreign Relations, 2019) often connected to activities considered as a hybrid threat (European Commission, 2017c; Treverton et al., 2018). Unfortunately, unequivocal state attribution of such sophisticated cyber attacks is very difficult.

A prominent example is the case of the malware 'NotPetya' (Greenberg, 2018). In 2017, it quickly spread all over the world, encrypting data and demanding a payment for recovery. In the end, analysts tend to agree on the fact that NotPetya had only disguised itself as ransomware; the real objective was to destabilise the initial target, Ukraine, through a series of attacks aimed at making some key services useless for a certain period of time. This new way of attacking makes it difficult to detect and attribute attacks, thereby leaving no way to swiftly mount any defence against the original threat actor.

It should be noted that the EU's 'Cyber Diplomacy Toolbox' explicitly retains the possibility to react diplomatically even when attribution is not entirely clear, marking a major shift in European policy (Council of the European Union, 2017; Bendiek, 2018). In this context, the EU is collaborating closely with NATO as hybrid threats often have military implications. In the EU-NATO Joint Declaration of Warsaw in 2016, 20 of the 74 proposals are devoted to hybrid threats.

From a geopolitical perspective, the emergence of cyber diplomacy issues raises the need to access innovative cybersecurity solutions to protect relevant national assets. Considering the current market in cybersecurity products, this will lead to looking for solutions beyond European borders. For that reason, the focus is increasingly on considering cybersecurity in discussions on strategic autonomy, especially when it comes to digital supply chains and critical infrastructures.

BOX 3. The attack against Estonia

In April 2007, Estonia, which was already an advanced digital society, suffered a series of coordinated cyber attacks that targeted governmental institutions and bodies, financial entities, telecommunication infrastructure and newspapers. A surge of DDoS attacks lasting several weeks caused disruptions at institutional sites and in national online public services and communications, impacting the normal functioning of the national government and society (Schmidt, 2013). These attacks were not highly sophisticated and, due to their nature, did not create any lasting damage to Estonia's digital infrastructure. However, they demonstrated how cyber attacks taking advantage of the digital transformation of governments and society could severely harm an entire country (Joubert, 2012). These attacks helped to shape Estonia into the leader in cyber defence it is today.

A recent example of this is the controversy over whether or not to allow Huawei, a Chinese tech company, to build European infrastructure for 5G networks (Cerulus, 2017).

5.3. Evolution of attack surfaces and attack tools

As no ICT system can be formally proven to be totally secure, the question that should be asked about security is not whether a system could be compromised but rather 'when, how and with what impact'. Regarding the 'when', clearly it is impossible to provide an answer *a priori* (without relying on certain intelligence information). 'How' and 'what impact' are essential questions which form the basis of cybersecurity strategy. This section will provide a brief overview of the evolution of how cyber attacks are executed and the typical vulnerabilities of modern IT systems.

5.3.1 Digital transformation and attack tools

The widening of the attack surface is a clear opportunity for threat actors to increase the diversity of targets and the variety of threat tools. Such an evolution is depicted in *Figure 24,* based on insights provided by ENISA's Threat Landscape Report (ENISA, 2019c; 2012; 2013; 2015; 2016b; 2017) published annually.

One of the most evident trends is the decline in recent years in the use of *exploit kits* (a utility program that attackers use to launch exploits against vulnerable programs). While exploit kits are turnkey solutions that are still in use, lately, threat actors have favoured other types of attack vectors, in particular those that employ legitimate tools, including penetration testing software. The reason behind this shift is that the maintenance of such tools is expensive and requires specific skills, which can be circumvented when misusing legitimate, often free-of-charge, well-maintained software.

This legitimate versus illegitimate use of machines, tools and, nowadays, software, is something cybersecurity must deal with properly. This is especially true for new and emerging technologies and cybersecurity tools themselves.

New technologies are often not fully understood when introduced and, moreover, lack standards or regulation regarding their exploitation and usage. A very relevant example from the current technological landscape is the potential use of AI tools and techniques by threat actors. We are only at the beginning of the widespread use of AI-based systems and, as a result, have not yet witnessed widespread misuse. However, cybersecurity should be both aware and ahead of this trend. It is entirely reasonable to expect more developments, including the increased targeting of human vulnerabilities via autonomous social engineering, social media manipulation, and AI-based fake content, or the development

RANK	2012	2013	2014	2015	2016	2017	2018
1st	Web-based attack	Web-based attack	Malware ▲	Malware	Malware	Malware	Malware
2nd	Malware	Malware	Web-based attack ▼	Web-based attack	Web-based attack	Web-based attack	Web-based attack
3rd	WebApp Kit	WebApp Kit	WebApp Kit	WebApp Kit	WebApp Kit	WebApp Kit	WebApp Kit
4th	Exploit Kit	Exploit Kit	Botnet ▲	Botnet	DoS ▲	Phishing ▲	Phishing
5th	Botnet	Botnet	DoS ▲	DoS	Botnet ▼	Spam ▲	DoS
6th	DoS	Physical Damage ▲	Spam ▲	Physical Damage ▲	Phishing ▲	DoS ▼	Spam
7th	Phishing	Identity Theft ▲	Phishing ▲	Insider Threat ▲	Spam ▲	Ransomware ▲	Botnet
8th	Data Breach	DoS ▼	Exploit Kit ▼	Phishing ▼	Ransomware ▲	Botnet ▼	Data Breach
9th	Ransomware	Phishing ▼	Data Breach ▲	Spam ▼	Insider Threat ▼	Insider Threat	Insider Threat
10th	Spam	Spam	Physical Damage ▼	Exploit Kit ▼	Physical Damage ▼	Physical Damage	Physical Damage

Figure 24: Evolution of the most-used attack vectors in the previous seven years

of unregulated autonomous cyber weapon or even real-weapon systems (Annoni et al., 2018; Brundage et al., 2018; Svenmarck et al., 2018).

When it comes to cybersecurity tools, it is important to understand that they can be misused quite easily to perform offensive actions, and that this is inevitable. However, it is also important to underline that offensive cybersecurity is not automatically the prerogative of malicious actors. Law-enforcement agencies need to employ advanced tools or approaches themselves to conduct lawful interception or to decrypt legally obtained evidence (e.g. consider key escrow technologies, code-obfuscation technologies, and backdoors). To counteract certain types of cyber attacks, it is almost inevitable to engage in offensive activities oneself, a prominent example being taking down a botnet. For this important matter, it is necessary to

reflect on society's underlying security needs. This complexity is captured by B. Schneier in his 2019 paper 'Cybersecurity for the Public Interest' (Schneier, 2019a).

5.3.2 Malware

Over the last five years, malware has been the most common attack vector, as shown in *Figure 25.* Malware can be defined as any code that has invaded a system or a service, aiming to affect its normal behaviour, for instance, by granting non-authorised access, blocking computing resources, or leaking private information. Several threat assessments have introduced a refined taxonomy of malware as it is considered that some types of malware deserve specific treatment, such as ransomware, banking Trojans and many others.

This report does not delve into this level of detail but instead refers to malware in broad terms and only using more specific terms where relevant. As illustrated in *Figure 25,* the use of malware has increased constantly over the last decade. More specifically, AV-Test spotted a rise in the number of malware from 47 million in 2010 to 868 million in 2018 (AV-TEST, 2018). For example, malware targeting mobile platforms increased from 5 million in 2014 to 20 million in 2017, according to McAfee (McAfee, 2018). There have been several massive attacks targeting the plethora of new pervasive devices, such as the Mirai botnet which affected a myriad of IoT devices (Kolias et al., 2017).

Today, malware is becoming an extremely elaborate tool able to adopt a number of techniques in order to remain hidden. Threat actors are increasingly taking advantage of cloud services, email providers, VPN services, etc. to reduce their activity footprint to allow them to remain undetected. In addition, the communication channel malware uses to exchange information with the threat actors is becoming encrypted more and more frequently. Cisco has pointed out a 300 % increase in encrypted communication from malicious software (Cisco, 2018). Malware is even seen now as a service as criminals are providing 24/7 customer support together with patches and updates to reinforce their malicious software (Europol, 2014b).

5.3.3 Vulnerabilities

Although attack tools differ at many levels (e.g. sophistication, target, impact, etc.), they all need an entry point into the targeted system(s). Vulnerabilities are not necessarily technological

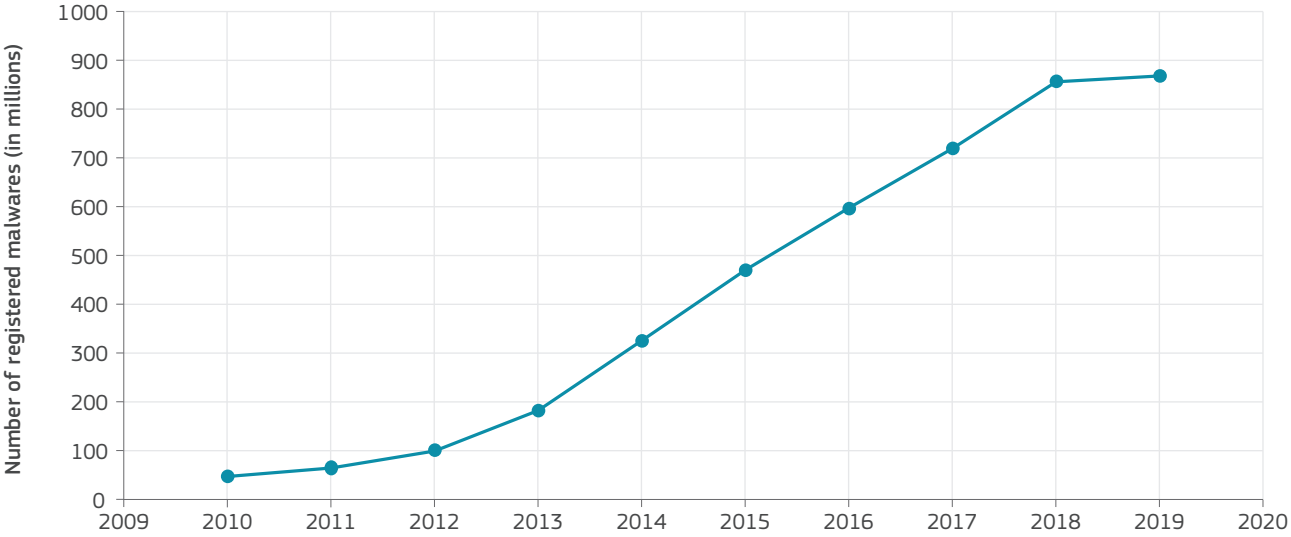


Figure 25: Malware evolution from 2010 to 2019, according to AV-TEST

or undesired in the first place. They can appear intentionally or otherwise during the design of the underlying code, its implementation or integration within the full architecture. There may also be a weakness in the foreseen used protocol, in a company's business processes, or in the end-user's understanding of the message, etc. Surprisingly, while security awareness is steadily growing, the number of detected vulnerabilities is also growing.

Technical limitations

External factors can add unavoidable constraints, sometimes at the expense of correct security properties. Such technical limitations can come from the specifications of a newly designed system. For example, the deployment of mobile sensors over wide areas – e.g. to enhance forest monitoring (White et al., 2016) – requires small, autonomous sensors. Such devices have limited processing, memory, and battery capabilities, thereby excluding the use of well-known and widely deployed security mechanisms.

Technical limitations can also be the consequence of the digitalisation of previously isolated systems. This is particularly relevant in the case of critical infrastructure and Industry 4.0. As industrial installations, especially large ones such as petrochemical installations or energy power plants, are expensive to build and maintain, their evolution typically follows an incremental, plug-in approach: new technologies have been added on top of the existing layers to guarantee backward compatibility with the devices that could not be changed.

This situation has resulted in the simultaneous coexistence of modern IoT devices and legacy devices. The fact is that legacy devices were deployed when industrial installations were considered a 'closed environment', difficult to access remotely, and therefore designed without any specific form of protection against cyber attacks. Thus, the 'opening up' of these infrastructures to the external world to exploit the potentials of IoT is potentially exposing vulnerable legacy systems to cyber attacks.

New technologies mean unforeseen weaknesses

Understanding the potential security flaws that new technologies entail from day one is a challenge in itself. A new vulnerability or design flaw in such a system can be of a very different nature, making its identification potentially harder at the very beginning. For example, this could be expected from quantum technologies opening up

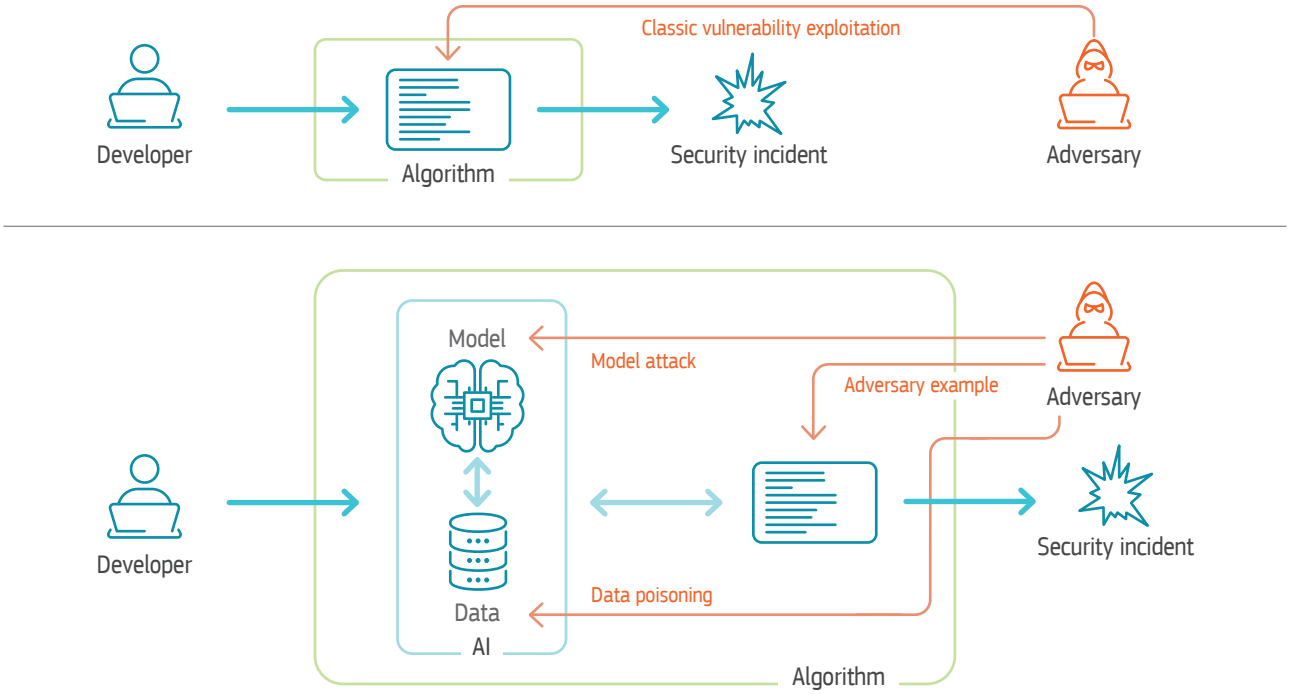


Figure 26: The inclusion of AI components may affect the security of the underlying system

new vulnerabilities in systems hitherto expected to be secure by means of legacy encryption techniques. Further, tracing an event and its cause, such as an attack on a system and its exploited vulnerability, can be a much more demanding task if the new technology is introducing inherently more complex systems.

The recent boom in AI-based systems is a concrete example of such a situation. In AI software, complex dependencies between the algorithm, the data with which the algorithm is trained, and the final AI model produced create entirely new ways to attack an ICT system. This situation is illustrated in *Figure 26* where by corrupting the data provided to the AI algorithm the attacker attempts to modify either the model generated by the algorithm or the decision taken using this model. There is growing evidence of just how easily these new vulnerabilities can be exploited in real applications (Biggio and Roli, 2018), affecting cyber physical systems such as autonomous cars, and thereby creating tangible dangers for end-users' lives (Eykholt et al., 2018). As the number of real-world systems containing an AI component is likely to grow, safeguarding such systems is of the utmost importance. Without doubt, the challenge to provide AI systems able to withstand malicious attacks will play an increasingly critical role in the cybersecurity arena.

The human factor

Software vulnerabilities are not the only entry point of an attack. Sometimes end-users unwittingly facilitate this through a lack of understanding of their actions. For example, although security updates are crucial to limit the impact of discovered vulnerabilities, users do not always apply security patches, thereby leaving the door open for attackers. In 2017, 41 % of Android users had not updated their phone for at least two months (Symantec, 2018). As a consequence, even if a given vulnerability is fixed, lack of human intervention is the remaining vulnerability allowing an attack to occur.

In other cases, the user installs a malware through a phishing attack giving key information through a social engineering approach, or installs an application on his or her mobile without paying attention to the permissions they grant to the application. This has been a feature throughout

the COVID-19 pandemic where, from the very beginning, phishing attacks have taken place, taking advantage of people's vulnerability throughout this period.

Sometimes, the security of a system also relies heavily on the user. Password-based authentication is known to have its limitations as humans are typically inefficient in generating and/or remembering randomness. Therefore, while some systems are secured with strong mechanisms, they may collapse because of a weak password or the reuse of passwords for websites and online services. In some cases, even a secure password can fall victim to a targeted social engineering attack involving the human behind the password. Two-factor authentication aims to reduce the impact of weak passwords by adding an extra security component.

"While some systems are secured *with strong mechanisms, they may collapse because of a weak password.*"

5.4. Growing impact of cyber attacks

In many scenarios, cyber attackers deliberately attempt to minimise the appearance of visible impacts in order to keep a low profile and maximise the reward obtained from a cyber attack. However, this does not imply that there will be no impact.

APTs are a good example of this. In APT scenarios, the impact is not immediately obvious as attackers aim to maximise their persistence in the compromise assets, further extending their presence over time by means of lateral movements. The impact will build up over time as no actions will be taken to mitigate it because initially it will not be obvious to the organisations affected. In this case, impacts tend to be higher in magnitude and scope.

In this context, it is also worth noting that the modern digital ecosystem exhibits complex interdependencies and that cyber attacks rarely occur in a linear fashion. Consequently, additional impacts will result from the exploitation of these dependencies. For example, in the DoS attacks conducted by the Mirai botnet in 2016, in addition to the loss of availability for the cyber attack targets (including parts of the DNS), additional impacts were registered due to abuse of the hundreds of thousands of compromised IoT devices used to conduct the attacks (e.g. consumer bandwidth consumed, degradation of the availability of the devices' legitimate functions, etc.).

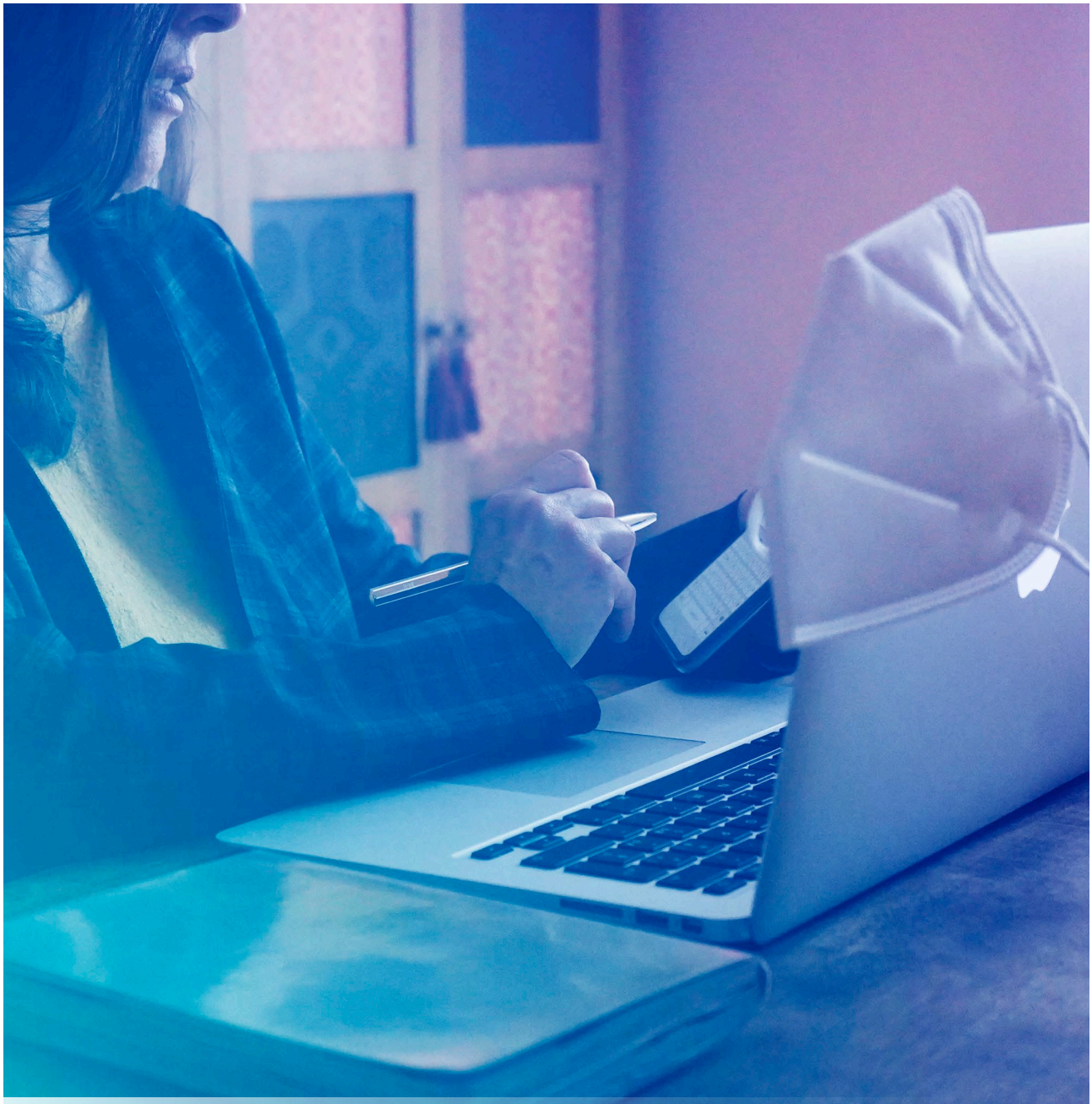
Cyber attacks that compromise the security of personal data are another relevant trend today. Massive cross-border personal data breaches can cause harm to millions of people who suddenly realise that their personal data can be violated by third parties threatening their fundamental right to privacy and data. Victims become more vulnerable to subsequent cyber attacks which misuse that information, such as online identity theft, financial fraud or extortion. Furthermore, the disclosure of personal information, in particular that of a sensitive nature, can have serious consequences for the individuals affected.

