Techno-Politics Series: 3

European Cybersecurity in Context

A Policy-Oriented Comparative Analysis

Edited by
Luigi Martino
Nada Gamal

Series Editor
Antonios Nestoras

Techno-Politics Series: 3

European Cybersecurity in Context

A Policy-Oriented Comparative Analysis

Edited by
Luigi Martino
Nada Gamal

Series editor
Antonios Nestoras

Published by the European Liberal Forum. Co-funded by the European Parliament.

The European Liberal Forum (ELF) is the official political foundation of the European Liberal Party, the ALDE Party. Together with 47 member organisations, we work all over Europe to bring new ideas into the political debate, to provide a platform for discussion, and to empower citizens to make their voices heard. Our work is guided by liberal ideals and a belief in the principle of freedom. We stand for a future-oriented Europe that offers opportunities for every citizen. ELF is engaged on all political levels, from the local to the European. We bring together a diverse network of national foundations, think tanks and other experts. In this role, our forum serves as a space for an open and informed exchange of views between a wide range of different EU stakeholders.

Graphic design: E&P Design
Page layout: Cheshire Typesetting Ltd, Cuddington, Cheshire
Editors: Luigi Martino, Nada Gamal
ISBN: 978-2-39067-035-3 / 9782390670353
ISSN (print): 2791-3880
ISSN (online): 2791-3899

This volume has been published in collaboration with the Center for Cyber Security and International Relations Studies, University of Florence

Contents

Foreword

Daniel Kaddik, ELF Executive Director

Worldwide connectivity has unleashed global digitalisation, creating cross-border social networks for communicating and spreading information. The use of digital identity for democratic procedures is becoming a reality and public services are shifting towards using digital tools to implement simplified procedures. At the same time, our houses are becoming more intelligent, our cities smarter, and the use of the Internet of Things is increasing exponentially. Businesses worldwide have benefitted from implementing information technologies' tools, and industry 4.0 increasingly relies on cloud services and the internet. Likewise, the e-commerce and platforms economy has developed in a way that was unthinkable only 30 years ago.

All this has contributed to creating a new and broader concept of 'cyberspace', where the notion of security is increasingly relevant. Thus, the very pervasiveness of digitalisation has made cybersecurity no longer only a matter of concern for computer scientists but a central transversal factor in securitising our future digital society.

Recently, both the Covid-19-related rise in the use of digital tools and the conflict in Ukraine, followed by an escalation in the use of weaponised cyberattacks, have raised questions about the security of cyberspace and how the EU should deal with this. Although cyber threats have been sharply rising for the past decade, forcing actors in the digital domain to keep up with new attack and defence techniques and technologies, the future that we Europeans want is ever more digital and so we can no longer afford not to talk about (cyber)security. With the potential of Artificial Intelligence and advanced Quantum Computing, the extensive use of cloud services, the new generations of networks and the use of space for communication, the ubiquity in the use of information technologies at every level of our societies is unavoidable. To clarify how to better regulate the future, it is necessary to assess what policymakers can do to foster a constructive approach between the Member States so that they can keep up with the challenges of cyberspace.

This study, edited by Professor Luigi Martino and Nada Gamal, approaches the topic from a multidisciplinary point of view, considering critical infrastructures, skills, strategic autonomy, AI, cybercrime, privacy, and the use of space. Starting from an EU perspective, the authors examine the regulatory achievements in this field and consider best practice for the implementation of rules and standards. Based on a holistic approach, the explanations and policy recommendations in the various chapters aim to define the role of the European Union in this dynamic and constantly changing world of cyberspace.

Editorial: European Cybersecurity in Context

Luigi Martino, University of Bologna and Director of the Center for Cyber Security and International Relations Studies, University of Florence

Nada Gamal, Center for Cyber Security and International Relations Studies, University of Florence

The almost total reliance of modern societies on information and communication technologies (ICTs) has made cybersecurity a top priority in EU agenda-setting and policy-making processes. Empirical data suggests that anarchy is likely to prevail in cyberspace, despite several international normative and regulatory attempts to govern the responsible use of this muddled domain. Indeed, the implementation of an effective governance system based on non-binding norms is apparently considered an optimistic mirage. This pessimistic evaluation is triggered and exacerbated by the intrinsic features that characterise cyberspace: as explained by the National Military Strategy for Cyberspace Operations in 2006, the cyber domain has core attributes belonging to the acronym VUCA (Vulnerability, Uncertainty, Complexity, Ambiguity). These attributes enable the increasing divergence between states' declarations in support of cyber norms and their real (or realistic) misconduct of large-scale cyber operations against their adversaries, for military, economic, and political purposes, which are deemed legitimate by the various sources. The result is a complex interplay between 'personalised' and vague regulations and the safeguarding of states' national interests.

