European Commission

CYBERSECURITY

OUR DIGITAL ANCHOR

A EUROPEAN PERSPECTIVE

EXECUTIVE SUMMARY

EUR 30277 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 30277 EN

PDF	ISBN 978-92-76-19959-5	ISSN 1831-9424	doi:10.2760/33974	KJ-NA-30277-EN-N
Print	ISBN 978-92-76-19960-1	ISSN 1018-5593	doi:10.2760/575498	KJ-NA-30277-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 – executive summary,* EUR 30277 EN, Publications Office of the European Union, Luxembourg, 2020, ISBN 978-92-76-19959-5, doi:10.2760/33974, JRC121051.

EXECUTIVE SUMMARY

EXECUTIVE SUMMARY

We are living in an era of great opportunities enabled by digital technologies. However, the advantages provided by digitisation could be at risk because the more digital our societies become, the more vulnerable they are to the deliberate exploitation of unsecure digital systems. Thus, more robust cybersecurity is essential to establish the trust without which the digital society cannot function. It can no longer be considered as an optional extra, but must be seen as an essential societal need.

The COVID-19 crisis has thrown the importance of cybersecurity into sharp relief. Measures put in place to combat the pandemic have resulted in unprecedented dependence on digital communications and online services. This is an opportunity for cyber attackers to exploit weaknesses and increase profits. The likely impact of attacks has increased, especially when hospitals or key medical facilities are targeted. It remains to be seen whether or not some of the changes the pandemic has brought about become permanent – for example, the greater use of teleworking. If so, the cybersecurity will become increasingly important.

The **'Cybersecurity: our digital anchor'** report gathers research from different disciplinary fields at the Joint Research Centre (JRC), the European Commission's science and knowledge service. It provides multidimensional insights into the challenges of cybersecurity and considers possible solutions.

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

Cybersecurity, a moving target

Today, cybersecurity risks are increasing for the following reasons:

More threat actors with more diverse motivations

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 and will be **more profitable than the global trade in all major illegal drugs combined,** putting at risk the incentives for innovation and investment.

Moreover, it is not only cyber criminals who are a cause for concern – i.e. those attacking digital systems for the sake of making a monetary or other type of profit. Now that digital services are at the heart of every critical infrastructure, their cybersecurity is already – and will become increasingly – a matter of **national security**.

Cybersecurity is also becoming a major concern as regards terrorism, hybrid threats and hacktivism.

Attackers are using more sophisticated attack tools. In particular, there has been a constant rise in the use of malware – i.e. code that invades a system or service and affects its normal behaviour, for instance, by granting non-authorised access or leaking private information. In the past five years, this has become the most frequently used attack vector.

Technological developments create new vulnerabilities

As the internet evolves, so do systemic weaknesses and vulnerabilities. We now have the Internet of Things (IoT) – multiple devices connected to the internet, including everyday items, such as fridges, and devices carried by individuals (e.g. smartphones or wearables). These IoT devices gather vast amounts of data about themselves and their environments as they perceive them (big data). Such data can be analysed and used to inform decisions (in business, government, etc.).

The more devices in our lives we connect to the internet, the more entry points we make available to bad actors. This is risky because IoT devices might have vulnerabilities rooted in their design, implementation and deployment. Most are designed to focus only on providing a target functionality, and with restricted budget (they must be cheap to take off in the market), hence with little attention being paid to cybersecurity issues.

In the past, many organisations relied on a 'segregate or isolate and defend' approach to cybersecurity, like building a castle with fortified walls and pulling up the drawbridge. However, in a globally interconnected digital ecosystem, this old 'castle wall' paradigm has become obsolete. Organisations hoping to benefit from the IoT and big data must remain open.

We therefore need to switch to a more collaborative and distributed 'device-by-device' defence. The aim must be to enable a more accurate and distributed monitoring of cybersecurity across all elements of the digital value chain.

Moreover, the big data paradigm involves the transmission of huge amounts of data to the cloud to be stored and/or processed. Decisions must be based on up-to-date data analysis, which means data has to be collected and analysed in real time. Thus, hyper-connectivity i.e. pervasive (99.99) connectivity is required all the time. However, recent episodes have shown that attacks against internet connectivity are feasible since the internet backbone does not have centralised governance which means its security cannot be homogeneously enforced.

Finally, the big data paradigm relies on the quality of the data collected to extrapolate new results, evidence and services. Today, the injection of fake data is the new frontier for cyber attacks.

> "We need to switch to *a more collaborative and distributed 'device-by-device' defence.*"

Greater impact of attacks

Not only are cyber attacks more likely but their potential impact has increased, too, as a result of the ever-growing interdependencies between heterogeneous digital services. The number of citizens currently impacted simultaneously by a single cyber incident can be huge, due to the pervasiveness of connected devices.