This type of privacy incident also adversely affects the organisation that suffered the breach in the form of loss of trust by investors and customers as well as potential lawsuits and fines.

BOX 4. Impact of the WannaCry cyber attack on the UK's National Health Service (NHS)

On 12 May 2017, the WannaCry cyber attack impacted the UK's National Health Service, affecting one-third of hospital trusts in England and over 600 primary-care and other NHS organisations (Smart, 2018; National Audit Office (NAO), 2018). As a result, hospitals could not receive patients, appointments had to be cancelled and staff had to rely on pen and paper given the malfunctioning of computer systems and communications. The overall estimated cost of the WannaCry cyber attack on the NHS was estimated to be £ 92 million (Department of health & Social Care (NHS) UK, 2018).

It was estimated that WannaCry ansomware infected over 230 000 computers in 150 countries on the first day alone (Department of health & Social Care (NHS) UK, 2018). This global ransomware outbreak revealed the weaknesses of governmental and industrial digital infrastructures around the globe and, in certain cases, caused major impacts on citizens, industry and governments.



SUMMARY

The COVID-19 pandemic has impacted many aspects of our everyday lives as the basic layers of our society have come under pressure. At a first glance, even though cybersecurity may appear to be an unrelated domain, it has been in the spotlight during this period. The unexpected increase in demand for digital services has been seen by cyber criminals as an opportunity to profit from the current situation, targeting businesses, governments and citizens. This chapter provides a snapshot of the actual evolution of cyber threats in relation the COVID-19 pandemic, and aims to demonstrate how cybersecurity is currently an important societal need, especially when global crises arise.

CYBER THREATS EVOLUTION AT THE TIME OF COVID-19

The events of the first half of 2020, with the COVID-19 pandemic hitting hard around the world, will be remembered for a long time.

All the basic layers of our society have been put under pressure, even domains such as cybersecurity which initially may have seemed far removed from the pandemic. The sudden large-scale move to teleworking, the use of digital services in hospitals, laboratories and government services, and the explosion in online schooling simultaneously accelerated the digitalisation of our society and, unfortunately, enlarged the attack surface at the disposal of malicious actors.

In other words, all the risk scenarios described in the previous section materialised together in the space of just a few weeks. This section presents a snapshot of the evolution of cyber threats in relation to the COVID-19 pandemic and demonstrates how cybersecurity is currently a societal need, especially when global crises arise. Below, we present a sort of 'war-diary' snapshot of cyber threats linked to the COVID-19 pandemic.

> Cybersecurity is fundamental to ensure operational and business continuity in periods of crises.

6.1. Malware (excluding ransomware)

In January and February 2020, reports of phishing campaigns and malware were already circulating[17]. On 13 February, a fake Chrome browser plugin (O'Donnell, 2020) employing COVID19-themed videos was used to empty victims' bank accounts. On March 18, researchers from CheckPoint (Lakshmanan, 2020b) revealed that hackers had created thousands of COVID-19-related websites as bait. Other recent reports note that cybercrooks altered their malvertising campaigns by making them COVID-19 relevant (Avast Threat Intelligence Team, 2020).

Spurred by the support measures taken by governments to assist people and businesses, there was a huge increase in targeted identity spoofing, typically by encouraging victims to click on seemingly trustworthy links and divulging personal information. On 19 March, IBM exposed a cyber criminal campaign aimed at distributing a keylogger via coronavirus-themed emails with messages impersonating the WHO Director-General, entitled 'Coronavirus Disease (COVID-19) CURE'. In a similar attack, dated 9 April[18], cyber criminals impersonated President Donald Trump and the White House.

COVID19-themed phishing also attacked industries and critical services, including aerospace, transport, manufacturing, hospitality, healthcare, and insurance, and has been distributed in several languages, including English, French, Italian, Japanese, and Turkish (Tidy, 2020a). Around 13 March, the WHO detected attempts to infiltrate their networks via a series of phishing emails (Satter, Stubbs, and Bing, 2020). There were also reports of attackers impersonating WHO staff to conduct cyber attacks (World Health Organization, 2020).

Examples of trojans used by cyber criminals also escalated in late March 2020, all exploiting a vulnerable public. Malwarebytes (Malwarebytes Threat Intelligence Team, 2020b), reported on an antivirus software allegedly capable of fighting real-life COVID-19 which installed a remote-access trojan. On March 25, Kaspersky researchers warned (Eremin, 2020) of the Ginp Android banking trojan which used a 'Coronavirus Finder', offering information on who was infected with COVID-19 in the user's vicinity for a minor charge, but which instead acquired the victim's credit-card details. On 25 March, Bitdefender (Arsene, 2020) reported that hackers were exploiting vulnerable routers to drop a malicious 'WHO' COVID-19 app. According to a 30 March report (Gatlan, 2020a), a banking malware was spreading through COVID-19 relief fund files where victims received phishing emails asking them to donate money by filling in forms for a coronavirus relief fund which instead downloaded the malware.

During the first week of April, ZDNet identified at least five new COVID-19-themed malware strains destined to wipe or rewrite files to disable a computer from rebooting (Cimpanu, 2020c). Kaspersky (Shcherbakova, 2020) unveiled a new type of phishing COVID-19-inspired scams that impersonated shipping carriers, including FedEx, UPS, and DHL to install a trojan or backdoor for vulnerable customers. With many people under lockdown, Microsoft warned that pirate streaming services and movie piracy sites were dropping malware (Gatlan, 2020b).

The April bulletins issued by CERT-EU reported at least 16 new family apps, all pretending to be legitimate COVID-19 software tools. According to a Europol report dated 14 April 2020, the number of malware families using COVID-19 continued to grow. ENISA reported in early May on the increasing sophistication and complexity of phishing and malware attacks since the pandemic hit Europe. On a more positive note, the growth now seems to be gradually receding.

6.2. Ransomware

Attacks on critical sectors and services, including energy, transportation, education, and healthcare have also proliferated. In February, the INA Group, Croatia's biggest oil company, became the victim of a ransomware infection (Cybersecurity Help, 2020a), while in the USA, a natural-gas processing plant was also compromised (CISA, 2020b). Within a day of ransomware operators stating that they would stop targeting health and medical organisations (Abrams, 2020b), the Maze ransomware group leaked sensitive data from a UK medical facility involved in coronavirus research following its refusal to pay a ransom (Goodwin, 2020).

Incidents continued throughout March and April in the USA and Europe with ransomware attacks on government and public health departments. Examples in the USA include the attack on a public health district in Illinois, a variety of attacks on hospitals using the Active Directory credentials ransomware and a hospital in Colorado treating COVID-19 patients (Pressey, 2020) and (CERT-EU, 2020a). Data from ExecuPharm, a pharmaceutical company, were posted on the dark web (Whittaker, 2020) and a wide range of confidential details from Berkine, a crude-oil exploration firm, were published by the Maze ransomware operator (Varghese, 2020).

In France, the IT systems used by several local authorities fell victim to ransomware attacks (Cimpanu, 2020a), while in Portugal, the systems of multinational electric power giant Energias de Portugal and the world's fourth largest producer of wind energy were encrypted by ransomware with a EUR 9.8 million ransom demanded (Gatlan, 2020c).

Furthermore, the coronavirus phenomenon was exploited by malicious mobile app coders. In mid-March, researchers revealed information on an Android ransomware called CovidLock which masquerades as a Coronavirus information tracker with the aim of locking the victim's smartphone until they accept to pay a ransom.

Overall, within a matter of weeks, ransomware attacks had increased by almost 150 % above the baseline levels in February 2020 (Upatham and Treinen, 2020). A recent ENISA report (ENISA, 2020b) on COVID-19 threats observed that the behaviour of cyber criminals had also changed, noting in particular that the time between infecting a system with ransomware and activation of the attack had fallen as cyber criminals attempted to maximise profits in the short term.

6.3. Critical infrastructures and services

Already under pressure from coping with the pandemic, health systems have been relentlessly attacked throughout this period. According to WHO's chief information officer, there were five times more security incidents targeting the organisation than during the same period in 2019 (Asokan, 2020). In fact, WHO has been the target of endless cyber attacks since the beginning of the COVID-19 pandemic (Ahmed, 2020).

One of the main testing facilities in Czechia, the Brno University Hospital, had to shut down its computers due to a cybersecurity incident on 13 March (Porter, 2020). A week later, Spanish police sent out an alert of a cyber attack targeting Spanish hospitals via a CoVID-19-themed malware (Dolz and Colomé, 2020). On 22 March, the Assistance Publique - Hôpitaux de Paris was targeted by a DoS attack (Fouquet, 2020), while on 27 March, the same kind of attack was launched against a consortium of hospitals in Europe. On 22 March, Ambry Genetics, a California-headquartered genetic testing laboratory reported an email hacking incident that may have exposed medical information on nearly 233 000 clients (McGee, 2020).

According to reports (Klöckner, Olk, and Rybicki, 2020), early in April, German public health minister Jens Spahn was the recipient of a ransom note entitled 'Attack on German hospitals', demanding EUR 25 million. In another April incident, the website of the Italian National Institute for Social Security suffered a DoS attack (Amante, 2020). On 1 April, the Russian state-owned telecom provider Rostelecom was involved in a major hijacking incident, when traffic routes intended for servers from Google, Amazon, Facebook and other cloud-hosting providers were diverted to Russian networks. On 20 April, COVID-19-themed attacks reportedly targeted the energy sector in Azerbaijan (Lakshmanan, 2020a). The scam uses MS Word documents as droppers to deploy a remote access trojan with the aim of exfiltrating sensitive documents, passwords, keystrokes, and others.

On 27 April, IT security researchers at Cyble, announced (Asif, 2020a) that it had identified hackers who had attacked Huiying Medical, a Chinese company with a worldwide presence. A raft of data, including information on COVID-19 experiments, was stolen, some of which have been spotted for sale on the dark web.

A recent CERT-EU cyber bulletin noted that no new COVID-19-related DoS attacks had been observed since 22 April (CERT-EU, 2020a). Nevertheless, on 30 April, the EU foreign policy chief Josep Borrell condemned the exploitation of the COVID-19 pandemic to launch cyber attacks on infrastructure and healthcare services (Council of the European Union, 2020).

6.4. State-sponsored actors

State-sponsored actors have also adapted their activities during the COVID-19 pandemic. Research institutions working in areas related to the pandemic have become targets of interest of state-sponsored actors seeking strategic advantage (CERT-EU, 2020b; 2020c). Fake news is another field where state-sponsored actors have become more active. In mid-March, the US Department of Health's IT systems were thought to have been attacked by a foreign actor (Stein and Jacobs, 2020).

Such attacks have been observed across the globe over the last few months and with varying motives. In March, a Pakistan-based threat actor dispatched a phishing email with a link to a malicious document imitating the Indian government (Cybersecurity Help, 2020b), while a campaign against the Mongolian public sector was also reported (Atlas Cybersecurity, 2020). According to reports (Panda, 2020), Vietnamese state-backed hackers launched campaigns against Chinese targets between January and April in order to collect intelligence on the COVID-19 crisis. In April, the Centre for Cyber Security in Denmark published a threat assessment (Centre for Cyber Security, 2020) warning of a very elevated threat from cyber espionage and cybercrime.

While scientists worldwide have been racing to develop a COVID-19 vaccine, the USA has observed foreign spy agencies carrying out reconnaissance of coronavirus-related research (Corera, 2020; Barth, 2020). Due to the pandemic, there is also a growing concern that the US

> "Research institutions working on areas related to the pandemic *have become the focus of interest for state-sponsored actors.*"

elections in November 2020 will be more vulnerable to outside interference (Miller, 2020).

6.5. Advanced persistent threats

Since COVID-19 was declared a pandemic, different types of phishing scams have been used by cyber criminals in an attempt to maximise their profits by preying on the fear of the virus. APT threat actors have also sought to exploit the pandemic via spear-phishing campaigns and watering-hole strategies, amongst others. According to Kaspersky's APT trends report Q1 2020 (GReAT, 2020), the list of attackers also included APT threat actors who, according to Open-source intelligence (OSINT), used COVID-19-themed traps to target their victims. Kaspersky reported the discovery of a suspicious infrastructure to health and humanitarian organisations, including the WHO. In addition, according to Malwarebytes researchers (Malwarebytes Threat Intelligence Team, 2020a), from late January, several cyber criminal and state-sponsored APT groups have used coronavirus-based phishing as their main infection vector to launch malware attacks. China was the first to be lined up as a target by APT groups, and as the virus spread worldwide, so did the attacks. Other recent reports (Dean Russell, 2020) highlighted that some APTs have capitalised on fake news, 'online trolls', and fake social media accounts to undermine other countries by spreading distrust and panic.

6.6. Data protection

Several countries, particularly in Europe, have made considerable efforts to develope contact tracing tools to curb the COVID-19 pandemic while also balancing privacy concerns. According to CERT-EU (CERT-EU, 2020a), as of 29 April, at least 43 countries globally had adopted or were currently testing surveillance technologies. The data typically stem from seven sources: mobile providers, smartphone apps, wearable devices like electronic wristbands, public cameras, facial recognition, aerial surveillance, and credit cards.

> "At least 43 countries have either adopted or are currently testing *contact tracing technologies with the aim of curbing the COVID-19 pandemic.*"

In addition, governments in several countries outsource data collection and data analytics to private companies or institutes, thereby creating additional risks of personal data abuse and privacy breaches. Attempts to safeguard privacy are diverse among countries. Four key criteria appear to be specifically relevant: grouped, anonymised surveillance versus individualised surveillance combined with identification; opt-in versus mandatory surveillance; degree of combination of several technologies; and the status of personal data protection regulations, such as the EU's GDPR. A characteristic example of this situation was the approval of emergency measures by the Israeli government for its security agencies to track the mobile phone data of people with suspected coronavirus (Tidy, 2020b). Bahrein and Hong Kong have also employed tracker wristbands to geo-fence individuals under compulsory home quarantine.

Another key issue of concern is the amount of data major tech companies, possess.

These giants are aware of individuals' whereabouts and habits and can profile them in the mid or long term. Although, if provided to authorities, such pieces of data can help in curbing the pandemic, the approach may create a negative privacy precedent, turning emergency contact tracing into a so-called 'new normal'.

On 9 April, the US National Law Review published an article offering privacy and cybersecurity regulatory and enforcement guidance around COVID-19 (Goldstick et al., 2020). In early April, a plethora of civil society groups signed a joint statement, enumerating several conditions for those governments currently using digital surveillance to fight the pandemic (Human Rights Watch, 2020). A similar list of principles for protecting civil and political rights in the fight against COVID-19 were published by the Freedom House (Freedom House, 2020) on March 24. According to Reuters (Busvine and Rinke, 2020), Germany altered its position on the centralisation of data generated by COVID-19-tacking mobile apps, opting for a decentralised approach to digital contact tracing, thereby abandoning a home-grown alternative that would have allegedly given health authorities central control over the tracing data.

Large- or medium-scale surveillance COVID-19-inspired campaigns also became the focus of cyber criminals. During the second half of March, Lookout! researchers discovered a malicious Android app called 'corona live 1.1.'. This app, a trojanised version of the legitimate 'corona live' app, appeared to be the most recent addition to the arsenal of a mobile surveillance campaign targeting Libyan individuals (Del Rosso, 2020). On 13 April, it was reported (Cyber Report, 2020) that the QR-code-based system that allowed Moscow citizens to generate permits for leaving their home was hacked while in beta-testing. For the sake of avoiding security by obscurity, the source code of a mobile app proposed to the Netherlands government to trace COVID-19 was publicly released. Developers were surprised to find that the source files contained user data stemming from another app (Osborne, 2020). In another similar case, a voluntary Bluetooth-based COVID-19 tracing app introduced by the Australian government falsely alerted users who were not tested for COVID-19 that they might be infected (Coble, 2020).

6.7. Cryptocurrencies and money mules

On 19 March, Coindesk announced (Hertig, 2020) that thousands of mining cryptocurrency machines were diverted to coronavirus research in cooperation with Stanford University in California. Specifically, CoreWeave redirected the processing power of 6 000 specialised computer chips towards research to find a therapy for the coronavirus.

On the downside, with many people unemployed or working from home due to the COVID-19 crisis, cyber criminals have been able to recruit many more 'money mules', namely, individuals who engage in money-laundering schemes under the premise of a work-at-home job offer (Krebs, 2020a). There were reports in Canada and the USA of money mules being recruited for a supposed COVID-19 foundation called 'Vasty Health Care Foundation'. Under this subterfuge, after completing a non-suspicious work-related task, individuals were asked to process donations in aid of fighting the virus. The mules received a specific amount into their bank accounts and could keep a portion with the remainder deposited in a Bitcoin ATM.

6.8. E-commerce marketplaces and the dark web

Cyber criminals and online opportunists have continued to prey on the public's vulnerability during the pandemic. They have sold counterfeit medical masks, fake treatments and cures on e-commerce marketplaces and social media platforms (Heilweil, 2020). According to Europol, the number of products which claim to treat or cure infection by coronavirus has increased sharply since the onset of the pandemic.

Scammers have requested upfront payment for such items, with buyers paying then not receiving the goods. The latest Europol reports stress that other types of scams, such as home-test kits or investments and donations related COVID-19, have also been detected. In fact, new variations of these COVID-19-themed scams are appearing daily, although as the pandemic recedes the number of such incidents is expected to decline over time.

The pandemic has also had a considerable impact on dark web operations. Given the shortages in source materials or special healthcare products, illicit goods have become more expensive. In many cases, fake and even dangerous coronavirus-related products have been offered at steep discounts (Bizga, 2020). Prominent examples of such products are personal protective equipment and home-care ventilators. An April report (Asif, 2020b) from HackRead.com noted that MP3 files 'with a special frequency' were being sold on the dark web with the claim that listening to them three to six times a day could help annihilate COVID-19. No less important, according to 13 April reports (Abrams, 2020a), half a million Zoom app accounts were put up for sale on the dark web. In fact, Cyble sent an alert that already by 1 April, free Zoom accounts were being posted on hacker forums.

6.9. Teleworking

In early April, CERT-EU reported how the COVID-19 crisis had resulted in a staggering number of employees working from home with a corresponding increase in the use of videoconferencing and chat apps, including Zoom, Slack, Skype, WebEx, Google Meet, and Microsoft Teams. While several vulnerabilities related to such apps were identified, a considerable number have affected Zoom (Hodge, 2020a; 2020b; Sebenius and Mehrotra, 2020). Also, in mid-April, a significant vulnerability was found to affect the Mail app on the iOS platform (Zecops Research Team, 2020). On 19 April, the US Cybersecurity and Infrastructure Security Agency announced that two separate attacks targeted as many as 50 000 different MS Teams users, with the purpose of phishing Office 365 logins (CISA, 2020a).

In this context, the cybersecurity protection of the smart home is of paramount importance (Europol, 2020a). ENISA describes a set of

> *The unprecedented adoption of teleworking schemes is clearly impacting the legacy schemes used to protect businesses and institutions.*

recommendations for both employers and staff to maintain an adequate level of cybersecurity when teleworking (ENISA, 2020c). In 30 April, the Microsoft Defender Advanced Threat Protection (ATP) research team announced the addition of new COVID-19-tagged assessments to their Threat and Vulnerability Management (Mittelman, 2020).

The need for social distancing, while maintaining close and everyday contact with other team members and stakeholders, has resulted in a massive uptake of cloud-based communication tools. In this accelerated uptake of cloud services, it is of the utmost importance to protect personal and business online identities by using strong passwords and even stronger forms of authentication (i.e. 2-factor authentication). The JRC has presented clear advice on how to choose strong passwords and to manage them securely (Joint Research Centre, 2019).

According to various recent reports, as VPN usage soared (Palmer, 2020), so did the number of poor (Scheels, 2020), exposed or vulnerable VPN services (Reynolds, 2020). In March, Europol (Europol, 2020a) stressed out that cybercrooks deploy fake VPNs to try to get access to mobile and personal devices, which now might contain company data too. No less important, on 24 April, the US National Security Agency published a comparative security assessment of current mainstream videoconferencing, text chatting, and collaboration tools (National Security Agency, 2020).

6.10. Disinformation campaigns, 'infodemic', conspiracy theories, and scammers

The increased use of digital and online services goes beyond the business dimension. A myriad of European citizens confined to their homes have depended almost exclusively on television, radio, social media, and instant messaging platforms to interact with society and stay informed of the rapidly evolving situation.

Adversaries have taken advantage of this situation by targeting society with disinformation campaigns and phishing attacks connected to the COVID-19 theme. This topic falls under the umbrella term 'anti-democracy attacks and cyber influencing', including fake news, cyber meddling, and astroturfing. 'We're not just fighting an epidemic; we're fighting an infodemic. Fake news spreads faster and more easily than this virus, and is just as dangerous,' said WHO Director-General at the Munich Security Conference on 15 February (World Health Organization, 2020). In contrast to closely policed platforms such as Facebook and Twitter, old-school text message campaigns, for example, via SMS or pivate WhatsApp and Messenger chats, spread COVID-19 fake news more easily. Many of the misinformation campaigns triggered relate to the capacities of national or regional authorities to deal with the crisis (CERT-EU, 2020a).

During this time, conspiracy theories, which try to satisfy a need for accuracy and knowledge, have proliferated, such as linking 5G technology to the pandemic (Gallagher, 2020) or others that fuel anti-immigrant and anti-Muslim sentiment (Krishnan, 2020).

> A pandemic easily leads to *an 'infodemic'*.

Even though there have been numerous examples of fake news linked to COVID-19, it is still not clear if they are the result of a targeted campaign. Newly introduced blockchain-based schemes that help the readership to check the origin of news is a step in the right direction. On 6 April, Italy's leading news agency ANSA announced ANSAcheck, a unique news-tracking system based on blockchain technology to enable readers to check the origin of news on their platforms (ANSA, 2020).

Email, SMS, instant messaging platforms, and even mobile and wireline connections have all been heavily exploited as phishing vectors. According to reports (Daly, 2020) dated 2 April, Russian scammers disseminated two different phishing emails impersonating President Donald Trump. The first was about an extended quarantine and an adjusted IRS tax deadline, while the other shared steps to slow the spread of the virus.