There is an extensive literature that covers the pro and cons of the cyber domain, ranging from technical definitions and socio-political peculiarities to ongoing progress in integrating the virtual and physical dimensions. However, recent political and military events (i.e., the Russia–Ukrainian conflict, USA–China confrontation, etc.) have stressed: a) the strategic importance of the cyber domain in the international political power dynamics of the twenty-first century, b) the growing intersection between cybersecurity and space security for national security and international stability and peace, c) the growing importance of private actors in guaranteeing both digital transformation and national security (i.e., Internet Service Providers, Over The Top, technology leading companies, SpaceX), d) the new powers acquired by non-state actors to influence conventional forms of conflict thanks to the unconventional means granted to them by the digital revolution.

With this distressing reality in mind, the major concern is that, due to the above-mentioned peculiarities of cyberspace, it is not possible to implement binding cyber rules or norms to deter the offensive use of cyber capabilities. According to a cost-benefit analysis (conducted in line with a construct of the realist theory of International Relations), an aggressor has more incentive to deviate from than to observe existing international norms of responsible state behaviour in cyberspace because no targeted retaliation is internationally declared if red lines are crossed. This creates a vicious cycle with serious political, social, and economic repercussions.

This scenario highlights the need for adequate normative and policy tools and an appropriate regulatory framework to avoid and prevent the malicious use of the cyber tools. In this sense, Joseph Nye, in an article published by *Foreign Affairs*, was correct to point out: 'violations, if not addressed, can weaken norms, but they do not render them irrelevant (...) history shows that societies take time to learn to how respond to major disruptive technological changes and to put in place rules that make the world safer from new dangers'.[1] He reminds

1. https://www.belfercenter.org/publication/end-cyber-anarchy.

us that the United States, after dropping nuclear bombs on Japan, took almost two decades to agree the Limited Test Ban Treaty and the Nuclear Non-proliferation Treaty. However, if we agree with Nye's approach, we should also ask ourselves whether, in order to reach an agreement on a Cyber Non-proliferation Treaty, we have to await the dropping of cyber bombs somewhere in the world or take preventive action to avoid the potential occurrence of disruptive events.

It is against this backdrop that this book explores the following research questions:

1. What has been achieved so far at EU level in the field of cybersecurity?

The first part of each chapter begins with a presentation of the state of the art of the chapter's main topic.

2. What are the major political and practical difficulties in both the designing and implementation process of rules and standards?

The second part of each chapter proceeds with an analysis, based on empirical evidence and literature review, of the major challenges and shortfalls of the current European Cyber Security Framework.

3. What can be done to cope with the apparent lack of binding obligations and rules?

In the final sections of their chapters, the authors propose a range of ad hoc policy recommendations and insights that may be useful to meet the gaps highlighted in the chapter.

Before presenting the content of the book, we would like to emphasise that editing a book entirely dedicated to the study of the dynamics of the EU in the context of cybersecurity is not a simple exercise. This is because the EU and cybersecurity are concepts that in themselves seem to be in total dichotomy. Cynics might say that cybersecurity cannot be investigated in a logical and scientific way, due to its inherent technical nature. A second possible criticism is that cybersecurity, being an integral part of national security, cannot be addressed through the study of a supranational actor such as the European Union, which has limited sovereignty.

The arguments presented here succeed in overcoming these two criticisms and in achieving two major objectives. First, they contributes to bridging existing knowledge gaps on these topics, highlighting how cybersecurity is a multidisciplinary subject per se. Second, they attempt to advance international best practice in such a way that it can be transposed in the European context in order to enhance policy-making in the field of cybersecurity. The book gathers contributions from distinguished first-hand experts who, despite their variegated fields of study, share a common research objective: to outline the role of the EU with respect to the dynamics of cyberspace. The outcome is an all-encompassing analytical framework that ranges from technical, political, and legal review to policy recommendations with respect to the research aim.

OVERVIEW OF THE STUDY

The book is structured in eleven chapters as follows:

Pablo A. Mazurier, Independent analyst
Cybersecurity Landscape: Technological Perspectives and Certification Framework, Products, and Services

Francesca Spidalieri, World Bank consultant
Meeting the Growing Demand for Cybersecurity Skills and Talent in Europe

Bushra Al Blooshi, Dubai Electronic Security Center, and Angelika Eksteen, AIDirections
Cyber Governance in the EU

Lior Tabansky, Tel Aviv University
Europe's Digital Discontent

Martina Castiglioni, Cyber 4.0, and Alessandro Lazari, F24 AG
The Normative Landscape in Security and Resilience: The Future of Critical Infrastructures and Essential Services in the EU

Marco Lisi, Independent consultant
The Security of Space Systems: A European Perspective

Arthur de Liedekerke, Rasmussen Global, and Maarten Toelen, Strategy consultant
The Unchecked Proliferation of Offensive Cyber Capabilities (OCC): A Dangerous New Reality?