Moreover, 5G will enable new use cases, such as remote real-time surgery, smarter and self-driving vehicles, drone control and a higher degree of industry automation. The criticality of these applications means that, if communications networks fail, the impact on our economies and societies could be substantial.

Historically, a type of cause-and-effect trend has guided the evolution of cybersecurity: the rise of new digital technologies, followed by the discovery of new vulnerabilities for which, in turn, further remediations were identified.

However, given the increased complexity and impact of cyber attacks today, this type of evolutionary approach is no longer adequate. We need to move from a passive model, where cybersecurity is seen as an 'add-on' to be injected into a second phase of the digital evolution, to a proactive one, where cybersecurity becomes the central element of digital design from the beginning ('security by design').

Artificial intelligence (AI) is part of the solution to these challenges. The application of at least partly autonomous algorithms in cybersecurity dates back to the 1990s. However, cybersecurity is increasingly affected by recent developments in AI, particularly machine learning which enables systems to become smarter and to identify progressively more complex threats as they are developed. However, while AI will bring clear benefits to cybersecurity, it will also introduce new challenges.

Cybersecurity, the challenges

We have seen above that constant connectivity and data sharing in the world of the IoT and big data are increasing cybersecurity risks. Efforts to mitigate these risks do not happen in a vacuum; economic and societal challenges will make the task more difficult.

Economic challenges

In most industries, **market forces** generate the necessary incentives for companies to improve their products and services. However, these forces seem inadequate in the cybersecurity domain. First, there is relatively little competition. For instance, the desktop operating system industry is dominated by two companies, while the mobile operating system segment is also characterised by a duopoly, a trend which applies to most digital sectors. This absence of effective competition adversely impacts the incentive for developers to produce secure code. Similarly, in markets with dominant suppliers, users tend to have very little bargaining power.

> Cultivating a cybersecurity-conscious approach *will lead in dealing with risks at an early stage.*

They are not able to exert much pressure on vendors to provide solutions to exposed vulnerabilities, resulting either in delayed releases of solutions or poor-quality ones.

Societal challenges

Unfortunately, the shift from the physical to the digital world is still not fully understood by the majority of people. To take one example, we all pay attention to our physical ID card and our credit cards but, paradoxically, we often forget to protect our credentials when using digital platforms such as Amazon or Facebook. The misleading assumption that 'since it is not physical, it is not important' makes an impact not only on the daily use of digital services but also, at a higher level, on the definition of strategic industrial decisions.

Balancing fundamental rights with cybersecurity can be challenging. For example, how can we ensure the right balance in processing personal data necessary for certain cybersecurity operations? How can we implement cybersecurity measures to combat hate speech or fake information campaigns without infringing on a citizen's right to freedom of expression? Cybersecurity as a discipline has no choice but to confront these issues.

For all these reasons, we must see cybersecurity as a societal, not just a technological, challenge. It requires behavioural change in all parts of society. It is a matter of education, culture, politics and policies. In other words, it is not only about adopting a security-by-design approach to products and services, but also building a 'secure digital society by design'.

Cybersecurity, the way forward

The task of achieving a 'secure digital society by design' must be tackled from a number of angles.

Ethics and rights

Balancing cybersecurity with fundamental rights requires a clear legal framework as well as clear guidance as to how the law should be interpreted and applied. In the case of the GDPR, best practices for cybersecurity experts still need to be established in detail.

Nor is it just a question of the law (which determines what we have to do) and its implementation. There are also questions of ethics (which propose what we should do), new social norms and good practices.

These issues require a collaborative effort from policymakers, legal experts, researchers, business leaders and cybersecurity experts.

(A lifelong) education

The job market is currently unable to respond to the growing demand for skilled people in the field of cybersecurity. Today, a visible consequence of this is the 1 million shortfall in employees which is expected to grow in the future.

A short-term answer to this problem is to **encourage existing workers to engage in a continuous education programme related to cybersecurity,**

> *Cybersecurity by design requires coherent and coordinated cyber secure policies by design.*

leading perhaps to a cybersecurity certification. International certification schemes exist which are recognised by industry, such as the Certified Information Systems Security Professional (CISSP). However, a European scheme could be designed to better address the type of expertise currently needed in Europe.

A longer-term solution is to **integrate the teaching of cybersecurity skills into school and university curricula.** This might encourage more young people to take up cybersecurity professions. Even if they enter other fields, their cybersecurity knowledge might well prove useful. More educated end-users will also demand more cyber secure digital products and services, creating extra incentives for industry to provide more of them.