In another announcement (ACCC, 2020), dated 6 April, Australian citizens were targeted by scammers attempting to steal superannuation funds partially released due to the COVID-19 crisis. In mid-April, reports (Cimpanu, 2020b) revealed that the local government of North Rhine-Westphalia in Germany may have lost millions of euros after it failed to build a secure website for distributing coronavirus emergency aid funding. As of 26 April (Waqas, 2020), it was reported that scammers were posing as WHO representatives to solicit donations.

6.11. E-education and minors

The hasty major adoption of distance education in educational institutions of all levels also highlighted cybersecurity and data protection risks, including phishing attacks, ransomware, extortion, exposure to inappropriate content, unsafe sharing of personal data, and cyberbullying. In March, it was reported that minors were being targeted with pornography during hacked Zoom conversations (Mail Online, 2020). According to

CERT-EU, e-learning infrastructure, online classes, food delivery services or public health issues information websites in Europe were affected by DoS attacks in March. Furthermore, in other extortion cases, cyber criminals have claimed to know details and secrets of their victims' lives by infecting their computers. Not only was financial compensation requested in order not to disclose sensitive information, threats were also made to infect the victims' families with coronavirus.

Medium- and long-term data protection implications could also be foreseen. Distance learning based on Internet platforms creates new spaces where children's data are generated, exchanged, and stored. Some of these spaces belong to the personal and private sphere, and sometimes the system pushes users to share them. This could easily lead to an unsafe oversharing of personal information with implications for cybersecurity and data protection for both parents and children. In a report in late March, Europol (Europol, 2020b) noted a strong indication of greater online activity by those seeking child-abuse material.

6.12. Takeaways

The pandemic is a new reality and affects us all. Nevertheless, as the worldwide fight against COVID-19 unfolds, the cybersecurity community will come under further pressure as cybercrooks and wily opportunists have proven to be adept and agile in envisioning *modus operandi* and mixing old-school tools along with novel ones to harness major crises.

New or mutated pandemic-themed malware, ransomware, scams, and frauds will emerge. The dread and panic the pandemic has inflicted may entice even tech- and security-savvy people to, unconsciously or otherwise, disregard risks and fall for fraudsters and cyber criminals. In addition to legacy defensive measures, this situation urgently calls for awareness-raising, particularly as large-scale and prolonged teleworking, online shopping, online education, and other societal seismic shifts are almost certain to remain elevated in the future.

> *"The pandemic is a new reality which is affecting the modus vivendi of the international community."*

Governments have rushed to devise or embrace novel contact tracing mechanisms and monitoring systems to deal with the COVID-19 pandemic. Several of these systems exploit real-time positioning data from cellular networks or utilise facial recognition and other mainstream tech. In this context, and for the sake of safeguarding basic freedoms, policymakers must ensure that any surveillance system complies with human rights principles while allowing the authorities to do what is essential to safeguard public health.


09:02
85%
CONTACT
TRACING
APP

SUMMARY

Since cybersecurity risks cannot be completely eliminated, how can they be mitigated? Cooperation, knowledge and timely communication regarding the threats and how to face them is an important step forward. Education is of equal importance, both for end-users and for industries: cultivating a security-conscious approach with techniques such as security-by-design and security-by-default help to deal with the risk at an early stage. However, cyber attacks will still take place. Therefore, it is crucial to be ready to face them with the lowest impact possible on the overall system, i.e. to demonstrate cyber resilience. Effective mitigation should concern all three above-mentioned risk aspects.

CYBERSECURITY RISK MITIGATION STRATEGIES

The fundamental question cybersecurity is facing every day is how to tame and mitigate the overall growing cybersecurity risk. The challenge lies in setting up strategies to effectively manage and control such risks. Below we give an overview of the most relevant measures.

> All the cybersecurity risk dimensions must be mitigated by taking the appropriate and effective measures.

7.1. Deter threat actors

Conceptually speaking, cybercrime is not that different from traditional crime. Cybersecurity risk can therefore be mitigated by acting on the threat-actor element of the risk equation with measures specifically aimed at discouraging malicious actions.

This is precisely the goal of the deterrence strategy behind cybercrime laws and efforts of law-enforcement bodies to prosecute cybercrime. This is easier said than done as cybercrime poses specific challenges to law-enforcement agencies.

7.1.1 Cooperation between law-enforcement authorities and other stakeholders

Today, cybersecurity must be approached from a global perspective. Increasing effective cooperation amongst law-enforcement authorities from different Member States is necessary to address the rapid global evolution of cybercrime. The cybersecurity community is highly internationalised and criminal threat actors are increasingly organised in complex networks spread all over the world with capabilities to react in real time, adapting their attacks and concealing their digital traces.

Cooperation amongst law enforcement in this area should also extend to the Computer Security Incident Response Team (CSIRT), industry and academic communities. Industry is usually the one in possession of valuable information that can be used as evidence to prosecute perpetrators of cyber attacks. The research community can contribute to improving and developing better technical means to enable effective deterrence.

Implementing this type of cooperation is not always straightforward. Motivating some industry communities to assist law enforcement is still controversial in some situations and regulatory frameworks should specify clearly who can access

> The concept of international borders in *the cyber world is almost non-existent.*

user information and when. For example, in the case of a company where the main added value lies in its security and privacy practices, such collaboration with law enforcement could be perceived by its customers as a negative element. This situation may change as end-users' attitudes to cooperation in the fight against cyber-enabled crime evolve.

Wide cross-border collaboration is fundamental considering that the concept of international borders in the cyber world is almost non-existent. The cross-border dimension is the norm in cyber attacks, both because perpetrators and victims are often located in several countries and because resources dispersed on a global scale are usually used to conduct cyber attacks.

Agile collaboration among law enforcers is of paramount importance as it can boost their capacities to investigate and prosecute such cases efficiently and bring the perpetrators to justice. The activities of Europol and Interpol in this field are encouraging examples of international efforts in this direction.

7.1.2 Cyber threat intelligence

Cyber threat intelligence (CTI) is a technical term unifying approaches and techniques for the collection of intelligence of various kinds (i.e. open source, social media, technical, etc.) related to cyber criminal activities. CTI can collectively contribute to risk mitigation at many levels. The most natural one is by providing valuable information that can assist law enforcers in identifying the perpetrators of a given cyber attack. Indeed, it is often the case that there is no direct link between the threat actor behind

a cyber attack, the computer system compromised and the location of the subsequent impact.

Attributing cyber attacks to the threat actors who initiated them not only contributes to the prosecution of the attacks but also to improving preparedness to prevent future cyber attacks by identifying trends and analysing the technical and organisational means used to implement and conduct such attacks. It can also help to deter them by naming and shaming perpetrators.

All this information can complement the knowledge of law enforcers, cybersecurity professionals and researchers, thereby helping them to keep pace with the rapidly changing cyber threat ecosystem. As a result, they can be better prepared to assess cybersecurity risks, anticipate potential cyber attacks, and design and implement more effective countermeasures.

7.1.3 Reporting cyber attack cases

The timely reporting of actual and potential cyber attacks is extremely relevant as it is the key step in triggering prosecution.

Companies that fall victim to cyber attackers often hesitate to formally report it because of the perceived potential negative impact on the trust of their customers and public opinion. Cyber attacks directly impacting individuals are also usually left unreported by victims, who may either be unaware of the right process to follow to report this type of incident or simply fail to understand the importance of reporting them.

It is easy to see some parallels here with the well-known 'broken windows theory' in traditional criminology. Originally proposed in 1982 (Wilson and Kelling, 1982), this theory states that when a community or ecosystem becomes used to criminal events, no matter the scale, and this type of event proliferates without any action taken to remedy the situation, further criminal events are implicitly incentivised and tend to escalate in magnitude and frequency[19].

When applied to cybersecurity, the broken window theory not only refers to the reporting of crimes and their prosecution but more generally to the community's engagement in collaborating and standing against this type of event. Any cyber incident should therefore be reported and handled as much as possible to better grasp the current situation about cybercrime as well as transmit a message that no crime is deliberately left unaccounted for and unpunished.

This approach requires that citizens have access to, and are aware of, existing reporting mechanisms and that companies collaborate in reporting cyber incidents, as is the case in the data protection domain with the mandatory reporting of personal data breaches following the GDPR. Steps in this direction are also taken in the cases of cybersecurity incidents affecting essential digital service providers, including critical infrastructure (see the NIS Directive (European Commission, 2016c) and Cybersecurity Act (European Commission, 2017d)) and trust service providers (eIDAS regulation) (European Parliament and Council of the European Union, 2014).

7.1.4 Innovative techniques to fight cybercrime

The prosecution of cybercrime crucially depends on the capabilities of law enforcement to gather evidence, attribute attacks to their origin, analyse the crime and eventually bring perpetrators to justice. All of this constitutes increasing technical challenges due to the evolving technological landscape and, thus, to the means employed by cyber attackers to carry out their attacks. One striking example of obvious relevance to prosecution concerns the difficulties encountered in dealing with cyber criminals' increased use of encryption and anonymisation techniques, as previously pointed out.

On a broader scale, digital services, automation and AI techniques for labour-intensive tasks have become a new playground for both cybercrime and law enforcement.

In the long run, these developments not only assist law enforcement in the investigation of cybercrime but also in traditional forms of crime where digital content can also play a key role in the investigation.

Apart from the growing arsenal of tools attached to the aforementioned AI-driven cyber threat analysis, the most prevalent examples come from the wide fields of big data analytics, data mining and data visualisation, digital forensics and biometrics used for criminal investigative purposes. This encompasses very different applications, ranging from computer and hard-drive forensics, fraud detection in large databases, audio or image content analytics, social media filtering, personal identification techniques, automated surveillance or the early identification if criminal behaviour from predictive modelling.

7.2. Mitigating vulnerabilities

The exploitation of vulnerabilities is a crucial and necessary step in every cyber attack. In most cases, vulnerabilities exploited in such attacks are either of a technical nature (i.e. weaknesses in the software/hardware), human, or a combination of both. Whereas in many cases it is in the technical dimension, we should not forget that the human element is largely considered to be the weakest link in the security chain and must be properly addressed in risk-mitigation strategies (Sasse, Brostoff and Weirich, 2001).

A classical strategy to reduce cybersecurity risk involves deploying measures aimed at mitigating vulnerabilities, regardless of their nature.
In the following subsections, we present key strategies to act on the vulnerability dimension of the cybersecurity risk.

> “The human element is largely considered to be *the weakest link in the security chain.*”

It is important to understand that none of these strategies can be sufficiently effective when considered in isolation. Indeed, the principle of defence in depth (also known as the castle approach) states that multiple complementary countermeasures should be deployed in layers to exploit the overall effectiveness of their combination. This principle, which is clearly illustrated by the analogy of the castle with its surrounding moat and system of walls, is one of the main driving principles in the design of a cybersecurity strategy aimed at mitigating cybersecurity vulnerabilities.

7.2.1 Research and innovation in the cybersecurity industry

A wide range of products already exists[20] with proven efficacy in mitigating certain cybersecurity risks by identifying and preventing attacks. Cybersecurity products are assets in the arsenal of weapons that can be deployed to manage cybersecurity risk.

As the technical means used by cyber attackers to conduct attacks and their *modus operandi* continue to evolve, constant research and innovation are required in the cybersecurity industry to keep up with this evolution and develop more advanced and effective solutions.

7.2.2 Security-by-design and by-default in digital products and services

Security-by-design and security-by-default[21] are important guiding principles in cybersecurity. They are ultimately oriented towards the goal of reducing vulnerabilities in digital systems, services and processes.

The effective application of the security-by-design principle implies that non-functional security requirements are identified early in the development life cycle of new products and services and are properly prioritised with respect to functional ones. In industry, the main problem in the practical application of this principle lies precisely in the need to prioritise security requirements, which are often perceived as non-essential by industry as they are not seen as direct contributors to building value in the end product.

Possible incentives to remedy this situation include the introduction of cybersecurity requirements in regulations applicable to the development of products and services. In particular, liability regulations for products and services could further incorporate cybersecurity aspects. This would motivate industry to follow secure-by-design and by-default principles in the development of services and products. A similar approach has been adopted by the GDPR, whereby data controllers and data processors can be subjected to substantial fines if they fail to comply with the regulation on the protection of personal data.

This initiative could be complemented by offering users and companies in specific domains economic incentives to provide more secure products. An analogy can be made with tax incentives for electric vehicles in some countries (Figenbaum, Assum and Kolbenstvedt, 2015).

Technology also has a role to play in enabling the practical application of security-by-design principles. Operating systems and compilers have increasingly embedded countermeasures against entire classes of long-lived vulnerabilities. New generations of programming languages have been specifically designed for secure software development that can enable a new generation of more secure digital infrastructure, products and services.

7.2.3 Cybersecurity education

Proper dedicated skills are required to incorporate security along the whole development, release and life cycle of a service or product. Unfortunately, there is currently a shortage of dedicated professional profiles in the world, and thus also in the EU, which will continue to widen in the near future. This shortage in the cybersecurity workforce is expected to reach around 3.5 million worldwide by 2021 (Burrell, 2018).

In recent years, the cybersecurity-skill landscape has exploded into a complex ecosystem encompassing skill sets clustered in many different domains and abstraction layers. This has led to a specialisation in the domain of cybersecurity. This trend is likely to continue further due to the increasing digitalisation of industry and society and cybersecurity's multidisciplinary nature.

> By 2021, the shortfall in the cybersecurity workforce *is expected to be around 3.5 million worldwide.*

Certification programmes (e.g. certified information security manager (CISM) or certified information systems security professional CISSP)) are good indicators for qualified workers in cybersecurity.

Promoting dedicated career training (e.g. the above-mentioned certifications, information security training, cyber ranges, etc.) is also a favoured approach to disseminating cyber skills. The mid-term effect this can have is that it would empower anyone to improve security at their own level, or at least identify security weaknesses that need to be addressed. Indeed, to further embrace the principle of security-by-design and by-default, there is a need to embed cybersecurity skills in other careers and professions, such as engineering and medicine.

7.2.4 Cybersecurity certification and labelling

There are many definitions for the process of cybersecurity certification. A definition derived from NIST (Ron Ross et al., 2004) states that it is a comprehensive assessment of the management, operational and technical security controls in an ICT system. In other words, a specific model and version of an ICT system is submitted to a rigorous testing process against specific security and privacy requirements before being deployed in the market. In this way, an ICT system can be assessed against known vulnerabilities or to fulfil specific requirements driven by a regulation or by users' needs.

Cybersecurity certification can be considered the first line of defence to mitigate cybersecurity threats. Security requirements are derived from a risk analysis process, based on the *known* security needs and vulnerabilities.

Cybersecurity certification can be complemented by a cybersecurity label, which contains information that represents the value of one or more security attributes of the ICT system. Then, if a specific model and version of an ICT system successfully passes a cybersecurity certification process, it can be assigned a label. This would provide concise information – for example, an index to users detailing what security requirements the ICT system has. The concept of a label can be used to address the lack of transparency about the security features implemented by a manufacturer.

The concept of defining cybersecurity certification schemes at the European level and the label concept are key elements in the recently proposed Cybersecurity Act (European Commission, 2017d). However, there is still considerable work to do to address some aspects of cybersecurity certification, which are presented below.
First, even if the main security certification standard is the Common Criteria (CC), which is widely adopted worldwide, there are slightly different implementations in a Europe of Common Criteria. The SOG-IS[22] agreement partly addresses this lack of harmonisation and the Cybersecurity Act supports an extension of its mandate. Another challenge is the cost and time needed by the CC certification process, which can be an obstacle for small companies or ICT products requiring a rapid time to market (as in the IoT domain). To mitigate this challenge, more efficient certification processes for specific categories of ICT products have been proposed, like the French Certification de Sécurité de Premier Niveau (CSPN) which uses limited-time black-box testing.

A timely and cost-effective cybersecurity certification process is required in particular when an ICT product (model and version) is subjected to an update/modification. Software updates are often needed in modern ICT systems to add new features and improvements. In many cases, they are also needed to address new security vulnerabilities. Zero-day attacks or vulnerabilities discovered after the initial evaluation and deployment on the market may require redrafting the Protection Profiles in CC and the application of a new re-evaluation process. If there are major changes, a re-evaluation is needed, which can be a considerable burden for an ICT vendor.

> Vulnerabilities, particularly zero-day ones, *are bought and sold openly on the market.*

Subsequently, research and standardisation efforts could be directed at more effective and automated cybersecurity certification processes for both the initial evaluation and the re-evaluation process (Matheu-García et al., 2018).

7.2.5 Vulnerability management

Despite the best efforts in following security-by-default and security-by-design principles, vulnerabilities are likely to be discovered over time. It is important to prepare for those events by developing an effective strategy for the management of vulnerabilities during the life cycle of digital services and products.

The time elapsed between the discovery of a vulnerability in a given product or service and the release and deployment of security patches or a fix to address it is critical. This time frame defines the window of opportunity for threat actors to exploit that vulnerability to conduct a cyber attack. The security risk quickly arises when the vulnerability is discovered, evolves during this time frame, and only declines to previous levels when all vulnerable systems have been patched. It is worth noting that for some widespread vulnerabilities it could take years to reach that point.

Those vulnerabilities that have been discovered but remain unknown to the manufacturer, who therefore cannot address them, deserve particular attention. They are known as zero-days and are of significant value for all interested parties, the threat actors seeking to exploit them, and parties involved in cybersecurity protection (e.g. manufacturers) that want to fix them.

Vulnerabilities, and in particular zero-day ones, are sold and bought openly on the market. Their value depends on the importance of the vulnerability, and the type of client buying it (threat actors, vendors, intermediaries, etc.).

Indeed, proper management of vulnerabilities during the entire life cycle of a digital product or infrastructure is key to ensuring continuous and homogeneous cybersecurity coverage of digital systems and infrastructures. Initiatives should be extensively encouraged to cover the early discovery of vulnerabilities, the timely release of proper fixes, and the accurate and planned installation of the related patches.

Bounty programs and platforms are put in place by manufacturers and other interested parties, with the aim of identifying and fixing

vulnerabilities (Householder et al., 2017; Schaake et al., 2018). These types of programs are also referred to as white markets. Unfortunately, threat agents also act at this level, creating a black market of vulnerabilities that typically pays up to 10 times more than the white market (Schneier, 2019b; Ablon and Bogart, 2017), mainly because they trade in functional exploits rather than simply knowledge of them.

The vulnerabilities identified, either by a program or any other means (e.g. research community), are traditionally fixed through security patch/updates of the underlying software or by a replacement program where a local update is not feasible. Unfortunately, this critical process is not always performed well in practice.

For example, deploying patches and security updates for IoT devices still faces significant challenges. Many IoT devices (e.g. small sensors or actuators) lack a user interface to facilitate the installation of patches, or users are simply not provided with the proper means to manage the deployment of security updates.

Difficulty in deploying the update may also pose a problem. In the case of industry, installation of a new patch could require stopping the industrial process, which may not be possible on demand or could imply huge costs. Moreover, the deployment of the patch itself is not exempt from risks (i.e. the deployment of the patch might have undesirable side effects) and it has non-negligible costs for both the manufacturer of the vulnerable software and the user. For this reason, the definition of corporate patching strategies must be put in place at all levels.

7.3. Limiting impact through cyber resilience

In today's hyperconnected digital world, the question is no longer whether a cyber attack will take place, but rather when. In this context, society, governments, businesses and organisations should hope for the best but prepare for the worst. Preparedness is crucial to effectively mitigate potential impacts and prevent catastrophic consequences in the event of a cyber attack. For this reason, the definition of a strategy to guarantee appropriate incident response and fit-for-purpose resilience is another key element to mitigate the effects of cyber attacks.

When speaking of 'cyber resilience', we are essentially referring to the ability of a system to survive as a whole under adverse cyber events. It could be said that cyber resilience is the intersection of information security, business continuity and organisational resilience. According to most definitions, cyber resilience incorporates the ability *to prepare, withstand, recover and adapt to stresses, attacks or compromises on cyber resources* (Bodeau and Graubart, 2017; Larkin et al., 2015; Björck et al., 2015).

Cyber resilience can encompass ICT systems, entire organisations and even society as a whole. In the latter situation, the notion of resilience also encompasses a societal perspective, which links to society's capacity to survive adverse influences from its environment and still function and continue to deliver societal well-being to current and future generations (Bodeau and Graubart, 2017).

As previously mentioned, adverse cyber events are either intentional or unintentional, with cyber attacks obviously falling into the first category. Similarly, strategies to increase cyber resilience and thereby mitigate the potential impacts of cyber attacks can largely be classified under two distinct categories. The first one encompasses all measures designed to ensure a fast and effective response to withstand and recover from cyber incidents. The second includes those measures and preparations aimed at ensuring that the system will still be able to operate in adverse circumstances, enabling it to function in degraded conditions.

Figure 27 depicts the classical development of events in the case of a successful cyber attack.

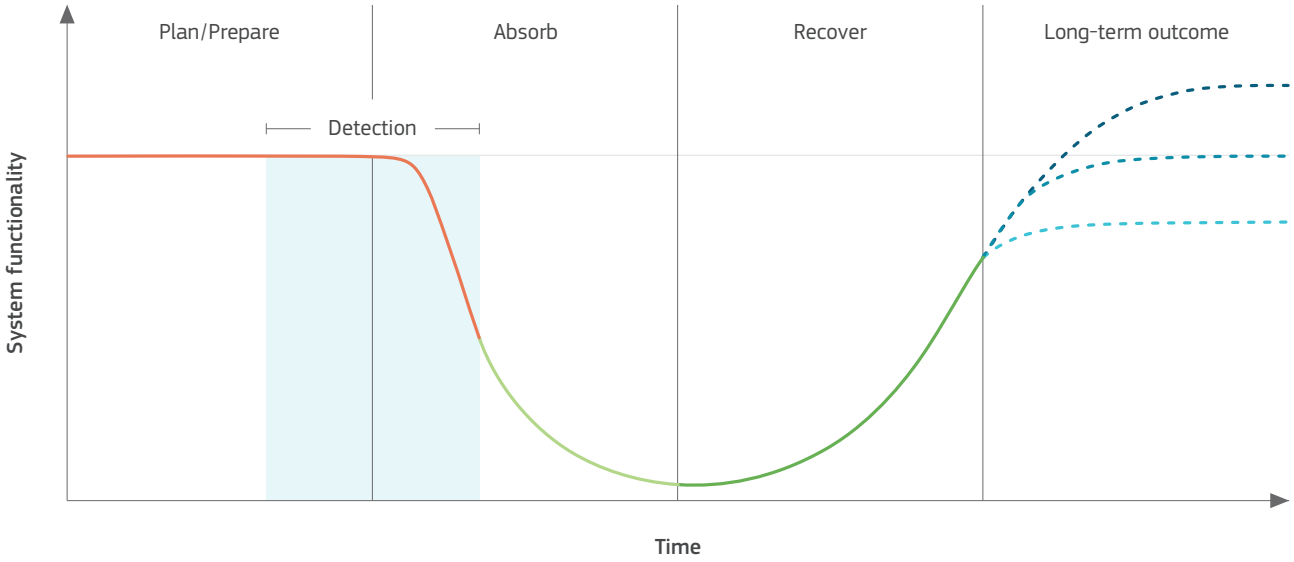


Figure 27: System functionality vs. resilience-response time

It shows a qualitative model of how system functionality[23] can evolve over time during a cyber attack. The time frame of a cyber attack is not always as precisely defined as for other types of adverse events, such as natural disasters. Therefore, there can be a significant delay between the beginning of a cyber attack and when its impact starts to be noticed. This delay may be desired by threat actors, as in the case of APT or industrial espionage.