Marco Ciappelli and Sean Martin, @ITSPmagazine
Cybersecurity in the Age of Artificial Intelligence: Secured by Design or We Are Too Late

Pierluigi Paganini, Cybhorus
Cybercrime-as-a-Service: EU Perspectives

Vagelis Papakonstantinou, Vrije Universiteit Brussel
The Need to Introduce a New Individual Right to Cybersecurity

Arturo Di Corinto, Sapienza University of Rome
The Manipulation of Perceptions: Why Fake News and Disinformation Are a Cybersecurity Issue

Pablo Mazurier's chapter focuses on the EU cybersecurity certification schemes framework and the multi-stakeholderism working programme. The main objective of his detailed analysis is to point out the background tensions between various groups of interests that shape the evolution of these dynamics. An understanding of these tensions, according to Mazurier, is 'crucial not only to better shape efficient, resilient, and recognised certification processes but also to highlight further struggles, vulnerabilities, risks, and paths to cooperation'. The study concludes by proposing several implementation measures for enhancing and reinforcing the framework, increasing the political autonomy and global prestige of the European Union.

Francesca Spidalieri addresses the cyber skill-shortage issue that is affecting public and private entities at international level. Spidalieri believes that there is no single panacea to attract more people to this growing field. However, in order to avoid this vicious circle, the priority should be to understand the weakness that have created this situation starting from the 'under-prioritising/under-funding cybersecurity research and development (R&D), education, and training and focusing solely on technical expertise'. Francesca describes European initiatives to cope with this issue, then moves on to offer examples of international best practice that inform her policy recommendations.

Bushra Al Blooshi and Angelika Eksteen stress the relevance of cyber governance as an 'increasingly important topic, which needs to be addressed mainly on the political, rather than technical level'. The analysis explores the levels of cyber governance in individual EU Member States in order to give perspective to the European approach. After introducing the state of the art of the European cyber governance framework and highlighting the main shortfalls, they advance an array of policy recommendations for the EU based on their Dubai case study.

Lior Tabansky conducts a critical analysis by questioning the ability of the EU to innovate its way into a leadership position in the technological race. Tabansky's analysis is based on a realistic approach and his final thesis is that sovereignty means real political power in the digital domain because 'the political structure prevents the EU from attempting moon shots. The longer the EU avoids acknowledging its structural impediments to innovation, the greater China and the United States' advantage over Europe will grow.

Martina Castiglioni and Alessandro Lazari cover the strategic role of critical infrastructures in the cybersecurity field. Their research question is pragmatic: are the EU's critical infrastructures safe and secure? Their response provides an analysis of the EU security agenda's milestones and upcoming initiatives for the long term and explores the EU's policies and regulations regarding critical infrastructures. Finally, using empirical evidence and case studies, they advance their policy recommendations.

Marco Lisi brings on board an extremely interesting and hot topic: the strategic relevance of the space sector in view of the apparent growth of convergence between defence and space. In Lisi's words: 'The war in Ukraine has provided ample evidence that security concerns and provisions need to be extended to all space assets, and of how strategically important it is for Europe to be autonomous in terms of technologies and access to space. The commonly shared perception is that space risks becoming the battleground of a future war, if it has not already become one.' Lisi investigates space technologies' vital role in maintaining information that is safe and secure in terms of confidentiality, availability, integrity, continuity, and quality of service. Focusing on the European perspective, he introduces the main EU space policies, initiatives and actors and concludes with insightful recommendations for enhancing the European position as a leading actor in the space sector.

Arthur de Liedekerke and Maarten Toelen deal with the usage and proliferation of cyber weapons, with a critical and thought-provoking approach. Using the Pegasus case study, the authors explain the evident accountability gap in the development of cyber intrusion tools, stating that 'the Pegasus saga is a damning and evident indictment of the international community's inability to effectively regulate the proliferation of offensive cyber capabilities'. However, they point out how 'it is by no means a standalone incident' given that 'the current laissez-faire regulatory approach to offensive cyber capabilities proliferation has left a dangerous grey zone from which unscrupulous actors are only too keen to benefit'.

Marco Ciappelli and Sean Martin approach the AI Act of the European Union from an ethical perspective, claiming that 'ethics and security are two sides of the same AI coin. One cannot exist without the other. In between the promises and the risks of artificial intelligence innovation lies a sea of uncertainty'. In analysing the EU's AI Act, they conducted

several interviews with leading experts in the field at technical, legal, and policy levels in order to advance some practical recommendations. They believe that 'European measures and regulations are not sufficient to cope with this increasingly sophisticated technology due to a lack of detailed guidance for effective methods to handle malicious or accidental cyber activities and guard against the potential impact that compromised AI can have on society'.

Pierluigi Paganini's chapter focuses on cyber crime and how it impacts on safety and security in the EU in economic, political, social and institutional terms. Paganini contends that 'the European authorities are aware of the risks and damage associated with cybercriminal operations and are defining a common strategy to curb illegal activities online'. Yet there is clear evidence of the impact of the ongoing conflict between Russia and Ukraine on the operations of cybercriminal gangs on a global scale. The chapter then addresses what the EU is doing to cope with cybercrime and to what extent the adopted measures can be viewed as effective are issues, and concludes with a set of policy recommendations.