Industry and digital services

In addition to the pressure from more educated end-users, firms' behaviour could be further altered if they were held liable for breaches of their cybersecurity obligations. For this reason, some have suggested that liability **legislation could be developed for products and services from a cybersecurity perspective. Although this might well improve consumer safety, enforcing such legislation would be a challenge.**

Standards are vital for ensuring that the design of products and services anticipates future cybersecurity risks. They should ensure the **interoperability of products and services** across all relevant layers of existing systems. Cybersecurity measures that are not interoperable across devices are often ignored.

It is not just a matter of integrating security into the initial design of a product or service. Vulnerabilities will emerge during the complete life cycle of products and services, so an effective strategy is essential to manage these, including vulnerability disclosure policies.

More transparent reporting of cyber incidents would allow firms to benefit from each other's misfortunes. However, many are reluctant to do this, fearing the effects on their share prices, even though such effects tend to be short-lived. Therefore, disclosure policies must be fairly balanced.

Improved coordination of research

Cybersecurity has to progress at the same speed or even faster than the digital society to be able to anticipate rising threats. Research is at the basis of every evolution and, as such, is crucial.

A recent study conducted by the JRC, mapping the cybersecurity research and development capabilities in Europe, shows a research community that is vibrant, productive, and recognised worldwide. However, better coordination of cybersecurity research funding is required throughout the EU

to ensure focus areas are properly addressed and not fragmented across many different research projects.

It is also urgent **to improve the magnitude of technology and innovation transfer to the market using research project outputs.** Patent filing is dominated by China, followed by the USA, while the EU is not in a prominent position. This is an extremely relevant critical issue from a European strategic autonomy perspective, too, since it introduces a dependency on products and services not available in the EU internal market.

Weak economic incentives in the sector imply that companies invest less in research and innovation.

A common culture of collaboration in cybersecurity

To enhance cybersecurity, silos between sometimes very different communities and fields need to be broken. Equally, Member States would all benefit if they cooperated more closely with each other.

Reinforced sharing of **cyber threat intelligence,** for example, will enable development of the most effective mitigation techniques and resilience mechanisms.

The establishment of a common culture of collaboration might also encourage firms to disclose cybersecurity breaches. A possible step towards this goal would be the **establishment of a central European platform for vulnerability management,** coordinating and encouraging the efforts of the cybersecurity community.

Ensure secure policy by design (governance)

As digital permeates across more and more areas of policy- and law-making, practices should **guarantee that considerations of cybersecurity are built into the processes of policymaking and governance from the outset.**

To this end, we should consider developing **a coordinated European framework for the full alignment of cybersecurity policy initiatives and actions at EU and Member-State level.**

Such an initiative will be key to ensuring the harmonisation and homogenisation of cybersecurity across Europe and is a significant step towards building a secure digital society for all European citizens.

Harness and adapt to emerging technologies

Although two technological areas – blockchain and quantum computing – are still at their nascent stage, they may be disruptive in the future.

Blockchain enables parties with no particular trust in each other to carry out transactions involving assets – i.e. things of value, such as money, intellectual property, stocks or bonds – on a peer-to-peer basis without the need for a 'middleman' or trusted third party.

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

Transactions are recorded in a single database or digital leger which is stored in a distributed network and is open to all. They are verified not by a middle-man, such as a bank, but via peer consensus, i.e. by the multiple connected nodes in the network.

From a cybersecurity perspective, the intrinsic nature of blockchain presents a unique set of advantages. A system without a single point of failure is harder to corrupt, since a hack into one part of the system will not affect others.

Quantum computers or quantum communication applications are still very experimental and probably quite a long way from widespread usability. However, they can have a potentially transformative impact on cryptography and information security. Two developments of particular relevance to cybersecurity are **post-quantum cryptography,** that is the study of quantum-resistant cryptographical schemes to replace the old algorithms, and the development of **quantum cryptography** techniques to improve the security of systems and devices.

Towards a cyber secure future

In February 2020, the Commission published its ideas and actions for a digital transformation powered by digital solutions that put people first, open up new opportunities for businesses, and boost the development of trustworthy technology to foster an open and democratic society and a vibrant and sustainable economy. Cybersecurity underpins this Commission priority of 'a Europe fit for a digital age'. A European framework to facilitate the development and marketing of cybers ecure technologies will be key to making this happen.

This report 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.

While the world as we once knew it has changed significantly due to COVID-19, the relevance of cybersecurity to our lives, whether as policymakers or individuals, has never been greater.

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-30277-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 978-92-76-19959-5
doi:10.2760/33974