Accordingly, early detection of cyber attacks is crucial to shorten such a potential hidden threat. Furthermore, it also ensures that the incident response phase, depicted in the second frame of *Figure 27,* will start as soon as possible to withstand and absorb the effects of the attack. The next phase is the recovery which aims to restore normal system functionality once the incident is under control. A good level of cyber resilience helps reduce periods during which system functionality is degraded and the level to which this occurs. Resilience also contributes to the system's capability to finally retrieve a normal level of functionality.

In addition, the incident response should not stop once the attack has been countered. A long-term approach should be initiated to understand the root causes for the success of an attack and what measures could have improved the system's overall resilience. In this way, it is even possible to consider that the post-incident functionality reaches a higher level than before, as the system would become more resistant to future attacks.

7.3.1 Rapid cybersecurity incident response

Rapid incident response to a cyber attack, coordination and CSIRT involvement are key elements of cyber resilience, helping to mitigate the impact of the attack (European Commission, 2017b).

No reaction is possible without detection. With the complexity and pervasiveness of our digital society, alongside the increasing sophistication and diversity of cyber attacks, it is increasingly likely that attacks are either detected too late or when the impact is already significant. Since most manual asynchronous checks of the logs are no longer feasible, automated real-time systems have to be employed these days, including antivirus, firewalls and intrusion-detection systems.

Following detection, the aim is to react properly to the attack to minimise both the decline in system functionality and the duration of

> Nowadays, it is increasingly likely that attacks *are either detected too late or when the impact is already significant.*

the attack so as to start the recovery phase as early as possible. However, simply stopping or isolating the attack may not be sufficient to initiate the recovery phase. A deep forensic analysis of the ICT system is typically required to identify the underlying mechanisms of the attack and restore the system to its original state. Depending on the complexity of the systems, this can become a lengthy procedure, while service downtimes have an ever-increasing impact in a hyperconnected world. It is crucial for all stakeholders to develop and maintain the capabilities to conduct such complex ICT forensics regardless of whether the attacked system is in a corporate setting, a public institution or of larger societal relevance, e.g. some part of the public infrastructure.

Detection, reaction and recovery can no longer be improvised or only start after the incident has occurred. Careful plans for all these activities must be devised and tested in advance to guarantee effectiveness and the shortest reaction time. Resources need to be allocated for incident-response activities. Staff must be properly educated to ensure they know how to react depending on the type of attack, and that they are aware of the designed continuity plan.

Generally speaking, highly skilled chief information security officers and trained and aware employees can reduce the overall reaction time as well as the efficiency of the incident response. Finally, swift information mechanisms concerning ongoing attacks are needed between all players who are potentially involved. This is of special importance if the attack is on a larger scale and where the system involved encompasses the sovereignty of several national players, e.g. different EU Member States (European Commission, 2017b).

7.3.2 Resilience by design

To ensure that the system is able to operate continuously under adverse conditions, resilience must be included in its design. This is essentially the same approach as underlies the principle of security-by-design. Cyber resilience considerations need to be integrated, maintained and updated, starting from the inception phase of any system and continuing throughout its entire life cycle.

Consistently followed design principles and technology measures are available and can help to increase the resilience of systems. However, more than ever, they need to be enforced, standardised and followed through for today's digital systems.

Increasingly complex digital systems with many different connections call for *diversity* and a *modular layered defence.* Reliance on a single type of component, defence approach, or emergency procedure should be avoided. The best option is a multiple of different mechanisms, located in different layers of the system so that, in the case of a lost outer component, such as a server, the core system could continue to function. On a larger scale, for instance in critical digital infrastructure, this depends significantly on considerations of strategic autonomy, where society should avoid dependence on single supply chains for critical systems.

Degraded-mode-functionality can also be achieved by adapting the technology of the system

components themselves to be more robust in adverse settings. Engineering should systematically consider the possibility of error and failures and offer alternative solutions in those scenarios rather than reinforcing a single safeguard leaving a system totally vulnerable when it fails.

Redundancy is a well-known key principle in engineering, including building in surplus and replicated system components together with back-up and fail-safe procedures. In particular for cyber resilience, redundancy should always be considered together with layered defence and diversity, since modern malware can often spread throughout homogeneously distributed resources (Bodeau and Graubart, 2017).

Such technological measures and remedies come at a cost both directly, by imposing higher investment costs in system design, and indirectly, by making the system more complex *per se,* possibly resulting in a loss of general robustness for a gain in resilience. These considerations need to be carefully weighed up and thought through.

Cyber resilience is not only a matter of engineering and technological system design. On the contrary, our society's resilience depends crucially on the behaviour of the individual citizen. In fact, cybersecurity is prominent among concerns expressed by European citizens (European Commission, 2011; 2016a). However, their online behaviour reveals a general liberality in the use of their personal data across online services or being over-trusting in digital interactions. Users generally lack the appropriate digital competences (skills, attitude, knowledge) (Carretero, Vuorikari and Punie, 2017) to implement an appropriate degree of individual security. Consequently, the same lack of knowledge and skills reduces the individual's resilience to cyber attack.

This cyber resilience will become even more important as we emerge from the COVID-19 pandemic. The huge upsurge in teleworking and distance learning has served to underline how essential such skills are for responsible online behaviour.

Raising awareness and improving the average skills in ICT while enhancing the transparency and usability of the technology may help to support a more resilient digital culture. In the first place, improving digital competences would help citizens to decrease online risks, reducing vulnerabilities and increasing the general level of cybersecurity among users. Developing an awareness culture would help to detect and withstand attacks and to take appropriate individual measures. This would reduce the impact on an individual, while collectively increasing the overall resilience. Improving the average ICT skills among users would also help to put in place quicker recovery mechanisms, thereby facilitating the restoration of a service, company, or infrastructure after an attack has taken place.

In the end, a collective culture of resilience will also help to maintain a minimum level of trust in services and products, and ultimately public digital infrastructure.

SUMMARY

Cybersecurity must advance alongside the technological shift to be able to guarantee a secure digital society. To do so, it has to utilise all six areas that have been mentioned throughout this report: ethics and rights, education, industry and digital services, research, a common culture of collaboration, and governance. Each area is not independent or stand-alone; they are all pillars for a new era of cybersecurity which will take advantage of the enormous technical opportunities that new technologies have to offer.

TOWARDS A MORE SECURE DIGITAL ECOSYSTEM

With the advent of full digitalisation, our society is embarking on an epochal shift, which promises to completely change our world and our way of life. This shift is so deep that it is not only technological but also, and most importantly, cultural.

Historically, the establishment of a security framework comprising policies, operating procedures, standards, guidelines, and systems governing, promoting and adding cybersecurity management, has been one of the most relevant components of this second step, acting as a stabiliser and guarantor for citizens' rights and safety.

If we look at the digital revolution and the number of new technologies and new keywords appearing daily, it might appear that we are still in the first phase of cultural change. However, if we observe the potential impact of the threats to which the rapid uptake of new digital technologies is potentially exposing citizens, a very different reality emerges. In effect, the pioneering phase of the current changes is either being completely skipped today or is evolving too fast so that huge parts of society are taking a leap forward without little in the way of harmonisation or finding a new equilibrium for societal models.

By helping to protect citizens, products and services, cybersecurity can be the cornerstone of the digital transformation. Without the guarantees provided by a strong cybersecurity position, all the promises and advantages of the digital revolution risk collapsing, leaving us in a worse position than before.

> Cybersecurity should be the cornerstone of the shift towards a new secure European digital society.

The overarching challenge for cybersecurity is to help build a 'secure digital society by design' with all the implications and difficulties that this infers.

8.1. Six areas of action

We have identified six clusters of possible action instrumental in the design of a secure European digital society:

- **Ethics and rights:** only by injecting ethics principles in the way in which cybersecurity will be implemented and administered will respect for human rights be guaranteed;
- **Education:** without true expertise it will not be possible to implement cybersecurity principles correctly in every corner of the digital society;

- **Industry and digital services:** only an industry fit for the cybersecurity challenge can hope to compete in the international arena;
- **Research:** the digital world is changing faster than anything else, hence, only equally evolving research and development in cybersecurity will ensure that a European digital society is prepared for the evolution of technologies;
- **Common culture of collaboration:** only a common ground in cybersecurity culture will allow cybersecurity measures and behaviour to flourish in every sector;
- **Governance:** to ensure that cybersecurity is considered at all relevant stages in policymaking. A coordinated framework to ensure the full alignment of policy initiatives and actions at EU and Member-State level in the different domains listed so far will be key to assuring the harmonisation and homogenisation of cybersecurity across Europe.

In the next part of this section, we will briefly explore ideas and suggested actions needed per identified area to quickly boost the creation of a secure European digital society.

8.1.1 Ethics and rights

The current situation is awash with questions about fundamental rights and social norms in the digital age; how to properly enforce elements such as rights to privacy, protection of personal data, the freedom of expression and thought; and how to derive proper ethical guidelines for behaviour in the digital age, on a societal level as well as on an individual or professional level. **All of these impact on cybersecurity, both fundamentally as a discipline and in practice.**

There is a long history of political discussion about how to balance and weigh rights, such as those concerning privacy and data protection, against some cybersecurity issues. However, cybersecurity as a discipline has no choice but to confront such issues. Thus, **there is not only a need for open debate and eventual decisions on how to implement the law, but also for clarity, guidelines, concrete legal frameworks and best practices that will ensure both adherence to the law and ethically acceptable behaviour when practising cybersecurity.**

The set of concrete issues is large and constantly growing. Some problems are connected to essentially unsolved larger problems concerning the globalised digital era. How to implement cybersecurity measures combating hate speech or fake information campaigns without infringing on a citizen's right to freedom of expression? How to handle grey zones in the usage and dissemination of technology and information that can potentially be misused? How can vulnerability disclosure policies (Schaake et al., 2018; CERT-EU; CIO Platform Nederland and Rabobank, 2016) – also known as the 'vulnerabilities equities process' debate in the USA – optimally balance the needs of all stakeholders? Others stem more from legal uncertainties of recently adapted laws, and especially in learning how to adapt practices in cybersecurity so that they comply with changing

laws. A prominent example is the GDPR, for which many best practices for experts still need to be established in detail. How can a clear framework for coordinated vulnerability disclosure be set up? How can the right balance be ensured in the processing of possible personal data necessary for certain cybersecurity operations? **It is clear that all these issues require a collaborative effort by policymakers, legal experts, researchers, business leaders and cybersecurity experts to provide a growing sense of legal and ethical security.**

8.1.2 Lifelong education and the need for public-interest technologists

There is a growing demand for skilled people in the field of cybersecurity to which, unfortunately, the job market is unable to respond. One visible consequence is the current 1 million shortfall in employees which is expected to grow in the future.

A short-term answer to this problem is to **encourage and support active workers to engage in a continuing education programme related to cybersecurity,** leading, for example, to cybersecurity certification like those already recognised by the industry (e.g. CISSP or certified ethical hacker (CEH)). **A European certification scheme should be designed** to oversee professional development and therefore better address the type of expertise currently needed.

The law-enforcement agencies sector is a good example of where continuing education and training on cybercrime and cybersecurity are key. In this context, one of the priorities of the Global Cybercrime Certification Project, launched in 2014, is to create a framework for certification of European cybercrime investigators and prosecutors by providing professional development in the area of transnational aspects of cybercrime.

The value of hands-on experience such as *cyber ranges* must be emphasised at all skill levels. By practising in more realistic environments, professionals gain technical insights and grasp challenges and solutions more readily. Experts benefit from such exercises by maintaining their knowledge and skills at a very high level. Such continuing professional education should be encouraged by companies through recognition or rewards, as they definitely benefit from the stronger cybersecurity skills among their employees.

A longer-term solution is to **integrate the teaching of cybersecurity skills at all levels of education.** It would serve the digital world as a whole to see cybersecurity becoming part of the global culture,

in general, and given its multifaceted nature, many areas of activity would benefit from this knowledge. In addition, this could increase the appeal of a career as cybersecurity expert to the younger members of society. There should also be a concerted effort to close the gender balance gap as women currently remain in the minority in the cybersecurity profession.

As a complementary benefit, an increase in citizens' digital competencies is a move towards a more secure digital society. End-users will become able to recognise unsecure software and bad digital habits, making them fully aware of their associated risks. Armed with such knowledge, they will be in a better position to judge and make an informed choice as to what products and services they would like to use. The demand for these would naturally be stimulated, thereby creating an incentive for the industry to offer more and better digital products and services.

In addition to the above-mentioned needs, there is a strong demand for public-interest technologists in the cybersecurity domain. Defined by Bruce Schneier as 'people who combine their technological expertise with a public-interest focus: by working on tech policy, by working on a tech project with a public benefit, or by working as a traditional technologist for an organisation with a public benefit', such profiles are required across the policy spectrum wherever cybersecurity and policy intersect. Within the same mindset, the 2016 report (Freedman et al., 2016) 'A Pivotal Moment – Developing a New Generation of Technologists for the Public Interest', concludes: 'But public interest organisations are facing a talent pipeline crisis: there are not enough technologists working or interested in joining public interest fields to meet growing demand'.

> "In the new open digital world, *there are simply no more clear walls to defend or single doors to close.*"

8.1.3 Industry of products and services

Creating incentives is important to ensure that industry applies security-by-design and security-by-default principles in the development of new products, from their design phase and across their life cycle. In parallel to rewarding motivation – like that based on the demand from informed citizens for more secure products – industries should be penalised for breaching their obligations. **Liability legislation should be developed for products and services from a cybersecurity perspective.** A cybersecurity certification of processes and professional skills in cybersecurity (such as the ISO 27005 series) is particularly relevant to ensure cybersecurity activities are assigned to capable professionals who guarantee their effectiveness and take responsibility for undesirable outcomes. Further developments of such policy initiatives to establish a liability regime creates a strong push for industry to prioritise cybersecurity requirements in their products, services and processes.

It is equally important to promote work on standardisation and recognise its importance in designing more secure products and services, anticipating future cybersecurity risks, by acting initially in the very early phase of their design. **Solid and secure standards must be developed and applied** as a strategic foundation to support a more secure and safer future ecosystem. Those standards should foresee that the **interoperability of products and services is**

> *A lack of interoperability has a negative impact on cybersecurity.*

systematically adopted by industry and enforced across all relevant layers of existing systems. Indeed, the lack of interoperability has a negative impact on cybersecurity as measures that are not interoperable across devices are often ignored and unnecessary dependencies are introduced thereby increasing risk. The definition of a common procurement language and codified service-level agreements could also greatly enhance the security level of product supply and value chains.

Industry's efforts should go beyond integrating security into a product or service. Vulnerabilities will always exist and the security of the underlying system and its users relies even more on the intentions, malicious or otherwise, of whoever is first to identify a vulnerability. An effective strategy is essential to manage vulnerabilities during the complete life cycle of products and services, including the shaping of fairly balanced vulnerability disclosure policies and the launching of regular bug bounty campaigns based, for instance, on tax incentives. Furthermore, effective means must be put in place to minimise the time between the discovery of a vulnerability and the release of security patches to fix it. Also in this context, **making companies liable for the damage resulting from their security products** would incentivise industry to improve the management of the vulnerability of their services and products.

8.1.4 Improved coordination of research

If the mission of cybersecurity is that of 'providing protection' for the continuously evolving digital society, it is obvious that it must also evolve at the same speed or even faster to be able to anticipate threats which may arise, thereby necessitating further research in the field.

In 2018, the impact assessment conducted on the setting up of the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres provides a detailed and complex picture of the situation. In general, this assessment shows a research community vibrant, productive, and recognised worldwide. However, two concerns raised are the lack of critical mass in some research fields and the lack of industrial collaboration.

The lack of a strong European cybersecurity industry further underlines the need for intervention in this area. **The urgency is to**

improve the magnitude of technology and innovation transfer to the market using research project outputs. This is also an extremely relevant critical issue from a European strategic autonomy perspective since it introduces a dependency on products and services not available in the EU's internal market.

These difficulties probably have their origins in: (1) the systemic lack of resources; (2) different priority agendas at the level of public investments across Member States; (3) the poor incentives for private investments in cybersecurity research and innovation; and (4) the shortage of advanced skills in the sector. As regards these last considerations, new EU measures for better coordination and cooperation must be defined.

There is also a need for better coordination of cybersecurity research funding across the EU to ensure focus areas are properly addressed and not fragmented across many different research projects. For example, the funding strategy should support the sharing of highly expensive infrastructures, as in the European Open Laboratory initiative. Finally, cooperation among funding bodies and recipients on the co-design of research plans is needed to ensure relevant cybersecurity research areas are effectively taken into consideration.

8.1.5 A common culture of collaboration in cybersecurity

Companies, governments, organisations and, more broadly, citizens need to embrace a culture of cybersecurity. Cross-fertilisation among all these groups would make the difference in leading the digital society to another level of safety. For example, the connections between cybersecurity, privacy and data protection offer synergies that should be exploited in order to benefit from common goals, optimise resources and maximise the effectiveness of actions. Cross-fertilisation can also lead to better-trained professionals and more educated and aware users able to recognise and understand the intricate interdependencies that exist between them, ultimately leading to safer digital products and services and a healthier online ecosystem.

> *"To release the full potential of cyber threat intelligence, the sharing of data among pertinent actors must be facilitated."*

One of the key elements promoting this cybersecurity community is reinforced information management and sharing among all the sub-communities. Knowledge is crucial in cybersecurity; one explicit example is **cyber threat intelligence** which aims to gather information from all possible means to better tailor mitigation techniques and resilience mechanisms. Clearly, to be effective, cyber threat intelligence requires access to the maximum of knowledge, currently maintained mainly within their corresponding silos. For the full potential of cyber threat intelligence to be realised, the sharing of data among pertinent actors must be facilitated. All EU Member States will strongly benefit from closer cooperation among them. Strong cyber threat intelligence will also empower law enforcers and national defence services, thereby establishing deterrence in the digital world.

European legislation, like the NIS Directive and the Cybersecurity Act, is already paving the way towards nourishing the creation of several Information Sharing and Analysis Centers (ISACs) and public-private partnerships within the EU. The creation of sectorial ISACs at the national level could accelerate the collaboration between industry, government and law enforcement (ENISA, 2020a).

To this end, **three main pillars should be established.** A *common strategy* must be defined, including all willing actors, to clarify what can be achieved and how it has to be done. *Interoperability* needs to be considered from the very beginning to facilitate all the exchanges and standardise the way to process the information gathered. *Implementation* of the system must ensure the security and privacy of all the gathered data without hindering its development.

The establishment of a general culture of collaboration in this field would have a positive cascading effect on all areas. Encouraging, or obliging the reporting of any cyber incident, would facilitate the setting up of better safeguards, benefit other players, and more broadly nurture other communities, thereby improving the overall situation. An action toward this goal is **the establishment of a European central platform for vulnerability management** coordinating and encouraging the efforts of the cybersecurity community to improve the overall security level of the digital world.

In the last years many advocated, in this context, on the need for a 'Digital Geneva Convention', covering the cyberspace. Many claimed that the Geneva Convention was conceived in 1949, for completely different reasons and there is no need to extend it to cyberspace. Nevertheless, as demonstrated by the cyber threats raised during the COVID-19 crisis, it is now the time for an international reflection on the digital space, its protection and the rules governing its security.

8.1.6 Ensure secure policy by design

We need to go further. Instead, we should be **building a secure digital European society with the security-by-design principle understood as a general philosophy for the digital era,** not simply as a mere product-design practice.

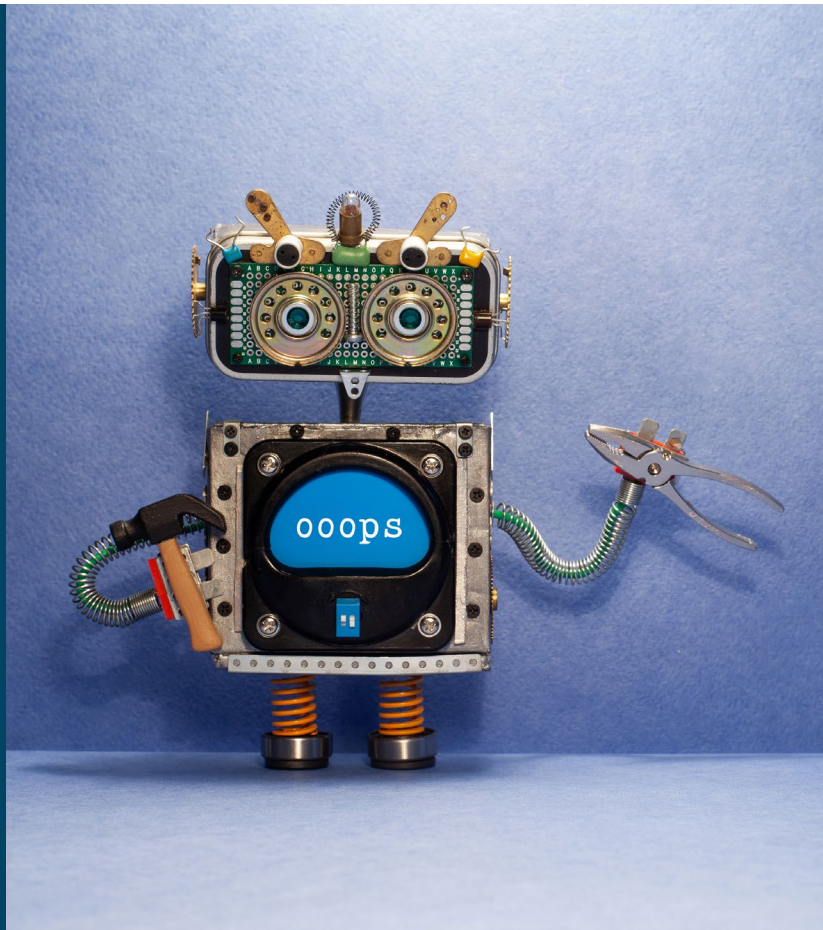
Consequently, we should also **ensure that our governance and policymaking practices start to adhere to this principle.** As digital permeates across more and more areas of policy and law making, practices should **guarantee that cybersecurity considerations are built into the policymaking and governance processes from the outset.**

To this end, **measures should be considered to develop a coordinated European framework for the full alignment of cybersecurity policy initiatives and actions at EU and Member-State level.** It should cover all the relevant areas listed in this chapter, ranging from fundamental rights to international collaboration. Such an initiative will be key in ensuring the harmonisation and homogenisation of cybersecurity across Europe and will be a significant step towards building a secure digital society for all European citizens.