Vagelis Papakonstantinou covers the role of individuals in the framework of policies and regulations issued by the EU. He stresses the lack of individuals' involvement in areas in which they are directly affected, stating that 'individuals ought not to be treated as passive recipients of cybersecurity, dependent on the goodwill and effectiveness of third parties. On the contrary, they need to be provided with the legal tools to protect themselves in the digital environment.' In an innovative proposal he arguing that the introduction by the EU of a new right to cybersecurity will enable individuals to protect their digital selves, while legally requiring third parties to respect their rights.

In the last chapter, Arturo Di Corinto addresses the increasingly worrying topic of disinformation. Starting from the recognition that disinformation has become a cyber problem, the author attempts to describe the issue of online information that is affected by 'information manipulation campaigns that make widespread use of fake news to sew doubt and discontent in the population'. These campaigns use the most pervasive tools, such as 'social networks, social environments engineered to encourage people's engagement and the polarisation of opinions so that they remain on the platforms as long as possible, increasing their value for advertisers'. The chapter's conclusion is as simple as it is dramatic: 'the more time you spend online, the more likely you are to be exposed to commercial information and products and the more you are a target of disinformation and manipulation campaign'.

As clearly emerges in the pages of this book, cyberspace is inherently transnational and transversal; any study must therefore take into consideration that in this domain 'one approach does not fit at all'. The main recommendation that EU policymakers should consider from the outcomes of this book are the following:

1. The EU must acknowledge that it is impossible (and dangerous) to replicate solutions that were valid for old phenomena to govern the new dynamics of cyberspace. The rules of the game have changed and the European policy agenda must be realistic, designing a strategy capable of pursuing the EU's vital interests. The EU's ultimate target should be lessening the intensity and frequency of cyber attacks, while working on increasing its cyber resilience and defence system. However, the first urgent point to work on is to set European red lines and credible responses should aggressors infringe those lines.
2. EU strategy needs to boost its multilateral and international component based on diplomacy, new forms of deterrence, and strategic partnerships with states that share the same values and rule-based system approach. Only through robust international alliances and strong transatlantic collaboration will it be possible to impose pragmatic and material costs on misconducts.
3. The EU is acknowledged as a potential 'civilised power', It should therefore work on enhancing and implementing further capacity-building projects in developing countries instead of being trapped in the vicious circle of 'hyper normativisation'.[2]

Although the digital era has kicked off *mutual permanent vulnerabilities*, where no actor is free of danger, the main role of EU policymakers is to adopt a real risk assessment approach. The most effective stance, following Niccolò Machiavelli's recommendations in *The Prince*, is to manage risks not by means of 'luck' but by 'virtue', given that risks and threats are like a raging river that sometimes rises and floods the plain, wreaking destruction in its wake. There's no way you can stop the river acting in this way; but we can try to prevent such actions in the future by building banks and dikes, so that when the water rises the next time it can be contained in a single channel and the rush of the river in flood is not so uncontrolled and destructive.

2. https://dergipark.org.tr/tr/download/article-file/1310

Cybersecurity Landscape: Technological Perspectives and Certification Framework, Products, and Services

Pablo A. Mazurier

https://doi.org/10.53121/ELFTPS3 • ISSN (print) 2791-3880 • ISSN (online) 2791-3899

ABSTRACT

This chapter focuses on the innovative EU cybersecurity certification schemes framework, a voluntary multistakeholder working programme under gradual implementation, highlighting the challenges it faces and providing suggestions. Such an analysis is necessary to better understand the background tensions between different groups of interests, which is crucial not only to better shape efficient, resilient, and recognised certification processes but also to identify further struggles, vulnerabilities, risks, and paths to cooperation. The chapter concludes by proposing several measures to be implemented in the political agenda in order to enhance and reinforce the framework, increasing the European' Union's political autonomy and global prestige.

ABOUT THE AUTHOR

Pablo Andrés Mazurier is an Italian-Argentine analyst specialising in global security, the digital world, and future studies. He holds a Law Degree, an MA in International Studies (University of Trento, Italy) and a PhD in Politics and Human Rights (Sant'Anna School of Advanced Studies, Italy). Formerly a researcher at King's College London, he is currently a member of the research team at the Center for Cyber Security and International Relations Studies, University of Florence.

INTRODUCTION

This chapter analyses the innovative EU *cybersecurity certification schemes framework* (CSF), a voluntary, multistakeholder working programme under gradual implementation, highlights the challenges it faces, and offers suggestions. This set of instruments will certainly become crucial for the success of the overall European effort to reshape Europe's internal digital landscape, making it more secure, resilient, and autonomous. It also reaffirms the role of the European Union as a key global player in the digital future.

The chapter comprises four sections. The first gives an introductory explanation of the need to implement the CSF on information and communications technology (ICT) products, services, and processes. The second section focuses on the interactions among the three main types of stakeholders currently serving as models for the whole process of creating the CSF. This multistakeholder analysis helps to better understand the background tensions between different interests, which is crucial not only to better shape efficient, resilient, and recognised certification processes, but also to highlight further struggles, vulnerabilities, risks, and paths to cooperation.