8.2. Elevating Europe to Cybersecurity 2.0 – our digital anchor

The European Commission has proposed a digital transformation that works for all. Within this ambitious strategy, there is a strong acknowledgement that such a transformation has cybersecurity embedded at its core. We have seen in this report that it covers a wide range of issues from trust in digital products, ensuring relevant cooperation between Member States, developing cyber resilience, deploying new tools against cyber criminals, to raising citizens' awareness of cybersecurity. We have also witnessed the ever-present vulnerabilities to malicious cyber attacks, illustrated in particular by the weaknesses exploited during the COVID-19 pandemic. Implementing the above recommendations, with cybersecurity as our digital anchor, will help our society achieve a successful digital transformation.

> *"In a new reality where physical and digital blend together, cybersecurity is the trust anchor of our society."*



LIST OF ABBREVIATIONS

AI	Artificial intelligence
APT	Advance persistent threats
ARPANET	Advanced Research Projects Agency Network
CaaS	Crime-as-a-Service
CC	Common Criteria
CEH	Certified ethical hacker
CISM	Certified information security manager
CISSP	Certified information systems security professional
CRI	Cyber Readiness Index
CSPN	Certification de Sécurité de Premier Niveau
CSIRT	Computer security incident response team
CTI	Cyber threat intelligence
DDoS	Distributed denial of service
DNS	Domain name system
DNSSEC	Domain name system security extensions
DoD	Department of Defense
DoS	Denial of service
EC3	European Cybercrime Centre
ECSO	European Cyber Security Organisation
ENISA	European Union Agency for Cybersecurity
EU	European Union
FSTEK	Federal Service for Technical and Export Control
GDPR	General Data Protection Regulation
HLEG	High-level Expert Group
ICT	Information and communications technology
IEC	International Electrotechnical Commission
IOCTA	Internet Organised Crime Threat Assessment
IoMT	Internet of Medical Things
IoT	Internet of Things
IP	Internet protocol
ISAC	Information Sharing and Analysis Center
ISMS	Information security management system
ISO	International Organization for Standardization
ITU	International Telecommunications Union
JRC	Joint Research Centre
MDR	Medical Devices Regulation
MS	Member State

NAO	National Audit Office
NATO	North Atlantic Treaty Organization
NCSS	National cyber security strategies
NHS	National Health and Social Care system
NIS	Network and information systems
NIST	National Institute of Standards and Technology
NISTIR	NIST Interagency/Internal Report
OECD	Organisation for Economic Co-operation and Development
OS	Operating system
PII	Personally identifiable information
PPP	Public-private partnership
SME	Small and medium-sized enterprise
SSL	Secure sockets Layer
TOE	Target of evaluation
USA	United States of America
VPN	Virtual Private Network
WEF	World Economic Forum
WHO	World Health Organization
WWW	World Wide Web

GLOSSARY

Accessibility
(ISO/IEC TR 13066-2:2016) Degree to which a computer system is easy to use by all people, including those with disabilities.

Access control
(ISO/IEC 27000) Means to ensure that access to assets is authorised and restricted based on business and ßsecurity requirements.
(FIPS 201-1) The process of granting or denying specific requests: 1) for obtaining and using information and related information-processing services; and 2) to enter specific physical facilities (e.g. federal buildings, military establishments, and border-crossing entrances.

Accountability
(ISO/IEC 2382:2015) Property that ensures that the actions of an entity may be traced uniquely to that entity.

Acquisition
(NIST SP 800-160) Process of obtaining a system, product or service.

Assurance
(ISO/IEC 15026) Grounds for justified confidence that a claim has been or will be achieved. Note 1: assurance is typically obtained relative to a set of specific claims. The scope and focus of such claims may vary (e.g. security claims, safety claims) and the claims themselves may be interrelated. Note 2: assurance is obtained through techniques and methods that generate credible evidence to substantiate claims.

Audit
(ISO/IEC 27000:2016) Systematic, independent and documented process for obtaining audit evidence and evaluating it objectively to determine the extent to

which the audit criteria are fulfilled. (An audit can be an internal audit, an external audit, or a combined audit.) (ISA 62443-1-2) Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies or procedures.

Asymmetric cryptographic algorithm
(NIST SP 800-133) A cryptographic algorithm that uses two related keys, a public key and a private key, both of which have the property that determining the private key from the public key is computationally infeasible – also known as a public-key algorithm.

Attack and cyber attack
Attack: (ISO/IEC 27000:2016) attempt to destroy, expose, alter, disable, steal or gain unauthorised access to or make unauthorised use of an asset.
Cyber attack: (NIST SP 800-53 Rev. 4) an attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/ infrastructure, or destroying the integrity of the data, or stealing controlled information.

Authentication
(ISO/IEC 27000) Provision of assurance that a claimed characteristic of an entity is correct.
(FIPS 200) Verifying the identity of a user, process or device, often as a prerequisite to allowing access to resources in an information system.

Availability
(ISO/IEC 27000:2016) Being accessible and usable upon demand by an authorised entity.
(FIPS 200) Ensuring timely and reliable access to and use of information.

Biometrics
(ISO/TR 18307:2001) Use of specific attributes that reflect unique personal characteristics, such as a fingerprint, an eye blood-vessel print, or a voice print, to validate the identity of entities.(NIST SP 800-63-3) Automated recognition of individuals based on their biological and behavioural characteristics.

Certification
(Proposal for a Regulation of the European Parliament and of the Council on ENISA, the 'EU Cybersecurity Agency') Certification comprises the formal evaluation of products, services and processes by an independent and accredited body against a defined set of criteria standards and the issuing of a certificate indicating conformance. Certification serves the purpose of informing and reassuring purchasers and users about the security properties of the products and services that they buy or use.
(FIPS 200) A comprehensive assessment of the management, operational and technical security controls in an information system, made in support of security accreditation, to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.

Collection
(ISO/IEC 27037:2012) Process of gathering the physical items that contain potential digital evidence.

Confidentiality
(ISO/IEC 27000:2016) Whereby information is not made available or disclosed to unauthorised individuals, entities or processes.
(FIPS 200) Preserving authorised restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.

Conformity
(ISO/IEC 27000:2016) Fulfilment of a requirement.

Cryptanalysis
(ISO/IEC 7498-2:1989, definition 3.3.18 and ISO/IEC 18033-1 2015) The analysis of a cryptographic system and/or its inputs and outputs to derive confidential variables and/or sensitive data, including cleartext.
(NIST SP 800-57 Part 1 Rev. 4) Operations performed to defeat cryptographic protection without initial knowledge of the key employed in providing the protection.

Cryptology
(Computer Security, Dieter Gollmann, John Wiley and Sons) Cryptology groups together the definition of cryptography (i.e. 'the science of secret writing') and cryptanalysis (i.e. the science of 'breaking ciphers').

For the scope of this taxonomy, this domain includes not only the mathematical foundations but also the technical implementations of cryptographic algorithms and architectures, as well as the implementation of cryptanalytic methodologies, techniques and tools. (CNSSI 4009-2015) The mathematical science that deals with cryptanalysis and cryptography.

Cryptographic hash function
(NIST SP 800-106) A function that maps a bit string of arbitrary length to a fixed-length bit string and is expected to have the following three properties: 1) collision resistance (see collision resistance); 2) preimage resistance (see preimage resistance); and 3) second preimage resistance.

Cybercrime
(ISO/IEC 27032:2012) A criminal activity in which services or applications in cyberspace are used for or are the target of a crime, or where the cyberspace is the source, tool, target or place of a crime.

Cybersecurity
(ISO/IEC 27032:2012) Preservation of confidentiality, integrity and availability of information in cyberspace. (NISTIR 8183) The process of protecting information by preventing, detecting and responding to attacks. (ITU-T, X.1205) The collection of tools, policies, security concepts, security safeguards, guidelines, risk-management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organisation and users' assets.

Cyberspace
(ISO/IEC 27032:2012) The complex environment resulting from the interaction of people, software and services on the internet by means of technology devices and networks connected to it, which does not exist in any physical form. (NIST SP 800-30 Rev. 1) A global domain within the information environment comprising the interdependent network of information system infrastructures, including the internet, telecommunications networks, computer systems, and embedded processors and controllers.

Data
(ISO/IEC 27000:2016) Collection of values assigned to base measures, derived measures and/or indicators. (NIST SP 800-88 Rev. 1) Pieces of information from which 'understandable information' is derived.

Digital evidence
(ISO/IEC 27037:2012) Information or data, stored or transmitted in binary form that may be relied on as evidence.

Digital signature
(NIST SP 800-63-2) An asymmetric key operation where the private key is used to digitally sign data and the public key is used to verify the signature. Digital signatures provide authenticity protection, integrity protection, and non-repudiation.

Digital rights management
(ISO/IEC 5127:2017) Digital technology that is separate to the product form of a specific digital publication and which is used to control access to content.

Distributed system
(Coulouris, George, Jean Dollimore, Tim Kindberg and Gordon Blair (2011), Distributed Systems: Concepts and Design (5th edition), Boston, Addison-Wesley, ISBN 0-132-14301-1) A distributed system is a model in which components located on networked computers communicate and coordinate their actions by passing messages. In this context, cybersecurity deals with all aspects of coordination, message integrity, availability and (if required) confidentiality. Message authentication is also within the scope.

Documented information
(ISO/IEC 27000:2016) Information required to be controlled and maintained by an organisation and the medium in which it is contained.

eIDAS
(Regulation (EU) No 910/2014) EU regulation proposed to ensure 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.

Effectiveness
(ISO/IEC 27000:2016) The extent to which planned activities are realised and planned results achieved.

Event
(ISO/IEC 27000:2016) Occurrence or change in a particular set of circumstances.

Executive management
(ISO/IEC 27000:2016) Person or group of people who have been delegated responsibility by the governing body to implement strategies and policies to accomplish the purpose of the organisation.

Governance of information security
(ISO/IEC 27000:2016) A system by which an organisation's information security activities are directed and controlled.

Governing body
(ISO/IEC 27000:2016) Person or group of people who are accountable for the performance and conformance of the organisation.

Hash function
(ISO/IEC 10118-1:2016) Hash functions map strings of bits of variable (but usually upper-bounded) length to fixed-length strings of bits, using a specified algorithm. They can be used to reduce a message to a short imprint for input into a digital signature mechanism, and to commit the user to a given string of bits without revealing this string.

Human error
Mistakes that unwittingly create opportunities for cyber attackers to exploit.

Identity
(NIST SP 800-79-2) The set of physical and behavioural characteristics by which an individual is uniquely recognisable.

Identity management
(ISO/IEC 24760-1:2011) Processes and policies involved in managing the life cycle and value, type and optional metadata of attributes in identities known in a particular domain.

Indicator
(ISO/IEC 27000:2016) A measure that provides an estimate or evaluation of specified attributes derived from an analytical model with respect to defined information needs (2.31).

Identification
(NIST SP 800-79-2) The process of discovering the true identity (i.e. origin, initial history) of a person or item from the entire collection of similar people or items.
Information security
(FIPS 200) The protection of information and information systems from unauthorised access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity and availability.

Information security continuity
(ISO/IEC 27000:2016) Processes and procedures for ensuring continued information security operations.

Information security incident
(ISO/IEC 27000:2016) A single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security.

Information security incident management
(ISO/IEC 27000:2016) Processes for detecting, reporting, assessing, responding to, dealing with, and learning from information security incidents.

Information system
(ISO/IEC 27000:2016) Applications, services, information technology assets, or other information-handling components.

Integrity and data integrity
Integrity: (ISO/IEC 27000:2016) demonstrating accuracy and completeness.
Data integrity: (NIST SP 800-63-3) whereby that data has not been altered by an unauthorised entity.

ISMS project
(ISO/IEC 27000:2016) Structured activities undertaken by an organisation (definition 2.57) to implement an ISMS.

Key management
(ISO/IEC 11770-1:2010 PART 1, definition 2.28)
Administration and use of generation, registration, certification, deregistration, distribution, installation, storage, archiving, revocation, derivation and destruction of keying material in accordance with a security policy.

Level of risk
(ISO/IEC 27000:2016) Magnitude of a risk (definition 2.68) expressed in terms of the combination of consequences (definition 2.14) and their likelihood.

Likelihood
(ISO/IEC 27000:2016) The chance of something happening.

Malware
(ISO/IEC 27033-1:2015) Malicious software designed specifically to damage or disrupt a system, attacking confidentiality, integrity and/or availability.
(NIST SP 800-53 Rev. 4) Software or firmware intended to perform an unauthorised process that will have an adverse impact on the confidentiality, integrity or availability of an information system. A virus, worm, Trojan horse, or other code-based entity that infects a host. Spyware and some forms of adware are also examples of malicious code.

Management system
(ISO/IEC 27000:2016) A set of interrelated or interacting elements of an organisation to establish policies, objectives and processes to achieve those objectives.

Message authentication
(ISO/IEC 9797-1) Process to authenticate a message, often done through message authentication codes (string of bits which is the output of a MAC algorithm).
(NIST SP 800-152) A process that provides assurance of the integrity of messages, documents or stored data.

Monitoring
(ISO/IEC 27000:2016) Determining the status of a system, a process (definition 2.61) or an activity.
(NIST SP 800-160) Continual checking, supervising, critically observing or determining the status in order to identify change from the performance level required or expected.

Network security
(ISO/IEC TR 29181-5) This is concerned with the hardware, software, basic communication protocols, network frame structure, and communication mechanisms factors of the network. Information security in the network context deals with data integrity, confidentiality, availability and non-repudiation while it is being sent across the network.

Non-conformity
(ISO/IEC 27000:2016) Non-fulfilment of a requirement.

Non-repudiation
(ISO/IEC 27000:2016) The ability to prove the occurrence of a claimed event for action and its originating entities.

Organisation
(ISO/IEC 27000:2016) Person or group of people with their own functions with responsibilities, authorities and relationships to achieve their objectives.

Outsource
(ISO/IEC 27000:2016) An arrangement whereby an external organisation performs part of an organisation's function or process.

Performance
(ISO/IEC 27000:2016) A measurable result.

Personally identifiable information (PII)
(ISO/IEC 24745:2011) Any information that identifies or can be used to identify, contact, or locate the person to whom such information pertains, from which identification or contact information of an individual person can be derived, or that is or might be directly or indirectly linked to a natural person.

Policy and security policy
Policy: (ISO/IEC 27000:2016) intentions and direction of an organisation as formally expressed by its top management.
Security policy: (NIST SP 800-37 Rev. 1) a set of criteria for the provision of security services.

Post-quantum cryptology
(NISTIR 8105) The goal of post-quantum cryptography (also called quantum-resistant cryptography) is to develop cryptographic systems that are secure against both quantum and classical computers and can interoperate with existing communication protocols and networks.

Preservation
(ISO/IEC 27037:2012) A process to maintain and safeguard the integrity and/or original condition of the potential digital evidence.

Process
(ISO/IEC 27000:2016) A set of interrelated or interacting activities which transforms inputs into outputs.

Protection profile
(ISO/IEC 15408-1:2009) Implementation-independent statement of security needs for a TOE type.

Privacy
(ISO/TS 25237:2008) Freedom from intrusion into the private life or affairs of an individual when that intrusion results from the undue or illegal gathering and use of data about that individual.
(Westin, A., 'Privacy and Freedom', Atheneum, New York, 1967) Privacy is the claim of individuals, groups or institutions to determine for themselves when, how, and to what extent information about them is communicated to others. Viewed in terms of the relation of the individual to social participation, privacy is the voluntary and temporary withdrawal of a person from the general society through physical or psychological means, either in a state of solitude or small-group intimacy or, when among larger groups, in a condition of anonymity or reserve.

Privacy enhancing technology (PET)
(ISO/IEC 29100:2011) Privacy control, comprising ICT measures, products or services, which protects privacy by eliminating or reducing PII or by preventing unnecessary and/or undesired processing of PII, all without losing the functionality of the ICT system.

Pseudonym
(RFC 6973) A name assumed by an individual in a certain context, unrelated to the individual's personal names known by others in that context, with the intention of not revealing the individual's identities associated with his or her other names. Pseudonyms are often not unique.

Pseudonymous
(RFC 6973) A property of an individual whereby that individual is identified by a pseudonym.

Pseudonymity
(ISO/IEC 25237:2017) A particular type of de-identification that both removes the association with a data subject and adds an association between a particular set of characteristics relating to the data subject and one or more pseudonyms.
(RFC 6973) The state of being pseudonymous.

Quantum cryptography
(ISO/TS 80004-12:2016(en), 6.6) The use of quantum phenomena for cryptographic purposes.

Reliability
(ISO/IEC 27000:2016) Having the property of consistent intended behaviour and results.

Reputation
(ISO/IEC 23006-4:2013) A measure of the credibility of, or the possibility for (e.g. legal) a user to be a party to a transaction.

Requirement
(ISO/IEC 27000:2016) The need or expectation that is stated, generally implied or obligatory.

Residual risk
(ISO/IEC 27000:2016) The risk remaining after risk treatment.

Review
(ISO/IEC 27000:2016) An activity undertaken to determine the suitability, adequacy and effectiveness of the subject matter to achieve the established objectives.

Risk and cyber risk
Risk: (ISO/IEC 27000:2016) effect of uncertainty on objectives. In the context of information security (2.33) management systems, information security risks can be expressed as effect of uncertainty on information security objectives. Information security risk is associated with the potential that threats will exploit vulnerabilities of an information asset or group of information assets and thereby cause harm to an organisation.
Cyber risk: (NISTIR 8183) Risk of financial loss, operational disruption, or damage from the failure of the digital technologies employed for informational and/or operational functions introduced to a manufacturing system via electronic means from the unauthorised access, use, disclosure, disruption, modification, or destruction of the manufacturing system.

Risk acceptance
(ISO/IEC 27000:2016) An informed decision to take a particular risk.

Risk analysis
(ISO/IEC 27000:2016) A process to comprehend the nature of risk and to determine the level of risk.

Risk assessment
(ISO/IEC 27000:2016) The overall process of risk identification, risk analysis and risk evaluation.

Risk evaluation
(ISO/IEC 27000:2016) The process of comparing the results of risk analysis with risk criteria to determine whether the risk and/or its magnitude is acceptable or tolerable.

Risk identification
(ISO/IEC 27000:2016) The process of finding, recognising and describing risks.

Risk management
(ISO/IEC 27000:2016) Coordinated activities to direct and control an organisation with regard to risk.

Risk management process
(ISO/IEC 27000:2016) Systematic application of management policies, procedures and practices to the activities of communicating, consulting, establishing the context of and identifying, analysing, evaluating, treating, monitoring and reviewing risk.

Risk owner
(ISO/IEC 27000:2016) A person or entity with the accountability and authority to manage a risk.

Risk treatment
(ISO/IEC 27000:2016) A process to modify risk (e.g. avoidance, removal, change, share, retain, mitigation).

Scale
(ISO/IEC 27000:2016) An ordered set of values, continuous or discrete, or a set of categories to which the attribute is mapped.

Security implementation standard
(ISO/IEC 27000:2016) A document specifying authorised ways to achieve security.

Security management policy
(ISO/IEC 28000:2007) An organisation's overall intentions and direction related to the security and the framework for the control of security-related processes and activities that are derived from and consistent with the organisation's policy and regulatory requirements.

Security measurement
(NIST SP800-55) Information security measures are used to facilitate decision-making and improve performance and accountability through the collection, analysis and reporting of relevant cybersecurity performance-related data. The purpose of measuring performance is to monitor the status of measured activities and facilitate improvement in those activities by applying corrective actions based on observed measurements.

Security-relevant event
(NISTIR 5153) Any event that attempts to change the security state of the system (e.g. change access controls, change a user's security level, change a user's password). Also, any event that attempts to violate the security policy of the system (e.g. too many logon attempts).

Security target
(ISO/IEC 15408-1:2009) Implementation-dependent statement of security needs for a specific identified TOE.

Symmetric cryptographic algorithm
(FIPS 140-2) A cryptographic algorithm that uses a single key (i.e. a secret key) for both encryption and decryption.

Threat and cyber threat
Threat: (ISO/IEC 27000:2016) potential cause of an unwanted incident, which may result in harm to a system or organisation.
Cyber threat: (SP 800-30 Rev. 1) any circumstance or event with the potential to adversely impact organisational operations (including mission, functions, image, or reputation), organisational assets, individuals, other organisations, or the nation through an information

system via unauthorised access, destruction, disclosure, modification of information, and/or denial of service.

Testing
(ISO/IEC 29109-1:2009) Determination of one or more characteristics of an object of conformity assessment, according to a procedure.

Top management
(ISO/IEC 27000:2016) Person or group of people directing and controlling an organisation at the highest level.

Trust
(ISO/IEC 25010:2011) The degree to which a user or other stakeholder has confidence that a product or system will behave as intended.

Unlinkability
(RFC 6973) Within a particular set of information, the inability of an observer or attacker to determine whether two items of interest are related or not (with a high enough degree of probability to be useful to the observer or attacker).

Validation
(ISO/IEC 27000:2016) Confirmation, through the provision of objective evidence, that the requirements for a specific intended use or application have been fulfilled.

Verification
(ISO/IEC 27000:2016) Confirmation, through the provision of objective evidence, that specified requirements have been fulfilled.

Vetting (referred to recruitment)
(Collins Online Dictionary) Employee screening: the process of investigating somebody to establish their trustworthiness.
(NIST SP 800-163) The process of verifying that an app meets an organisation's security requirements. An app vetting process comprises app testing and app approval/rejection activities.

Vulnerability
(ISO/IEC 27000) The weakness of an asset or control that can be exploited by one or more threats.

ENDNOTES

1 According to a recent study by FireEye, in Europe, the dwell time of a cyber attack before detection is increasing from 106 days to 175 days.

2 According to the OECD Digital Economy Outlook 2017 (OECD, 2017), today more than 90 % of businesses in the world are connected to the internet.

3 Examples of standards bringing security features into network communications include the secure software layer (SSL) in 1995, DNSSEC in 1997, and S/MIME for email security in 1998.

4 The 2000s decade witnessed major and contemporary evolutions at the technological level, from the availability of low-cost computers to the advent of home broadband and mobile connectivity. The net result is a much more 'vivid' internet with multimedia content and social media. The 'Web 2.0' was born.

5 Cyber-physical systems refer to systems with a software component which are capable of interacting with the physical world.

6 In 2012, a major data breach hitting more than 10 million credit cards opened a series of large cybercrime attacks (Krebs, 2012), followed by the Yahoo data breach which hit more than 400 million accounts (Volz, 2016). We could also mention the Sony PlayStation attack (Quinn and Arthur, 2011), the Adobe attack (Welch, 2013), Ashley Madison (2015) (Zetter, 2015) and more recently Equifax (2017) (Federal Trade Commission, 2020) data breaches that each put the data of millions of users at stake.

7 Several suicides were reported as a result of the massive personal data breach in the Ashley Madison case (Baraniuk, 2015). The Sony PlayStation hack was also considered to have had a negative influence on consumers' trust in the e-market for digital services.

8 In 2017, the European Commission published the Communication 'Resilience, Deterrence and Defence: Building strong cybersecurity for the EU' whereby it outlines its plan to face the current cybersecurity challenges by proposing actions linked to the protection of systems, networks and services, the prosecution of crimes and the defence area.

9 Whereas 'the cyberspace' is defined as 'the complex environment resulting from the interaction of people, software and services on the internet by means of technology devices and networks connected to it, which does not exist in any physical form'.

10 Article 7 (respect for private and family life) of the Charter of Fundamental Rights of the European Union.

11 Article 4 of the GDPR (principles relating to processing of personal data) states that personal data shall be 'processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ("integrity and confidentiality")'. Further, article 32 (security of processing), requires that both data controller and processor implement appropriate technical and organisational measures to ensure the security of personal data, following a risk-based approach.

12 ENISA published a comprehensive map of MS cybersecurity strategies (ENISA, 2020b).

13 Although such systems have not always been referred to as 'artificial intelligence'.

14 In contrast to classical information technologies based in semiconductor devices for which quantum physics only provides a background understanding of the materials being used.

15 In cybersecurity, the term *attack surface* refers to the collection of all potential entry points that attackers could use to compromise services, systems or information by using vulnerabilities.

16 There are always cases of threat actors offering their crime as a service and therefore looking for money. However, in such cases, it is the sponsor of the attack who is driven by ideals.

17 Dashboards that provide up-to-date information on the virus have been created by several organisations. For instance, some pieces of malware are disguised as a 'Coronavirus map' to spread them effectively.

18 This was done to lure recipients to websites to download malware on their systems.

19 The classical example is that of a building in a neighbourhood that one day appears with a window broken. Days pass by without the window being fixed then, at some point, another window appears broken, which is then followed up by many more in the following days. Eventually, other more serious offences start to develop around that building.

20 Cybersecurity products, such as antiviruses, firewalls, intrusion detection systems or vulnerability scanners, are effective in the identification and prevention of some types of attack.

21 In software, security-by-default requires that the default configuration settings are the most secure settings possible, without even the end-user knowing it is there or having to enable it. For example, a social networking site should set users' profile settings in the most privacy-friendly option in an effort to limit from the onset the accessibility of the users' profiles to third persons. The interested reader should also refer to the 'Establish secure defaults' security principle as defined by the Open Web Application Security Project.

22 The SOG-IS agreement was produced in response to the EU Council Decision of 31 March 1992 (92/242/EEC) in the field of security of information systems, and the subsequent Council Recommendation of 7 April 1995 (1995/144/EC) on common information technology security evaluation criteria.

23 Note that 'system functionality' is intentionally left as a general term and could stand for a wide range of notions, such as service operability, business income, trust in the service or public institution, etc.

REFERENCES

Ablon, L. and A. Bogart, Zero Days, *Thousands of Nights: The Life and Times of Zero-Day Vulnerabilities and Their Exploits,* RAND Corporation, Santa Monica, California, 2017, https://doi.org/10.7249/rr1751.

Ablon, L., P. Heaton, D. Lavery and S. Romanosky, *Consumer Attitudes Toward Data Breach Notifications and Loss of Personal Information,* RAND Corporation, 2016, https://doi.org/10.7249/rr1187.

Abrams, L., Over 500, *000 Zoom Accounts Sold on Hacker Forums, the Dark Web,* BleepingComputer, 13 April 2020a, https://www.bleepingcomputer.com/news/security/over-500-000-zoom-accounts-sold-on-hacker-forums-the-dark-web.

Abrams, L., *Ransomware Gangs to Stop Attacking Health Orgs During Pandemic,* BleepingComputer, 18 March 2020b, https://www.bleepingcomputer.com/news/security/ransomware-gangs-to-stop-attacking-health-orgs-during-pandemic.

ACCC, *Scammers Targeting Superannuation in COVID-19 Crisis,* Australian Competition and Consumer Commission, 6 April 2020, https://www.accc.gov.au/media-release/scammers-targeting-superannuation-in-covid-19-crisis.

Ahmed, D., *Hackers Are Actively Targeting WHO amid Coronavirus Pandemic,* HackRead, 25 March 2020, https://www.hackread.com/hackers-are-actively-targeting-who-amid-coronavirus-pandemic.

Amante, A., *Italy's Social Security Website Hit by Hacker Attack,* Reuters, 1 April 2020, https://www.reuters.com/article/us-health-coronavirus-italy-cybercrime-idUSKBN21J5U1.

Amodei, D., C. Olah, J. Steinhardt, P.F. Christiano, J. Schulman and D. Mané, *Concrete Problems in AI Safety,* 2016, https://arxiv.org/abs/1606.06565.

Annoni, A., P. Benczur, P. Bertoldi, B. Delipetrev, G. De Prato, C. Feijoo, E. Fernandez Macias et al., *Artificial Intelligence: A European Perspective,* Publications Office of the European Union, 2018, JRC113826. https://doi.org/10.2760/11251.

ANSA, *ANSA Leveraging Blockchain Technology to Help Readers Check Source of News,* ANSA, 6 April 2020, http://www.ansa.it/english/news/2020/04/06/ansa-using-blockchain-tech-to-help-readers-source-check_465ed8fb-c1d3-4f64-b94a-823f0f8576d0.html.

Antonakakis, M., T. April, M. Bailey, M. Bernhard, E. Bursztein, J. Cochran, Z. Durumeric et al., *Understanding the Mirai Botnet,* 2017, pp. 1093-1110, https://www.usenix.org/conference/usenixsecurity17/technical-sessions/presentation/antonakakis.

Arsene, L., *New Router DNS Hijacking Attacks Abuse Bitbucket to Host Infostealer,* Bitdefender Labs, 25 March 2020, https://labs.bitdefender.com/2020/03/new-router-dns-hijacking-attacks-abuse-bitbucket-to-host-infostealer.

Asiapedia, *Cyber-Security Law of the People's Republic of China,* Dezan Shira & Associates, January 2019, https://www.dezshira.com/library/legal/cyber-security-law-china-8013.html.

Asif, S., *Chinese COVID-19 Detection Firm Hacked; Source Code Sold on Dark Web,* HackRead, 27 April 2020a, https://www.hackread.com/chinese-covid-19-detection-firm-hacked-dark-web.

Asif, S., *Dark Web Scammers Selling Ventilators & MP3 Files to Kill Coronavirus,* HackRead, 20 April 2020b, https://www.hackread.com/dark-web-scammers-ventilators-mp3-files-kill-coronavirus.

Asokan, A., *WHO Reports 'Dramatic' Increase in Cyberattacks,* BankInfoSecurity, 25 April 2020, https://www.bankinfosecurity.com/who-reports-dramatic-increase-in-cyberattacks-a-14184.

Atlas Cybersecurity, *Tracking Coronavirus/COVID19 Cyber Threat Campaigns,* Atlas Cybersecurity, 30 March 2020, https://www.atlas-cybersecurity.com/covid19_tracking.

Australian Cyber Security Centre, *Australian Government Information Security Manual,* Australian Government, March 2020, https://www.cyber.gov.au/ism.

Australian Government, 'Protective Security Policy Framework', *Australian Government Protective Security Policy,* 2020, https://www.protectivesecurity.gov.au/node/45.

- Avast Threat Intelligence Team, *Malvertising Campaign Taking Advantage of COVID-19 Targeting Internet Explorer Users to Steal Their Information,* Avast, 16 April 2020, *https://blog.avast.com/malvertising-campaign-targeting-internet-explorer-users*.
- AV-TEST, 'Malware Statistics & Trends Report', 28 November 2018, *https://www.av-test.org/en/statistics/malware*.
- Baraniuk, C., '"Suicides' over Ashley Madison Hack', *BBC News,* 24 August 2015, *https://www.bbc.com/news/technology-34044506*.
- Barreno, M., B. Nelson, R. Sears, A.D. Joseph and J.D. Tygar, 'Can Machine Learning Be Secure?', *Proceedings of the 2006 ACM Symposium on Information, Computer and Communications Security, ASIACCS '06,* ACM, New York, NY, USA, 2006, pp. 16-25, *https://doi.org/10.1145/1128817.1128824*.
- Barrett, D. and K. O'Keeffe, 'FBI Suspects Insider Involvement in $81 Million Bangladesh Bank Heist', *WSJ,* 10 May 2016, *https://blogs.wsj.com/indiarealtime/2016/05/10/fbi-suspects-insider-involvement-in-81-million-bangladesh-bank-heist*.
- Barrett, M.P., 'Framework for Improving Critical Infrastructure Cybersecurity Version 1.1', *NIST,* 16 April 2018, *https://doi.org/10.6028/NIST.CSWP.04162018*.
- Barth, B., *Nation-State Hackers Reportedly Hunting for COVID-19 Research,* The Cyber-Security Source, 21 April 2020, *https://www.scmagazineuk.com/article/1680822*.
- Bendiek, A., *The EU as a Force for Peace in International Cyber Diplomacy,* SWP, 19 April 2018, *https://www.swp-berlin.org/en/publication/the-eu-as-a-force-for-peace-in-international-cyber-diplomacy*.
- Bennett, C.H. and P.W. Shor, 'Quantum Information Theory', *IEEE Transactions on Information Theory,* Vol. 44, No. 6, September 2006, pp. 2724-2742, *https://doi.org/10.1109/18.720553*.
- Biggio, B. and F. Roli, 'Wild Patterns: Ten Years after the Rise of Adversarial Machine Learning', *Pattern Recognition,* Vol. 84, 1 December 2018, pp. 317-331, *https://doi.org/10.1016/j.patcog.2018.07.023*.
- Bishop, M., *Computer Security: Art and Science,* Addison-Wesley, Boston, 2003, *https://dl.acm.org/doi/10.5555/579090*.
- Bizga, A., *Treasure Trove of Covid-19 Protective Gear and Medical Supplies Selling on Dark Web Markets,* HOTforSecurity, 30 April 2020, *https://hotforsecurity.bitdefender.com/blog/treasure-trove-of-covid-19-protective-gear-and-medical-supplies-selling-on-dark-web-markets-23143.html*.
- Björck, F., M. Henkel, J. Stirna and J. Zdravkovic, 'Cyber Resilience – Fundamentals for a Definition', in A. Rocha, A.M. Correia, S. Costanzo, and L.P. Reis (eds.), *New Contributions in Information Systems and Technologies, Advances in Intelligent Systems and Computing,* Springer International Publishing, Cham, 2015, pp. 311-316, *https://doi.org/10.1007/978-3-319-16486-1_31*.
- Bodeau, D. and R. Graubart, *Cyber Resiliency Design Principles Selective Use Throughout the Lifecycle and in Conjunction with Related Disciplines,* MITRE, January 2017, *https://www.mitre.org/sites/default/files/publications/PR%2017-0103%20Cyber%20Resiliency%20Design%20Principles%20MTR17001.pdf*.
- Brundage, M., S. Avin, J. Clark, H. Toner, P. Eckersley, B. Garfinkel, A. Dafoe et al., 'The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation', 20 February 2018, *http://arxiv.org/abs/1802.07228*.
- Burrell, D.N., 'An Exploration of the Cybersecurity Workforce Shortage', *International Journal of Hyperconnectivity and the Internet of Things (IJHIoT),* Vol. 2, No. 1, 1 January 2018, pp. 29-41, *https://doi.org/10.4018/IJHIoT.2018010103*.
- Busvine, D., and A. Rinke, *Germany Flips to Apple-Google Approach on Smartphone Contact Tracing,* Reuters, 26 April 2020, *https://www.reuters.com/article/us-health-coronavirus-europe-tech-idUSKCN22807J*.
- Carretero, S., R. Vuorikari and Y. Punie, *DigComp 2.1 the Digital Competence Framework for Citizens with Eight Proficiency Levels and Examples of Use,* Joint Research Centre, 2017, *https://doi.org/10.2760/38842*.
- Centre for Cyber Security, *Threat Assessment: The Cyber Threat Against Denmark During the COVID-19 Pandemic,* April 2020, *https://fe-ddis.dk/cfcs/publikationer/Documents/The%20Cyber%20Threat%20Against%20Denmark%20During%20the%20COVID-19%20Pandemic.pdf*.
- CERT-EU, *CERT-EU Responsible Disclosure Policy,* CERT-EU, 2020, *https://cert.europa.eu/cert/newsletter/en/latest_HallOfFame_.html#CERTpolicy*.

- CERT-EU, COVID-19 *Cyber Bulletin #8, Threat Memo - TM 20-033,* Version 8.0, CERT-EU, 29 April 2020a.
- CERT-EU, COVID-19, *Threat Memo - TM 20-033,* Version 3.0, CERT-EU, 25 March 2020b.
- CERT-EU, COVID-19, *Threat Memo - TM 20-035,* Version 1.0, CERT-EU, 23 March 2020c.
- Cerulus, L., 'China's Ghost in Europe's Telecom Machine', *Politico,* 11 December 2017, *https://www.politico.eu/article/huawei-china-ghost-in-europe-telecom-machine*.
- Cimpanu, C., 'Internet Traffic From Mobile Browsers Exceeds Desktop Traffic for the First Time', *BleepingComputer,* 11 November 2016, *https://www.bleepingcomputer.com/news/software/internet-traffic-from-mobile-browsers-exceeds-desktop-traffic-for-the-first-time*.
- Cimpanu, C., *France Warns of New Ransomware Gang Targeting Local Governments,* ZDNet, 19 March 2020a, *https://www.zdnet.com/article/france-warns-of-new-ransomware-gang-targeting-local-governments*.
- Cimpanu, C., *German Government Might Have Lost Tens of Millions of Euros in COVID-19 Phishing Attack,* ZDNet, 18 April 2020b, *https://www.zdnet.com/article/german-government-might-have-lost-tens-of-millions-of-euros-in-covid-19-phishing-attack*.
- Cimpanu, C., *There's Now COVID-19 Malware That Will Wipe Your PC and Rewrite Your MBR,* ZDNet, 2 April 2020c, *https://www.zdnet.com/article/theres-now-covid-19-malware-that-will-wipe-your-pc-and-rewrite-your-mbr*.
- CIO Platform Nederland and Rabobank, *Coordinated Vulnerability Disclosure Manifesto,* April 2016, *https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/manifesto-coordinated-responsiblity-disclosure.pdf*.
- CISA, *Microsoft Office 365 Security Recommendations,* Department of Homeland Security, 29 April 2020a, *https://www.us-cert.gov/ncas/alerts/aa20-120a*.
- CISA, *Ransomware Impacting Pipeline Operations,* Department of Homeland Security, 18 February 2020b, *https://www.us-cert.gov/ncas/alerts/aa20-049a*.
- Cisco, *Annual Cybersecurity Report,* February 2018, *https://www.cisco.com/c/dam/m/hu_hu/campaigns/security-hub/pdf/acr-2018.pdf*.
- Coble, S., '#COVID19 Tracking App Tells Untested Aussies They're Infected', *Infosecurity Magazine,* 28 April 2020, *https://www.infosecurity-magazine.com:443/news/covid19-tracking-app-australia*.
- Cognizant, *Cognizant Security Incident Update,* Cognizant Technology Solutions, 18 April 2020, *https://news.cognizant.com/2020-04-18-cognizant-security-update*.
- Cohen, F., 'Experiments with Computer Viruses', *Fred Cohen & Associates,* 1984, *http://all.net/books/virus/part5.html*.
- Corera, G., *Coronavirus: Cyber-Spies Seek Coronavirus Vaccine Secrets,* BBC News, 1 May 2020, *https://www.bbc.com/news/technology-52490432*.
- Corkery, M. and M. Goldstein, 'North Korea Said to Be Target of Inquiry Over $81 Million Cyberheist' – *The New York Times,* 22 March 2017, *https://www.nytimes.com/2017/03/22/business/dealbook/north-korea-said-to-be-target-of-inquiry-over-81-million-cyberheist.html*.
- Council of Europe, Convention on Cybercrime, *European Treaty Series - No. 185,* XI.2001, *https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561*.
- Council of the European Union, *Declaration by the High Representative Josep Borrell, on Behalf of the European Union, on Malicious Cyber Activities Exploiting the Coronavirus Pandemic,* European Council, Council of the European Union, 30 April 2020, *http://www.consilium.europa.eu/en/press/press-releases/2020/04/30/declaration-by-the-high-representative-josep-borrell-on-behalf-of-the-european-union-on-malicious-cyber-activities-exploiting-the-coronavirus-pandemic*.
- Council of the European Union, Draft Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ('Cyber Diplomacy Toolbox') – Adoption, *9916/17,* 7 June 2017, *http://data.consilium.europa.eu/doc/document/ST-9916-2017-INIT/en/pdf*.
- Council on Foreign Relations, 'Connect the Dots on State-Sponsored Cyber Incidents', *Council on Foreign Relations,* 2019, *https://www.cfr.org/interactive/cyber-operations*.

- CSAN, *Cyber Security Assessment Netherlands,* National Coordinator for Security and Counterterrorism, Ministry of Justice and Security, August 2018, *https://english.nctv.nl/documents/publications/2018/08/07/cyber-security-assessment-netherlands-2018*.
- CSIS, 'Significant Cyber Incidents', *Center for Strategic and International Studies*, April 2020, *https://www.csis.org/programs/technology-policy-program/significant-cyber-incidents*.
- Cyber Report, *Attackers Hacked the Digital Pass System of Moscow Residents,* Cyber Report, 14 April 2020, *https://www.cyberreport.io/news/attackers-hacked-the-digital-pass-system-of-moscow-residents?article=18807*.
- Cybersecurity Help, *Croatia's Largest Petrol Station Chain Joins List of Victims of Ransomware Attacks,* Cybersecurity Help, 21 February 2020a, *https://www.cybersecurity-help.cz/blog/957.html*.
- Cybersecurity Help, *Pakistan-Linked APT 36 Uses Coronavirus-Themed Phishing to Drop Crimson RAT,* Cybersecurity Help, 18 March 2020b, *https://www.cybersecurity-help.cz/blog/991.html*.
- Cybersecurity Ventures, *The 2019 Official Annual Cybercrime Report,* Herjavec Group, 2019, *https://www.herjavecgroup.com/the-2019-official-annual-cybercrime-report*.
- Cyware, *Live Updates: COVID-19 Cybersecurity Alerts,* CYWARE, 5 May 2020, *https://cyware.com/blog/live-updates-covid-19-cybersecurity-alerts-b313*.
- Daly, A., *White House Phishing Scam: INKY Catches Another Coronaphish,* Inky, 2020, *https://www.inky.com/blog/white-house-phishing-scam-inky-catches-another-coronaphish*.
- Del Rosso, K., *New Threat Discovery Shows Commercial Surveillanceware Operators Latest to Exploit COVID-19,* Lookout, 18 March 2020, *https://blog.lookout.com/commercial-surveillanceware-operators-latest-to-take-advantage-of-covid-19*.
- Department of Health and Social Care (NHS) UK, *Securing Cyber Resilience in Health and Care: October 2018 Update,* Department of Health and Social Care, 11 October 2018, *https://www.gov.uk/government/publications/securing-cyber-resilience-in-health-and-care-october-2018-update*.
- Dolz, P.O., and J.P. Colomé, *La policía detecta un ciberataque al sistema informático de los hospitales,* El País, 23 March 2020, *https://elpais.com/espana/2020-03-23/la-policia-detecta-un-ataque-masivo-al-sistema-informatico-de-los-hospitales.html*.
- Doyle, C., *Cybercrime: An Overview of the Federal Computer Fraud and Abuse Statute and Related Federal Criminal Laws,* Congressional Research Service, 15 October 2014, *https://fas.org/sgp/crs/misc/97-1025.pdf*.
- Duch-Brown, N., *The Competitive Landscape of Online Platforms, JRC Working Papers on Digital Economy,* Joint Research Centre (Seville site), July 2017, *https://ec.europa.eu/jrc/en/publication/eur-scientific-and-technical-research-reports/competitive-landscape-online-platforms*.
- ECSO, 'ECSO - European Cyber Security Organisation', *ECSO - European Cyber Security Organisation,* 2019, *https://ecs-org.eu/cppp*.
- ENISA, *Cloud Computing, Benefits, Risks and Recommendations for Information Security,* ENISA, 20 November 2009, *https://www.enisa.europa.eu/publications/cloud-computing-risk-assessment*.
- ENISA, *Definition of Cybersecurity - Gaps and Overlaps in Standardisation,* ENISA, 1 July 2016a, *https://doi.org/10.2824/4069*.
- ENISA, *ENISA Good Practices for Security of Smart Cars,* ENISA, November 2019a, *https://doi.org/10.2824/17802*.
- ENISA, *ENISA Threat Landscape 2012 - Responding to the Evolving Threat Environment,* ENISA, September 28, 2012, *https://www.enisa.europa.eu/publications/ENISA_Threat_Landscape*.
- ENISA, *ENISA Threat Landscape 2013 - Overview of Current and Emerging Cyber-Threats,* ENISA, 11 December 2013, *https://doi.org/10.2824/022950*.
- ENISA, *ENISA Threat Landscape 2014 - Overview of Current and Emerging Cyber-Threats,* ENISA, 27 January 2015, *https://doi.org/10.2824/061861*.
- ENISA, *ENISA Threat Landscape 2015,* ENISA, 27 January 2016b, *https://www.enisa.europa.eu/publications/etl2015*.
- ENISA, *ENISA Threat Landscape for 5G Networks,* ENISA, November 2019b, *https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-5g-networks*.