After analysing the benefits of the certification schemes for each type of stakeholder, the third section is dedicated to highlighting the current challenges faced by the new CSF. The study concludes by proposing several measures to be implemented in the political agenda in order to enhance and reinforce the framework.

THE EUROPEAN CERTIFICATION OF ICT PRODUCTS, SERVICES, AND PROCESSES

The more digital a society becomes, the greater its exposure to malicious cyber threats and other forms of disruption. This constant risk erodes public trust in digital devices, while making the digital transformation and enrichment of people's lives stressful and problematic. This is the main reason why the European Union is adopting a whole branch of communitarian regulations to make the common digital market more cybersecure, resilient, predictable, and strategically autonomous. One of the key measures implemented to achieve these goals is the cybersecurity certification of ICT products, services, and processes, created by the EU Cyber Security Act in 2019. This working programme, still being rolled out is being implemented through a schemes framework (ENISA, 2022),[1] which currently includes three schemes: the EU Common Criteria (EUCC), the EU Cloud Services (EUCS), and the EU Mobile Networks (EU5G) schemes. Other key innovative areas and strategic priorities are expected to be identified and regulated in the future.

Under the strategic guidance of the Commission and the technical control of the European Union Agency for Cybersecurity (ENISA), the CSF is still voluntary, with the expectation of becoming a mandatory regulation after a four-year probation period, ending on 31 December 2023, and a positive assessment of the Commission.

Cybersecurity assessment through certification also implies an enhancement from the organisational and socio-cultural point of view, due to the fact that nowadays cybersecurity is no longer considered just an appendix sector of economic processes, but is becoming a new way of thinking and designing inherently cybersecure ICT products, services, and industrial processes.

Notwithstanding the multiple challenges the CSF presents, its adoption will surely represent a crucial step towards a more strategically autonomous Europe, which will be able to not only better control and enhance the quality and uniformity of its common digital market, but also reinforce its influence on foreign industries, states, and regions. Thanks to instruments such as the CSF, the EU will still be considered a key actor in a global geopolitical scenario mostly dominated by the technological race between the United States and China.

ANALYSING THE CSF FUNCTIONAL NETWORK FROM A MULTISTAKEHOLDER PERSPECTIVE

As already stressed, the future of human societies is inherently linked to an adequate development of the digital world. Therefore, the EU is currently taking bold steps towards the regulation of digital markets, with the objective of not only providing citizens and businesses with a trustful, human-centric, secure, and sustainable transition to a fully integrated digital society (European Commission, 2021), but also maintaining and increasing its strategic autonomy with respect to both private and public technological giants, in an extremely complex, highly dynamic, and innovative digital global scenario.

The institutional network created to manage the CSF is led at the communitarian level by the Commission, the Member States, and ENISA, with the help of ad hoc working groups, academic experts, and other relevant stakeholders, in order to develop draft certification schemes (ENISA, 2022). Two other EU institutions have a gravitational role in enhancing technological sovereignty through joint investment in strategic cybersecurity projects: the European Cybersecurity Competence Centre and the Network of National Coordination Centres.[2] They both coordinate the European framework to support innovation and industrial policy in cybersecurity, thanks to their decisions on strategic investments and pooled resources.

At the national level, Conformity Assessment Bodies (CABs) audit, test, and/or certify ICT products, services, and processes. CABs are supervised by National Cybersecurity Certification Authorities (NCCAs) which monitor compliance with the certificates issued by the CABs in their Member States.

Each scheme distinguishes three different cybersecurity assurance levels, as shown in Table 1.[3]

TABLE 1: **Cybersecurity assurance levels**

Basic Level	Substantial Level	High Level
The aim is to minimise known basic risks of incidents and cyberattacks. It mostly requires a self-assessment to demonstrate the absence of publicly known vulnerabilities. Most of the ICT products and services in circulation within the common market are in this category.	To minimise known cybersecurity risks and the risk of incidents and cyberattacks carried out by actors with limited skills and resources.	Focused on reducing the risk of state-of-the-art cyberattacks carried out by actors with significant skills and resources. In this case, providers must demonstrate state-of-the art-techniques to implement the necessary security functionalities, and also should be able to prove resilience against skilled attackers by using penetration testing.

Depending on each of these levels of assurance, CABs must apply different approaches to effectively monitor compliance with the requirements in order to proceed with evaluation and certification in accordance with EU schemes and NCCA regulations. In September 2021, ENISA published a guide (ENISA, 2021a) on the methodology for sectoral cybersecurity assessments applicable in the context of ICT Security for sectoral multistakeholder systems and CSF. This innovative methodological approach integrates sectoral, product, process, and potentially also Information security Management System-based CSFs, representing an enhancement of the typical risk assessment procedure, by adding cyber threat intelligence and taking a deep dive to gain detailed information about the intended use of relevant subsystems, products, and services.

Without any doubt, all three current schemes provide a more organised and secure assessment for the European digital market of products and services, creating more opportunities for all actors and increasing the level of cybersecurity of society as a whole, expanding European influence as a global normative power (Manners, 2002).[4] As cybersecurity dimension is transversal, inherently related to all digital products, services, and processes, European certification will be a key instrument for maintaining strategic autonomy, as it would provide cyber stability and public trust while influencing foreign providers and other states to comply with the schemes in order to access to the EU common market.