- ENISA, *ENISA Threat Landscape Report 2016 - 15 Top Cyber-Threats and Trends,* ENISA, 8 February 2017, *https://doi.org/10.2824/92184*.
- ENISA, *ENISA Threat Landscape Report 2018 - 15 Top Cyberthreats and Trends,* ENISA, 28 January 2019c, *https://doi.org/10.2824/622757*.
- ENISA, *EU Member States Incident Response Development Status Report,* ENISA, November 2019d, *https://doi.org/10.2824/74233*.
- ENISA, *Good Practices for Security of IoT, Secure Software Development Lifecycle,* ENISA, 19 November 2019e, *https://doi.org/10.2824/742784*.
- ENISA, *Good Practices in Innovation on Cybersecurity under the NCSS,* ENISA, 19 November 2019f, *https://doi.org/10.2824/01007*.
- ENISA, *Information Sharing and Analysis Centers (ISACs),* ENISA, 2020a, *https://www.enisa.europa.eu/topics/national-cyber-security-strategies/information-sharing*.
- ENISA, *Joint Fight against COVID-19 Related Threats,* ENISA, 20 March 2020a, *https://www.enisa.europa.eu/news/enisa-news/joint-fight-against-covid-19-related-threats*.
- ENISA, *National Cyber Security Strategies - Interactive Map,* ENISA, 2020b, *https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map*.
- ENISA, *Port Cybersecurity, Good Practices for Cybersecurity in the Maritime Sector,* ENISA, 26 November 2019g, *https://doi.org/10.2824/328515*.
- ENISA, *Situation Report on Covid-19 Related Cyber Threats,* ENISA, 1 May 2020b.
- ENISA, *Tips for Cybersecurity When Working from Home,* ENISA, 24 March 2020c, *https://www.enisa.europa.eu/tips-for-cybersecurity-when-working-from-home*.
- Estonia's e-Governance Academy, 'National Cyber Security Index', 2019, *https://ncsi.ega.ee*.
- European Central Bank, *Fifth Report on Card Fraud,* September 2018, *https://doi.org/10.2866/450506*.
- European Commission, A European Strategy for Data, *COM(2020) 66 Final,* 19.2.2020.a, *https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020DC0066*.
- European Commission, *Artificial Intelligence for Europe,* 25 April 2018a, *https://ec.europa.eu/transparency/regdoc/rep/1/2018/EN/COM-2018-237-F1-EN-MAIN-PART-1.PDF*.
- European Commission, Commission Recommendation (EU) 2017/1584 of 13 September 2017 on Coordinated Response to Large-Scale Cybersecurity Incidents and Crises, 13 September 2017a, *https://eur-lex.europa.eu/eli/reco/2017/1584/oj*.
- European Commission, Commission Recommendation (EU) 2019/534 of 26 March 2019, Cybersecurity of 5G Networks, *https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32019H0534*.
- European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic And Social Committee and the Committee of the Regions, The European Agenda on Security, *COM(2015) 185 Final,* 28 April 2015, *https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52015DC0185*.
- European Commission, *Flash Eurobarometer 443: E-Privacy,* December 2016a, *http://ec.europa.eu/COMMFrontOffice/publicopinion/index.cfm/Survey/getSurveyDetail/instruments/FLASH/surveyKy/2124*.
- European Commission, Joint Communication to the European Parliament and the Council, Joint Framework on Countering Hybrid Threats - a European Union Response, *JOIN(2016) 18 Final,* 4 June 2016b, *https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52016JC0018*.
- European Commission, Joint Communication to the European Parliament and the Council, Resilience, Deterrence and Defence: Building Strong Cybersecurity for the EU, *JOIN(2017) 450 Final,* 13 September 2017b, *https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1505294563214&uri=JOIN:2017:450:FIN*.
- European Commission, Joint Communication to the European Parliament, the European Council and the Council, Increasing Resilience and Bolstering Capabilities to Address Hybrid Threats, *JOIN(2018) 16 Final,* 13 June 2018b, *https://eur-lex.europa.eu/legal-content/GA/TXT/?uri=CELEX:52018JC0016*.

- European Commission, Joint Report to the European Parliament and the Council on the Implementation of the Joint Framework on Countering Hybrid Threats - a European Union Response, 19 July 2017c, *https://ec.europa.eu/docsroom/documents/24601*.
- European Commission, On Artificial Intelligence - A European Approach to Excellence and Trust, *COM(2020) 65 Final,* 19 February 2020b, *https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2020:65:FIN*.
- European Commission, Proposal for a Regulation of the European Parliament and of the Council Establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres, *COM(2018) 630 Final,* 9 December 2018c, *https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A52018PC0630*.
- European Commission, Proposal for a Regulation of the European Parliament and of the Council on ENISA, the 'EU Cybersecurity Agency', and Repealing Regulation (EU) 526/2013, and on Information and Communication Technology Cybersecurity Certification ('Cybersecurity Act'), *COM(2017) 477 Final,* 13 September 2017d, *https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2017:477:FIN*.
- European Commission, Shaping Europe's Digital Future, *COM(2020) 67 Final,* 19 February 2020c, *https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020DC0067*.
- European Commission, *Special Eurobarometer 359: Attitudes on Data Protection and Electronic Identity in the European Union,* June 2011, *https://ec.europa.eu/commfrontoffice/publicopinion/index.cfm/Survey/getSurveyDetail/search/359/surveyKy/864*.
- European Commission, 'The Directive on Security of Network and Information Systems (NIS Directive)', *Digital Single Market - European Commission,* 5 July 2016c, *https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive*.
- European Commission, and Directorate-General for Research and Innovation, *Cybersecurity in the European Digital Single Market,* 2017, *https://doi.org/10.2777/466885*.
- European Parliament, and Council of the European Union, Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector, 2002, *https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32002L0058*.
- European Parliament and Council of the European Union, Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 Concerning Measures for a High Common Level of Security of Network and Information Systems across the Union, 6 July 2016a, *https://eur-lex.europa.eu/eli/dir/2016/1148/oj*.
- European Parliament and Council of the European Union, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), *2016/679,* 4 May 2016b, *https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679*.
- European Parliament and Council of the European Union, Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market, *910/2014,* 28 August 2014, *https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2014.257.01.0073.01.ENG*.
- European Parliament, Council of the European Union, European Economic and Social Committee, and Committee of the Regions, Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, 2013, *https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52013JC0001*.
- European Union, Charter of Fundamental Rights of the European Union, 326/02, 26 October 2012, *https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:12012P/TXT&from=EN*.
- Europol, *Cyber Bits, Series: Trend, COVID-19 Cyber,* Europol, March 2020a.
- Europol, *Internet Organised Crime Threat Assessment (IOCTA) 2018,* 2018, *https://doi.org/10.2813/858843*.

Europol, *Make Your Home a Cyber Safe Stronghold,* Europol, 2020a, *https://www.europol.europa.eu/activities-services/public-awareness-and-prevention-guides/make-your-home-cyber-safe-stronghold*.

Europol, *Pandemic Profiteering: How Criminals Exploit the COVID-19 Crisis,* Europol, March 2020b, *https://www.europol.europa.eu/publications-documents/pandemic-profiteering-how-criminals-exploit-covid-19-crisis*.

Europol, *The Internet Organised Crime Threat Assessment (IOCTA) 2014b, https://doi.org/10.2813/16*.

Eykholt, K., I. Evtimov, E. Fernandes, B. Li, A. Rahmati, F. Tramer, A. Prakash, T. Kohno and D. Song, *Physical Adversarial Examples for Object Detectors,* 2018, *https://www.usenix.org/conference/woot18/presentation/eykholt*.

Facebook, *Facebook Reports Fourth Quarter and Full Year 2018 Results,* Facebook Investor Relations, 30 January 2019, *https://investor.fb.com/investor-news/press-release-details/2019/Facebook-Reports-Fourth-Quarter-and-Full-Year-2018-Results/default.aspx*.

Federal Trade Commission, 'The Equifax Data Breach', *Federal Trade Commission,* January 2020, *https://www.ftc.gov/equifax-data-breach*.

Figenbaum, E., T. Assum and M. Kolbenstvedt, 'Electromobility in Norway: Experiences and Opportunities', *Research in Transportation Economics, Vol. 50, Electric Vehicles: Modelling Demand and Market Penetration,* 1 August 2015, pp. 29-38, *https://doi.org/10.1016/j.retrec.2015.06.004*.

Fouquet, H., *Paris Hospitals Target of Failed Cyber-Attack, Authority Says,* Bloomberg, 23 March 2020, *https://www.bloomberg.com/news/articles/2020-03-23/paris-hospitals-target-of-failed-cyber-attack-authority-says*.

Freedman, T., J. Roeder, A. Hart, K. Doran and K. Sklar, *A Pivotal Moment, Developing a New Generation of Technologists for the Public Interest,* Freedman Consulting, 2016, *https://www.netgainpartnership.org/s/pivotalmoment.pdf*.

Freedom House, *Principles for Protecting Civil and Political Rights in the Fight against Covid-19,* Freedom House, 24 March 2020, *https://freedomhouse.org/article/principles-protecting-civil-and-political-rights-fight-against-covid-19*.

Gallagher, R., *5G Virus Conspiracy Theory Fueled by Coordinated Effort,* Bloomberg, 9 April 2020, *https://www.bloomberg.com/news/articles/2020-04-09/covid-19-link-to-5g-technology-fueled-by-coordinated-effort*.

Gal-Or, E. and A. Ghose, 'The Economic Incentives for Sharing Security Information', *Information Systems Research,* Vol. 16, No. 2, 1 June 2005, pp. 186-208, *https://doi.org/10.1287/isre.1050.0053*.

Gatlan, S., *Banking Malware Spreading via COVID-19 Relief Payment Phishing,* BleepingComputer, 30 March 2020a, *https://www.bleepingcomputer.com/news/security/banking-malware-spreading-via-covid-19-relief-payment-phishing*.

Gatlan, S., *Microsoft Warns of Malware Surprise Pushed via Pirated Movies,* BleepingComputer, 28 April 2020b, *https://www.bleepingcomputer.com/news/security/microsoft-warns-of-malware-surprise-pushed-via-pirated-movies*.

Gatlan, S., *RagnarLocker Ransomware Hits EDP Energy Giant, Asks for €10M,* BleepingComputer, 14 April 2020c, *https://www.bleepingcomputer.com/news/security/ragnarlocker-ransomware-hits-edp-energy-giant-asks-for-10m*.

Gatlan, S., *US Govt: Hacker Used Stolen AD Credentials to Ransom Hospitals,* BleepingComputer, 18 April 2020d, *https://www.bleepingcomputer.com/news/security/us-govt-hacker-used-stolen-ad-credentials-to-ransom-hospitals*.

Goldstick, S., C. Lawson, S. Millendorf, K. Parsons-Reponte, and J. Rathburn, *COVID-19: Privacy and Cybersecurity Regulatory and Enforcement Guidance,* The National Law Review, 9 April 2020, *https://www.natlawreview.com/article/covid-19-privacy-and-cybersecurity-regulatory-and-enforcement-guidance*.

Goodwin, B., Cyber Gangsters H*it UK Medical Firm Poised for Work on Coronavirus with Maze Ransomware Attack,* ComputerWeekly, 22 March 2020, *https://www.computerweekly.com/news/252480425/Cyber-gangsters-hit-UK-medical-research-lorganisation-poised-for-work-on-Coronavirus*.

GReAT, *APT Trends Report Q1 2020,* Kaspersky SecureList, 30 April 2020, *https://securelist.com/apt-trends-report-q1-2020/96826*.

Great Britain, *Computer Misuse Act 1990: Chapter 18,* HMSO, London, 1990, *http://www.legislation.gov.uk/ukpga/1990/18/pdfs/ukpga_19900018_en.pdf*.

Greenberg, A., 'The Untold Story of NotPetya, the Most Devastating Cyberattack in History', *Wired,* 22 August 2018, *https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world*.

- Heilweil, R., *Coronavirus Scammers Are Flooding Social Media with Fake Cures and Tests,* Vox, 17 April 2020, *https://www.vox.com/recode/2020/4/17/21221692/digital-black-market-covid-19-coronavirus-instagram-twitter-ebay*.
- Hertig, A., *Thousands of These Computers Were Mining Cryptocurrency. Now They're Working on Coronavirus Research,* CoinDesk, 19 March 2020, *https://www.coindesk.com/thousands-of-these-computers-were-mining-cryptocurrency-now-theyre-working-on-coronavirus-research*.
- Hodge, R., *Using Zoom While Working from Home? Here Are the Privacy Risks to Watch out For,* CNET, 2 April 2020a, *https://www.cnet.com/news/using-zoom-while-working-from-home-here-are-the-privacy-risks-to-watch-out-for*.
- Hodge, R., *Zoom Security Issues: Zoom Could Be Vulnerable to Foreign Surveillance, Intel Report Says,* CNET, 28 April 2020b, *https://www.cnet.com/news/zoom-security-issues-zoom-could-be-vulnerable-to-foreign-surveillance-intel-report-says*.
- Hope, K., V. Peycheva, S. McKiernan, J. Julius, L. Koch, D. Herr and P. Muller, *Annual Report on European SMEs 2016/2017: Focus on Self-Employment,* Internal Market, Industry, Entrepreneurship and SMEs, Publications Office of the European Union, 15 November 2017, *https://doi.org/10.2873/742338*.
- Householder, A.D., G. Wassermann, A. Manion and C. King, *The CERT Guide to Coordinated Vulnerability Disclosure,* Carnegie Mellon University, Software Engineering Institute, August 2017, *https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=503330*.
- Human Rights Watch, *Joint Civil Society Statement: States Use of Digital Surveillance Technologies to Fight Pandemic Must Respect Human Rights,* Human Rights Watch, 2 April 2020, *https://www.hrw.org/news/2020/04/02/joint-civil-society-statement-states-use-digital-surveillance-technologies-fight*.
- Huntley, S., *Findings on COVID-19 and Online Security Threats,* Google Blog, 22 April 2020, *https://blog.google/technology/safety-security/threat-analysis-group/findings-covid-19-and-online-security-threats*.
- Independent High-Level Expert Group on Artificial Intelligence, *A Definition of Artificial Intelligence: Main Capabilities and Scientific Disciplines,* Text, European Commission, 8 April 2019, *https://ec.europa.eu/digital-single-market/en/news/definition-artificial-intelligence-main-capabilities-and-scientific-disciplines*.
- Instagram, 'Instagram Business', *Instagram for Business,* 2020, *https://business.instagram.com*.
- Internet Live Stats, 'Internet Live Stats - Internet Usage and Social Media Statistics', *Internet Live Stats,* 2020, *https://www.internetlivestats.com*.
- Internet World Stats, *Mobile Internet - Mobile Phones and Smart Mobile Phones,* Internet World Stats, 19 September 2017, *https://www.internetworldstats.com/mobile.htm*.
- Jo, A.R., *The Effect of Competition Intensity on Software Security - An Empirical Analysis of Security Patch Release on the Web Browser Market*, San Diego, 2017, *https://www.semanticscholar.org/paper/The-effect-of-competition-intensity-on-software-of-Jo/7e7c7825f7f8f7ac558e1478c56c003ed3da2a44*.
- Joint Research Centre, *Be Safe out There: Choose Your Passwords Wisely and Protect Them,* EU Science Hub - European Commission, 25 January 2019, *https://ec.europa.eu/jrc/en/research-topic/security-privacy-and-data-protection/password-security*.
- Joint Task Force Transformation Initiative, *Guide for Conducting Risk Assessments,* National Institute of Standards and Technology, 17 September 2012, *https://doi.org/10.6028/NIST.SP.800-30r1*.
- Joubert, V., *Five Years after Estonia's Cyber Attacks: Lessons Learned for NATO?,* NATO, May 2012, *https://www.files.ethz.ch/isn/143191/rp_76.pdf*.
- Kannan, K., J. Rees and S. Sridhar, 'Market Reactions to Information Security Breach Announcements: An Empirical Analysis', *International Journal of Electronic Commerce,* Vol. 12, No. 1, September 2007, pp. 69-91, *https://doi.org/10.2753/JEC1086-4415120103*.
- Kienzle, D.M. and M.C. Elder, 'Recent Worms: A Survey and Trends', *Proceedings of the 2003 ACM Workshop on Rapid Malcode, WORM '03,* ACM, New York, NY, USA, 2003, pp. 1-10, *https://doi.org/10.1145/948187.948189*.

- Klöckner, J., J. Olk, and B. Rybicki, *Cyberkriminalität: Erpresserschreiben auch an Spahn: Hacker greifen in Coronakrise verstärkt Krankenhäuser an,* Handelsblatt, 9 April 2020, *https://www.handelsblatt.com/technik/medizin/cyberkriminalitaet-erpresserschreiben-auch-an-spahn-hacker-greifen-in-coronakrise-verstaerkt-krankenhaeuser-an/25726550.html*.
- Knud Lasse Lueth, 'State of the IoT 2018: Number of IoT Devices Now at 7B – Market Accelerating', *IoT Analytics,* 8 August 2018, *https://iot-analytics.com/state-of-the-iot-update-q1-q2-2018-number-of-iot-devices-now-7b*.
- Kolias, C., G. Kambourakis, A. Stavrou and J. Voas, 'DDoS in the IoT: Mirai and Other Botnets', *Computer,* Vol. 50, No. 7, 2017, pp. 80-84, 10.1109/MC.2017.201.
- Krebs, B., *Coronavirus Widens the Money Mule Pool,* Krebs on Security, 17 March 2020a, *https://krebsonsecurity.com/2020/03/coronavirus-widens-the-money-mule-pool*.
- Krebs, B., Krebs on Security, Krebs on Security, 30 April 2020b, *https://krebsonsecurity.com*.
- Krebs, B., *MasterCard, VISA Warn of Processor Breach,* Krebs on Security, March 2012, *https://krebsonsecurity.com/2012/03/mastercard-visa-warn-of-processor-breach*.
- Krishnan, M., *Coronavirus Pandemic Used to Stir-up Anti-Muslim Prejeudice in India,* RFI, 13 April 2020, *http://www.rfi.fr/en/international/20200413-coronavirus-pandemic-used-to-stir-up-anti-muslim-prejeudice-in-india*.
- Kunreuther, H. and G. Heal, 'Interdependent Security', *Journal of Risk and Uncertainty,* Vol. 26, No. 2, 1 March 2003, pp. 231-249, *https://doi.org/10.1023/A:1024119208153*.
- Lakshmanan, R., *COVID-Themed Lures Target SCADA Sectors With Data Stealing Malware,* The Hacker News, 20 April 2020a, *https://thehackernews.com/2020/04/coronavirus-scada-malware.html*.
- Lakshmanan, R., *Hackers Created Thousands of Coronavirus (COVID-19) Related Sites As Bait,* The Hacker News, 18 March 2020b, *https://thehackernews.com/2020/03/covid-19-coronavirus-hacker-malware.html*.
- Landers, S., E. Madigan, B. Leff, R.J. Rosati, B.A. McCann, R. Hornbake, R. MacMillan, et al., 'The Future of Home Health Care: A Strategic Framework for Optimizing Value', *Home Health Care Management & Practice,* Vol. 28, No. 4, 1 November 2016, pp. 262–278, *https://doi.org/10.1177/1084822316666368*.
- Larkin, S., C. Fox-Lent, D.A. Eisenberg, B.D. Trump, S. Wallace, C. Chadderton and I. Linkov, 'Benchmarking Agency and Organizational Practices in Resilience Decision Making', *Environment Systems and Decisions,* Vol. 35, No. 2, 1 June 2015, pp. 185-195, *https://doi.org/10.1007/s10669-015-9554-5*.
- Lazari, A., G.-L. Ruzzante, N. Polemi, M. Figwer, R. Neisse and I. Nai Fovino, *European Cybersecurity Centres of Expertise Map: Definitions and Taxonomy,* Joint Research Centre, 11 September 2018, *https://doi.org/10.2760/622400*.
- Leyden, J., *Bitcoin Exchange: Greedy Traders to Blame for DDoS Attack,* The Register, 5 April 2013, *https://www.theregister.co.uk/2013/04/05/bitcoin_ddos_analysis*.
- Mail Online, *Zoom under Scrutiny over Privacy, Porn Hacks,* Mail Online, 31 March 2020, *https://www.dailymail.co.uk/news/article-8173759/US-investigates-Zoom-porn-hacks.html*.
- Makrushin, D., 'The Cost of Launching a DDoS Attack', *Kaspersky,* 23 March 2017, *https://securelist.com/the-cost-of-launching-a-ddos-attack/77784*.
- Malwarebytes Threat Intelligence Team, *APTs and COVID-19: How Advanced Persistent Threats Use the Coronavirus as a Lure,* Malwarebytes Labs, 9 April 2020a, *https://blog.malwarebytes.com/threat-analysis/2020/04/apts-and-covid-19-how-advanced-persistent-threats-use-the-coronavirus-as-a-lure*.
- Malwarebytes Threat Intelligence Team, *Fake 'Corona Antivirus' Distributes BlackNET Remote Administration Tool,* Malwarebytes Labs, 23 March 2020b, *https://blog.malwarebytes.com/threat-analysis/2020/03/fake-corona-antivirus-distributes-blacknet-remote-administration-tool*.
- Matheu-García, S., J. Hernández-Ramos, A. Skarmeta, G. Baldini, P. Cousin and F. Le.Gall, *Towards a Standardized Cybersecurity Certification Framework for the IoT,* ARMOUR project and the University of Murcia, 2018, *https://www.armour-project.eu/wp-content/uploads/2018/01/white_paper_ARMOUR-IoT-Certification.pdf*.
- McAfee, *McAfee Mobile Threat Report Q1, 2018,* 2018, *https://www.mcafee.com/enterprise/en-us/assets/reports/rp-mobile-threat-report-2018.pdf*.