The CSF is shaped by two types of global political dynamics. On the one hand, an internal dynamic conceives certification schemes as a key tool for increasing internal unity among Member States, harmonising their national regulations and engaging all key national and international actors on respecting and promoting a common set of rules, standards, procedures, recognition, and values. And as a consequence, on the other hand, a global dynamic is enabled, expanding the recognition and applicability of these schemes to external actors and regions, not only in operational terms but also as a geopolitical recognition of the EU as a relevant actor for the digital future.

Moreover, these two *centripetal* and *centrifugal* dynamics interact, allowing the EU to keep on producing more regulations on new areas with the experience and prestige gained in normative processes. For instance, the global success of the GDPR regulation in recent years was crucial for the EU to focus more of its resources on the transition to a digital society, creating a whole universe of programmes and regulations: Europe's Digital Decade (European Commission, 2021), the project for a Cyber Resilience Act (2022), the Digital Markets Act and the Digital Services Act (2022), the Commission's 'White Paper on Artificial Intelligence' (2021), the Parliament's Report on Artificial Intelligence in a Digital Age (AIDA) (2021), and the Digital Education Action Plans (2018 and 2020), among others.

> In terms of foreign policy, the big question relies on how to align EU cybersecurity certification schemes with other certification schemes in other parts of the world

From a multistakeholder and multidisciplinary perspective, the CSF process implies a complex network of interactions among three main groups of interests (GoI) (see Table 2).

As a result of this multistakeholder model, the EU certification schemes are produced through continuous, *multi-level* interaction among these three groups,[5] taking into consideration every stakeholder's needs, capabilities, and specific circumstances in order to engage all or at least most of them and generate a common consensus, acceptance, and recognition of the regulation. The more these stakeholders interact, creating what is called an *epistemic community*, the more they will create a common vision on how to behave in order to better strengthen the European cybersecurity environment as a whole. The outcome of this multistakeholder model of the regulation process conceived for the certification schemes offers many benefits, depending on each stakeholder's viewpoint, as shown in Table 3.

TABLE 2: **CSF process interactions among GoI**

Political and Regulatory GoI	Business GoI	Technical GoI
It implies values, public interests, and social dynamics in action through political and/or regulatory processes.	It analyses certification in terms of trading costs and benefits, risks and opportunities, and sanctions and rewards, in order to decide whether to comply with regulations. It also includes other factors: funding, time and energy invested in the certification processes, how other competitors or markets behave, the quality of services and products, the existence of asymmetries, liabilities, the possibility and capacity to access new markets, business scalability and specialisation, skills required, and other indirect costs such as insurance, bureaucracy, corporate image, reputation, managerial adaptation and engagement.	It is focused on standards, levels of cybersecurity, risk assessments, horizontal and vertical assessment processes, specific types of products and services, supply chains, and industries.
From a political perspective, certification represents a tool to increase trust, transparency, political unity, harmonisation, and proactive global influence, as well as to avoid fragmentation and other organisational and social gaps and distortions.	From a business viewpoint, the whole EU certification process reinforces the internal market in terms of cybersecurity while creating a brand new market for cybersecurity service providers in education, certification, and monitoring.	In technical terms, certification represents the most rigorous tool available to efficiently increase cybersecurity through risk-based control and management of products, services, and processes.

TABLE 3: **Benefits of the CSF process according to different stakeholders**

From a *political perspective*	Certification avoids fragmentation, fostering a stronger union of the Member States into a single, harmonious, and powerful bloc, to better protect their interests in the new digital world.
From a *geopolitical perspective*	A broad acceptance of the certification schemes from key global actors confirms the increasing EU role as a normative power and the efficacy of its multistakeholder democratic and inclusive model of negotiation and engagement.
From the *final users' perspective*	The certification schemes generate three main kinds of benefits. The crucial factor is that standardisation and certification increase public trust in the whole system. Trust is essential for the creation of the sustainable, human-centred digital society that the EU envisions. Secondly, certification schemes lower the risks of deficiencies and asymmetric information, providing adequate protection to all social sectors and ensuring a common, cybersecure level of quality of services and products. Thirdly, thanks to this communitarian initiative, citizens will have also more options to choose better and more adequate products and services in the market to satisfy their specific needs.
From a *legal perspective*	Certification fosters legal certainty and predictability, and also makes risk assessment and compliance easier and more affordable. Moreover, the higher the level of cybersecurity, the lesser opportunities for cybercrime, which represents another key factor in enhancing public trust in the digital world.
From the *service providers' perspective*	Certification represents an opportunity to secure access to a huge market, comprising 27 different national markets. The benefits do not limit themselves to efficiency, operational resilience, and economic benefits, but also expand to fulfil other key managerial aims: a more solid corporate image, business continuity, operational resilience, and global reputation. Certification also allows companies to reduce incidents involving third-party products and services, increasing their specific skills, mitigating risks, and reducing costs.
From the perspective of the *Member sSates*	Certification represents a unique opportunity to upgrade their national cyber skills and to reduce the gap among Member States in terms of cybersecurity skills and digital market products, services, and processes. European funds will be allocated to solving these problems to create a common, equally fair, and skilled digital market.

FURTHER CHALLENGES FOR THE EU CERTIFICATION PROCESS

Looking at a medium-term scenario, the CSF will be a mandatory regulation, with at least the three schemes (EUCC, EU5G and EUCS) already implemented. Other schemes could also be considered for acceptance and implementation (i.e., artificial intelligence, robotics, nanotechnology, big data, cryptocurrencies) and the whole procedural institutional mechanism of multistakeholder consultation, legislation, and implementation should already be performing efficiently and smoothly.

One of the most critical variables to take into consideration with regard to a scenario three–five years in the future is the adoption and compliance of the whole certification framework by the Member States' national systems. It is desirable that the whole national network of CABs and their national agencies would be fully operative, guaranteeing a high level of control over the evaluation/certification processes, while exercising competent oversight over the already certified ICT products, services, and processes. But the whole system must be aware of local attempts to abuse the opportunity that the new certification providers market creates, by lowering the levels of control on the certification processes in order to attract businesses with easy practices of certification. Unfair competition and single-market distortions should be prevented and dismantled.

In terms of global acceptance, CSF should follow the same path taken from the successful implementation and influence generated by the GDPR rules worldwide. A coordinated, strong, and consistent implementation, promotion, and defence of these certification processes will be crucial to providing the EU with limited but essential room for autonomy in the global digital scenario.

After analysing the whole situation, many challenges can be highlighted.

From an EU perspective, the most crucial political struggle is to make the national implementation of the certification framework efficient, avoiding fragmentation and market distortions. These processes require a strong multi-level political consensus and a strict top-down control on implementation with an inclusive bottom-up engagement to meet the levels of cybersecurity required to achieve certification.

Member States need to understand that efficient local implementation of the certification framework is crucial to reinforcing the whole digital transformation process that the EU authorities have promoted in recent years. It thus represents an exceptional opportunity to achieve a position of collective global leadership in the market of the future. Notwithstanding this, it could also lead to greedy calculus based on national interests, depending on how advanced and organised each national system is. Larger and more advanced countries have to understand this circumstance and help the rest of the Union in order to avoid a multi-speed Europe in terms of cybersecurity.

Another challenging task is organisational, regarding how to help national bodies organise and provide high-level skills to their own local CABs for accreditation. In particular, there are two key issues for national accreditation bodies: 1) the recruiting and/or training of competent technical personnel and experts involved in the certification bodies, and 2) the cooperation between the national accreditation bodies and the NCCAs.

In terms of internal cooperation, the challenge is focused on maintaining coherence and consistency among the different EU certification schemes currently in force, avoiding overlap and fragmentation, particularly in specific industrial supply chains with a complex number of products, services, processes, and levels of security to meet.

International commerce needs more harmonisation and alignment between different standardisation and certification schemes around the world, particularly those regulating the big tech markets and innovation.

From a business perspective, there will always be the challenge of balancing costs and benefits, risks and securities. The certification framework certainly represents a unique opportunity for a new, very lucrative market for experts in cybersecurity to flourish. Many other actors might also be interested in participating, but not have the required skills, expertise, or motivation. The European authorities will have to put their best effort to keep this market attractive yet exclusive.

Last but not least, the EU must engage all actors proactively in order to encourage them to do their best to meet the set requirements in terms of cybersecurity vision, skills, investments, cooperation, transparency, and public education.

POLICY RECOMMENDATIONS FOR DIFFERENT STAKEHOLDERS

Several political measures have been suggested to enhance and reinforce the CSF, which would increase the political autonomy and global prestige of the European Union. They can be categorised into three

TABLE 4: **Policy measures to strengthen the CSF implementation**

Capacity-building measures	Community-building measures	Awareness-raising measures
Technical workshops for internal industries, providers, and governmental agencies.	Fostering the engagement of all stakeholders, by building circles of trusted partners.	Forming a committee of experts on ethical issues.
Enhancing national bodies' skills to efficiently audit and oversee local certification schemes.	Promoting international cooperation and compliance on cybersecurity certification.	Increasing public education on cybersecurity and the benefits of using certified products and services.
Forming a committee of experts on networking efficiency and communitarian engagement.		
Forming a committee of experts on geo-strategic issues to increase EU political autonomy and global normative power.		

main areas: capacity-building, community-building, and awareness-raising measures (Table 4).

1. **Enhance cybersecurity expertise on operational cybersecurity issues:** The first proposal is to organise regular technical workshops in order to: obtain cutting-edge information and expertise on innovative technologies and industries, increasing the resilience of the whole epistemic community in the current cybersecurity landscape. There is an important gap among the Member States in terms of organisation and promotion of cyber camps, contests, and teams of ethical hackers. ENISA should better research it to offer a clear map of any national resource available and the capacity they need in order to offer adequate cybersecurity on the three levels of risk designated by the CSF.