- McGee, M.K., *Genetic Testing Lab Hack Affects 233,000,* GovInfoSecurity, 24 April 2020, *https://www.govinfosecurity.com/genetic-testing-lab-hack-affects-233000-a-14182*.
- Merchdope, *37 Mind Blowing YouTube Facts, Figures and Statistics – 2019,* MerchDope, 26 February 2020, *https://merchdope.com/youtube-stats*.
- Miller, M., *Experts Worry US Elections Even More Vulnerable with COVID-19,* The Hill, 30 April 2020, *https://thehill.com/policy/cybersecurity/495364-election-resources-stretched-thin-by-dual-focus-on-mail-in-voting-and*.
- Mittelman, G., *Harden Endpoint Security for COVID-19 and Working from Home with Threat & Vulnerability Management,* Microsoft, 30 April 2020, *https://techcommunity.microsoft.com/t5/microsoft-defender-atp/harden-endpoint-security-for-covid-19-and-working-from-home-with/ba-p/1343641*.
- Moor, J., 'The Dartmouth College Artificial Intelligence Conference: The Next Fifty Years', *AI Magazine,* Vol. 27, No. 4, 15 December 2006, p. 87, *https://doi.org/10.1609/aimag.v27i4.1911*.
- Moore, T., S. Dynes and F. Chang, 'Identifying How Firms Manage Cybersecurity Investment', Berkeley, CA, 2016, *https://tylermoore.utulsa.edu/ciso15ibm.pdf*.
- Nai Fovino, I., R. Neisse, J. Hernández-Ramos, N. Polemi, G.-L. Ruzzante, M. Figwer and A. Lazari, *A Proposal for a European Cybersecurity Taxonomy,* Joint Research Centre, 6 November 2019, *http://dx.doi.org/10.2760/106002*.
- National Audit Office (NAO), *Investigation: WannaCry Cyber Attack and the NHS,* 25 April 2018, *https://www.nao.org.uk/wp-content/uploads/2017/10/Investigation-WannaCry-cyber-attack-and-the-NHS.pdf*.
- National Security Agency, *Selecting and Safely Using Collaboration Services for Telework,* 24 April 2020, *https://media.defense.gov/2020/Apr/24/2002288652/-1/-1/0/CSI-SELECTING-AND-USING-COLLABORATION-SERVICES-SECURELY-LONG-FINAL.PDF*.
- Netcraft, *Netcraft - About Netcraft,* Netcraft, 2020, *https://www.netcraft.com/about-netcraft*.
- Nielsen, M.A. and I.L. Chuang, *Quantum Computation and Quantum Information: 10th Anniversary Edition,* 10th ed., Cambridge University Press, New York, NY, USA, 2011, *https://www.worldcat.org/title/quantum-computation-and-quantum-information/oclc/844974180*.
- O'Connor, C., *FBI Warns of Major Spike in Cyber Attacks,* Security Boulevard, 30 April 2020, *https://securityboulevard.com/2020/04/fbi-warns-of-major-spike-in-cyber-attacks*.
- O'Donnell, L., *Overlay Malware Leverages Chrome Browser, Targets Banks and Heads to Spain,* Threatpost, 13 April 2020, *https://threatpost.com/overlay-malware-exploits-chrome-browser-targets-banks-and-heads-to-spain/154713*.
- OECD, *OECD Digital Economy Outlook 2017,* OECD, 2017, *https://doi.org/10.1787/9789264276284-en*.
- Omale, G., 'Gartner Identifies Top 10 Strategic IoT Technologies and Trends', *Gartner,* 7 November 2018, *https://www.gartner.com/en/newsroom/press-releases/2018-11-07-gartner-identifies-top-10-strategic-iot-technologies-and-trends*.
- Osborne, C., *Proposed Government Coronavirus Tracking App Falls at the First Hurdle Due to Data Breach,* ZDNet, 20 April 2020, *https://www.zdnet.com/article/proposed-government-coronavirus-app-falls-at-the-first-hurdle-due-to-data-breach*.
- Osoba, O.A. and W.I. Welser, *The Risks of Artificial Intelligence to Security and the Future of Work,* RAND, 2017, *https://doi.org/10.7249/PE237*.
- Palmer, D., *VPN Use Surges as Coronavirus Outbreak Prompts Huge Rise in Remote Working,* ZDNet, 23 March 2020, *https://www.zdnet.com/article/vpn-use-surges-as-coronavirus-outbreak-prompts-huge-rise-in-remote-working*.
- Panda, A., *Offensive Cyber Capabilities and Public Health Intelligence: Vietnam, APT32, and COVID-19,* The Diplomat, 24 April 2020, *https://thediplomat.com/2020/04/offensive-cyber-capabilities-and-public-health-intelligence-vietnam-apt32-and-covid-19*.
- Paxson, V., 'Bro: A System for Detecting Network Intruders in Real-Time', *Computer Networks,* Vol. 31, No. 23, 14 December 1999, pp. 2435-2463, *https://doi.org/10.1016/S1389-1286(99)00112-7*.
- Pingdom, 'The Incredible Growth of the Internet since 2000', *Pingdom Royal,* 22 October 2010, *https://royal.pingdom.com/incredible-growth-of-the-internet-since-2000*.

Ponemon Institute, *Cost of a Data Breach Study,* IBM Security, July 2018, *https://www.ibm.com/security/data-breach*.

Porter, S., *Cyberattack on Czech Hospital Forces Tech Shutdown during Coronavirus Outbreak,* Healthcare IT News, 19 March 2020, *https://www.healthcareitnews.com/news/europe/cyberattack-czech-hospital-forces-tech-shutdown-during-coronavirus-outbreak*.

Pressey, D., *C-U Public Health District's Website Held Hostage by Ransomware Attack,* The News-Gazette, 11 March 2020, *https://www.news-gazette.com/news/local/health-care/c-u-public-health-districts-website-held-hostage-by-ransomware-attack/article_2dadedcd-aadb-5cb1-8740-8bd9e8800e27.html*.

Quantum Flagship, *Quantum Communication,* Quantum Technology, 2019a, *https://qt.eu/discover/applications-of-qt/quantum-communication*.

Quantum Flagship, *Quantum Technology | The Future Is Quantum,* Quantum Technology, 2019b, *https://qt.eu/*.

Quinn, B. and C. Arthur, 'PlayStation Network Hackers Access Data of 77 Million Users', *The Guardian,* 26 April 2011, *https://www.theguardian.com/technology/2011/apr/26/playstation-network-hackers-data*.

Radware, 'The Trust Factor: Cybersecurity's Role in Sustaining Business Momentum', *Radware,* 1 December 2019, *https://www.radware.com/documents/infographics/trust-factor-cybersecurity-sustaining-business*.

Reinsel, D., J. Gantz and J. Rydning, *The Digitization of the World, From Edge to Core,* IDC, November 2018, *https://www.seagate.com/files/www-content/our-story/trends/files/idc-seagate-dataage-whitepaper.pdf*.

Reynolds, C., US, *UK Warn of Widespread Scanning for Unpatched VPNs, Citrix Vulnerability,* Computer Business Review, 9 April 2020, *https://www.cbronline.com/news/covid-19-hacking-advisories*.

Ross, R., M. Swanson, G. Stoneburner, S. Katzke and L. Johnson, *Guide for the Security Certification and Accreditation of Federal Information Systems,* National Institute of Standards and Technology, 20 May 2004, *https://doi.org/10.6028/NIST.SP.800-37*.

Ross, R.S., 'Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy', *NIST,* 20 December 2018, *https://doi.org/10.6028/NIST.SP.800-37r2*.

Russell, D., *COVID-19 Exploits and Vulnerabilities,* Yorkshire & Humber Regional Organised Crime Unit, 2020, *http://www.yhrocu.org.uk/departments/regional-cyber-crime-unit/covid-19-information/covid-19-exploits-and-vulnerabilities*.

Russell, S.J. and P. Norvig, *Artificial Intelligence: A Modern Approach,* Third edition, Global edition., Prentice Hall Series in Artificial Intelligence, Pearson, Boston Columbus Indianapolis, 2016, *https://doi.org/10.1017/s0269888900007724*.

Sasse, M.A., S. Brostoff and D. Weirich, 'Transforming the 'Weakest Link' – a Human/Computer Interaction Approach to Usable and Effective Security', *BT Technology Journal,* Vol. 19, No. 3, 1 July 2001, pp. 122-131, *https://doi.org/10.1023/A:1011902718709*.

Satter, R., J. Stubbs, and C. Bing, *Exclusive: Elite Hackers Target WHO as Coronavirus Cyberattacks Spike,* Reuters, 24 March 2020, *https://www.reuters.com/article/us-health-coronavirus-who-hack-exclusive-idUSKBN21A3BN*.

Schaake, M., L.M. Pupillo, A.H.B. Ferreira, G. Varisco and Centre for European Policy Studies, *Software Vulnerability Disclosure in Europe: Technology, Policies and Legal Challenges: Report of a CEPS Task Force,* 2018, *https://dl.acm.org/doi/book/10.5555/3306854*.

Scheels, C., *EXPOSED: Poor VPN Performance Handcuffs Remote Workforce,* AppGate, 27 March 2020, *https://www.appgate.com/blog/software-defined-perimeter/exposed-poor-vpn-performance-handcuffs-remote-workforce*.

Schmidt, A., *A Fierce Domain: Conflict in Cyberspace,* 1986 to 2012, Edited by J. Healey, Cyber Conflict Studies Association, Vienna, VA, 2013, *https://www.directtextbook.com/isbn/9780989327404*.

Schneier, B., 'Cybersecurity for the Public Interest', *IEEE Security Privacy,* Vol. 17, No. 1, January 2019a, pp. 84-83, *https://doi.org/10.1109/MSEC.2018.2889891*.

Schneier, B., 'Prices for Zero-Day Exploits Are Rising - Schneier on Security', *Schneier on Security,* 17 January 2019b, *https://www.schneier.com/blog/archives/2019/01/prices_for_zero.html*.

Seals, T., *Revamped HawkEye Keylogger Swoops in on Coronavirus Fears,* Threatpost, 20 March, 2020, *https://threatpost.com/revamped-hawkeye-keylogger-coronavirus-fears/154013*.

- Sebenius, A., and K. Mehrotra, *Zoom Struggles With Security Flaws as Demand for Videoconferencing Spikes,* Time, 3 April 2020, *https://time.com/5814981/zoom-videoconferencing-security-flaws-coronavirus*.
- Serajul Quadir, 'How a Spelling Mistake Stopped Hackers Stealing $1bn in a Bank Heist', *The Independent,* 11 March 2016, *http://www.independent.co.uk/news/world/asia/spelling-mistake-stops-hackers-stealing-1-billion-in-bangladesh-bank-heist-a6924971.html*.
- Shcherbakova, T., *COVID-19 in Spam and Phishing Related to Deliveries,* Kaspersky Daily, 27 April 2020, *https://www.kaspersky.com/blog/covid-fake-delivery-service-spam-phishing/35125*.
- Shor, P.W., 'Algorithms for Quantum Computation: Discrete Logarithms and Factoring', *Proceedings of the 35th Annual Symposium on Foundations of Computer Science,* IEEE Comput. Soc. Press, Santa Fe, NM, USA, 1994, pp. 124-134, *https://doi.org/10.1109/SFCS.1994.365700*.
- Smart, W., *Lessons Learned Review of the WannaCry Ransomware Cyber Attack,* 1 February 2018, *https://www.england.nhs.uk/wp-content/uploads/2018/02/lessons-learned-review-wannacry-ransomware-cyber-attack-cio-review.pdf*.
- StatCounter, *StatCounter Global Stats - Browser, OS, Search Engine Including Mobile Usage Share,* StatCounter Global Stats, 2020, *https://gs.statcounter.com*.
- Stein, S., and J. Jacobs, *Cyber-Attack Hits U.S. Health Agency Amid Covid-19 Outbreak,* Bloomberg, 16 March 2020, *https://www.bloomberg.com/news/articles/2020-03-16/u-s-health-agency-suffers-cyber-attack-during-covid-19-response*.
- Styczynski, J., N. Beach-Westmoreland and S. Stables, *When the Lights Went Out,* Booz Allen Hamilton, 2016, *https://www.boozallen.com/content/dam/boozallen/documents/2016/09/ukraine-report-when-the-lights-went-out.pdf*.
- Svenmarck, P., L. Luotsinen, M. Nilsson and J. Schubert, *Possibilities and Challenges for Artificial Intelligence in Military Applications,* Swedish Defence Research Agency, 25 May 2018, *https://www.sto.nato.int/publications/STO%20Meeting%20Proceedings/STO-MP-IST-160/MP-IST-160-S1-5.pdf*.
- Symantec, *Financial Threats Review 2017, Internet Security Threat Report,* May 2017, *https://www.symantec.com/content/dam/symantec/docs/security-center/white-papers/istr-financial-threats-review-2017-en.pdf*.
- Symantec, *Mobile Threat Intelligence Report, 2017: The Year In Review,* 2018, *https://www.symantec.com/content/dam/symantec/docs/reports/mobile-threat-intelligence-report-2017-en.pdf*.
- The Hacker News, *How CISOs Should Prepare for Coronavirus Related Cybersecurity Threats,* The Hacker News, 18 March 2020, *https://thehackernews.com/2020/03/coronavirus-cybersecurity-ciso.html*.
- The Potomac Institute for Policy Studies, 'Cyber Readiness Index (CRI)', *The Potomac Institute for Policy Studies,* 2016, *https://www.potomacinstitute.org/academic-centers/cyber-readiness-index*.
- Tidy, J., *Coronavirus: How Hackers Are Preying on Fears of Covid-19,* BBC News, 13 March 2020a, sec. Technology, *https://www.bbc.com/news/technology-51838468*.
- Tidy, J., *Coronavirus: Israel Enables Emergency Spy Powers,* BBC News, 17 March 2020b, sec. Technology, *https://www.bbc.com/news/technology-51930681*.
- Travagnin, M. and A. M. Lewis, *Quantum Key Distribution, in-field implementations, technology assessment of QKD deployments,* Scientific and Technical Research Report, 15 October 2019, *https://doi.org/10.2760/38407*.
- Travagnin, M., A.M. Lewis, C. Ferigato and E. Florescu, *The Impact of Quantum Technologies on the EU's Future Policies. Part 3, Perspectives for Quantum Computing.,* Scientific and Technical Research Report, 15 November 2018, *https://doi.org/10.2760/737170*.
- Treverton, G.F., A. Thvedt, A.R. Chen, K. Lee and M. McCue, *Addressing Hybrid Threats,* Försvarshögskolan (FHS), 2018, *http://urn.kb.se/resolve?urn=urn:nbn:se:fhs:diva-7574*.
- Twitter Investor Relations, *Q4 and Fiscal Year 2018 Letter to Shareholders,* Twitter, 7 February 2019, *https://s22.q4cdn.com/826641620/files/doc_financials/2018/q4/Q4-2018-Shareholder-Letter.pdf*.
- Upatham, P., and J. Treinen, *Amid COVID-19, Global Orgs See a 148% Spike in Ransomware Attacks; Finance Industry Heavily Targeted,* VMware Carbon Black, 15 April 2020, *https://www.carbonblack.com/2020/04/15/amid-covid-19-global-orgs-see-a-148-spike-in-ransomware-attacks-finance-industry-heavily-targeted*.

- US Department of Defense, *Department of Defense Cyber Strategy,* 2018, *https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF*.
- US Government, *National Cyber Strategy,* The White House, 2018, *https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf*.
- Varghese, S., Algerian Petroleum JV Hit by Maze Ransomware, Data Posted Online, ITWire, 6 April 2020, *https://www.itwire.com/security/algerian-petroleum-jv-hit-by-maze-ransomware,-data-posted-online.html*.
- Varian, H., 'System Reliability and Free Riding', in L.J. Camp and S. Lewis (eds.), *Economics of Information Security, Advances in Information Security,* Springer US, Boston, MA, 2004, pp. 1-15, *https://doi.org/10.1007/1-4020-8090-5_1*.
- Villani, C., *For A Meaningful Artificial Intelligence: Towards A French And European Strategy,* March 2018, *https://www.aiforhumanity.fr/pdfs/MissionVillani_Report_ENG-VF.pdf*.
- Volz, D., 'Yahoo Says Hackers Stole Data from 500 Million Accounts in 2014', Reuters, 23 September 2016, *https://www.reuters.com/article/us-yahoo-cyber-idUSKCN11S16P*.
- Waldron, K., *Resources for Measuring Cybersecurity,* R Street, October 2019, *https://www.rstreet.org/wp-content/uploads/2019/10/Final-Cyberbibliography-2019.pdf*.
- Waqas, *Exclusive: Scammers Using Fake WHO Bitcoin Wallet to Steal Donation,* HackRead, 26 April 2020, *https://www.hackread.com/scammers-use-fake-who-bitcoin-wallet-steal-donation*.
- Welch, C., 'Over 150 Million Breached Records from Adobe Hack Have Surfaced Online', *The Verge,* 7 November 2013, *https://www.theverge.com/2013/11/7/5078560/over-150-million-breached-records-from-adobe-hack-surface-online*.
- White, J.C., N.C. Coops, M.A. Wulder, M. Vastaranta, T. Hilker and P. Tompalski, 'Remote Sensing Technologies for Enhancing Forest Inventories: A Review', *Canadian Journal of Remote Sensing,* Vol. 42, No. 5, 2 September 2016, pp. 619-641, *https://doi.org/10.1080/07038992.2016.1207484*.
- Whittaker, Z., *Hackers Publish ExecuPharm Internal Data after Ransomware Attack,* TechCrunch, 27 April 2020, *https://techcrunch.com/2020/04/27/execupharm-clop-ransomware/?guccounter=1*.
- Wilson, J.Q. and G.L. Kelling, 'Broken Windows', *The Atlantic,* 1 March 1982, *https://www.theatlantic.com/magazine/archive/1982/03/broken-windows/304465*.
- World Economic Forum, *Cyber Resilience: Playbook for Public-Private Collaboration,* January 2018, *https://www.weforum.org/reports/cyber-resilience-playbook-for-public-private-collaboration*.
- World Health Organization, *Beware of Criminals Pretending to Be WHO,* World Health Organization, 2020, *https://www.who.int/about/communications/cyber-security*.
- World Health Organization, *Munich Security Conference,* World Health Organization, 15 February 2020, *https://www.who.int/dg/speeches/detail/munich-security-conference*.
- Zecops Research Team, 'You've Got (0-Click) Mail!', *ZecOps Blog,* April 20, 2020, *https://blog.zecops.com/vulnerabilities/youve-got-0-click-mail*.
- Zetter, K., 'Hackers Finally Post Stolen Ashley Madison Data', *Wired,* 18 August 2015, *https://www.wired.com/2015/08/happened-hackers-posted-stolen-ashley-madison-data*.

LIST OF TABLES AND BOXES

LIST OF FIGURES

ACKNOWLEDGEMENTS

The main contributors to this report were: Igor Nai Fovino (ed, auth), Geraldine Barry (ed), Stephane Chaudron (ed, auth), Iwen Coisel (ed, auth), Marion Dewar (ed), Henrik Junklewitz (ed, auth), Georgios Kambourakis (ed, auth), Ioannis Kounelis (ed, auth), Barbara Mortara (ed), Jean-Pierre Nordvik (ed, auth), Ignacio Sanchez (ed, auth), Gianmarco Baldini (auth), Josefa Barrero (auth), Gerard Draper (auth), Nestor Duch-Brown (auth), Olivier Eulaerts (auth), Dimitrios Geneiatakis (auth), Geraldine Joanny (auth), Stephanie Kerckhof (auth), Adam Lewis (auth), Tania Martin (auth), Stefano Nativi (auth), Ricardo Neisse (auth), Demosthenes Papameletiou (auth), José Ramos (auth), Vittorio Reina (auth), Gianluigi Ruzzante (auth), Luigi Sportiello (auth), Gary Steri (auth), Salvatore Tirendi (auth).
Additionally, we would like to thank Laura Spirito and Massimiliano Gusmini for taking care of the graphical aspects of the report.

We are also grateful to the many other colleagues from the following JRC units who offered their support and feedback:

- B.6 Digital Economy
- E.2 Technology Innovation in Security
- E.3 Cyber & Digital Citizens' Security
- E.7 Knowledge for Security and Migration
- F.2 Consumer Products Safety
- H.2 Knowledge Management Methodologies, Communities and Dissemination
- I.3 Text and Data Mining

We are particularly grateful to the reviewers for their insightful comments and constructive feedback:

- CERT-EU: Saâd Kadhi, Arthur De Liedekerke Beaufort
- DG CNECT: Miguel Gonzalez-Sancho
- DG DIGIT: Ken Ducatel
- DG ENER: Stephan Lechner
- DG HOME: Cathrin Bauer-Bulst, Andrea De Candido, Michele Socco
- ENISA: Ann Charlott Andersson, Steven Purser

Finally, a special big thank you goes to the many colleagues from different services for printing, distributing, registering, and assisting in the finalisation of this report.

GETTING IN TOUCH WITH THE EU

IN PERSON

All over the European Union there are hundreds of Europe Direct information centres. You can find the address of the centre nearest you at: ***https://europa.eu/european-union/contact_en***.

ON THE PHONE OR BY EMAIL

Europe Direct is a service that answers your questions about the European Union. You can contact this service:

- by freephone: **00 800 6 7 8 9 10 11** (certain operators may charge for these calls),
- at the following standard number: **+32 22999696,** or
- by electronic mail via: ***https://europa.eu/european-union/contact_en***.

FINDING INFORMATION ABOUT THE EU

ONLINE

Information about the European Union in all the official languages of the EU is available on the Europa website at: ***https://europa.eu/european-union/index_en***.

EU PUBLICATIONS

You can download or order free and priced EU publications from EU Bookshop at: ***https://publications.europa.eu/en/publications.*** Multiple copies of free publications may be obtained by contacting Europe Direct or your local information centre (see ***https://europa.eu/european-union/contact_en***).

EU LAW AND RELATED DOCUMENTS

For access to legal information from the EU, including all EU law since 1952 in all the official language versions, go to EUR-Lex at: ***http://eur-lex.europa.eu***.

OPEN DATA FROM THE EU

The EU Open Data Portal ***(http://data.europa.eu/euodp/en)*** provides access to datasets from the EU. Data can be downloaded and reused for free, for both commercial and non-commercial purposes.

KJ-NA-30276-EN-N

The European Commission's science and knowledge service

Joint Research Centre

JRC Mission

As the science and knowledge service of the European Commission, the Joint Research Centre's mission is to support EU policies with independent evidence throughout the whole policy cycle.

EU Science Hub

ec.europa.eu/jrc

@EU_ScienceHub

EU Science Hub - Joint Research Centre

EU Science, Research and Innovation

EU Science Hub

Publications Office of the European Union

ISBN 978-92-76-19957-1
doi:10.2760/352218