2. **Increase capacity-building measures to enhance national bodies' skills to conduct fair and efficient audits and oversight:** It is critical to ensure excellent implementation of the certifications, which should not be seen as a box-ticking procedure, but as specific, continuous, sustainable, tailored-made control and monitoring of a precise standard of cybersecurity required of any product, service, or process circulating in the common market. Compliance expertise, long-term vision and technical excellence are skills every auditor and CAB must master.

3. **Continue fostering engagement from all stakeholders:** This would actively contribute to: 1) the identification and rating of cybersecurity risks; 2) the identification and development of the best procedures, tools, and networks to mitigate cybersecurity risks and to attribute and react to high-risk cyberattacks; 3) the enhancement of collective trust and resilience through transparent and regular communication and cooperation between public authorities, the private sector, and technical experts.

4. **Promote international cooperation on EU cybersecurity standardisation and certification frameworks and the promotion of its virtues:** International recognition of and adaptation to the European certification schemes shall be promoted by both the EU as a whole and individual Member States thanks to constant engagement and agreement with other states, regions, international organisations, and specialised bodies. A good example is the Joint Statement signed with Singapore (European Commission, 2022) to accelerate steps towards a comprehensive and forward-looking digital partnership, to cooperate on the full spectrum of digital issues, including digital economy and trade, a secure and sustainable digital infrastructure, more resilient supply chains, digital regulations, the development of digital skills for workers, and the digital transformation of businesses. This innovative process of international cooperation, starting with bilateral technical workshops followed by a political agreement in 2022, also includes new and emerging areas with transformative economic and social potential, such as 5G/6G, artificial intelligence, and digital identities.

5. **Create three permanent groups of experts to monitor the implementation and development of the certification schemes:** It would also be crucial to create three groups of experts designated by the EU authorities, the Member States, and civil society, in order to analyse and offer solutions not only on the development and implementation of the certification schemes but also the whole process of communitarian regulation of digital markets in the following areas:

A. **An expert committee on ethical issues:** This group would debate on and produce specific guidelines, with limitations and interpretations on the content of the areas regulated by the standards and certification schemes framework, in order to better protect human rights, ethical

principles, and European values. Innovative areas such as artificial intelligence, cloud services, robotics, drones, and 5G/6G implementation have a clear and sometimes disruptive impact on human rights and they represent huge ethical challenges that need to be understood, studied, and regulated. Many EU Member States have already created such boards to better deal with the impact of digital transition on different aspects of social life (Bundesministerium für Digitales und Verkehr, 2021).[6]

B. **An expert committee on networking efficiency and communitarian engagement:** This committee would assess operational efficiency, interaction among public and private actors, the process of institutionalisation, public policies of communication, and protection of the whole network dedicated to the implementation of the certification schemes, including all stakeholders: the communitarian institutions, national governmental agencies, national bodies of implementation of the regulation, the business and industrial sectors, the expert community, and civil society. Topics such as overlap or fragmentation of the single framework can be subjects of analysis by this committee.

C. **An experts committee on geo-strategic issues:** This team would be dedicated to exploring the external impact of the European regulation on foreign digital markets; the reaction of foreign corporations and agencies dealing with EU certification processes; the analysis and evaluation of alternative frameworks of standardisation and certification worldwide and how to deal with them in terms of adaptation, cohesion, or cooperation; the assessment on how to better match EU interests with international and global trends on digital topics; and providing strategic counselling and anticipatory advice to protect and promote the EU's autonomy and global reputation.

6. **To increase public education on cybersecurity and the benefits of consuming certified products and services:** The success of the implementation of the certification schemes relies also on public acceptance and demand for certified products and services. In order to achieve an adequate level of public concern, targeted advertising campaigns should be undertaken to explain, in simple, engaging, and transparent ways, the benefits in terms of cybersecurity and trust of consuming only certified products and services (ENISA, 2021b).[7]

NOTES

1. A scheme is defined as a 'comprehensive set of rules, technical cybersecurity requirements, standards and evaluation procedures, defined at the EU level and applying to the certification of specific ICT products, services or processes.'
2. https://cybersecurity-centre.europa.eu/index_en.
3. Art. 52, Cyber Security Act (2019), 'Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013', http://eur-lex.europa.eu/eli/reg/2019/881/oj.
4. The concept of 'Normative Power Europe' was developed by Ian Manners, who stressed how the European Union shapes the international environment, producing changes in global standards and norms, not by using material instruments but through the power of the attractiveness of European standards, values, principles, and procedures.
5. From a multistakeholder perspective, successful regulatory implementation processes need to avoid extreme up-down and bottom-up dynamics, promoting a common ground for collective, skilled, responsible, and equal participation.
6. For instance, the German Ministry of Transport has a Board of Academic Advisors that meets regularly and has a public website showing all their decisions and debates.
7. ENISA has recently launched a video that is a good example of advertising European certification schemes and the importance of CABs' role.

REFERENCES

Bundesministerium für Digitales und Verkehr (2021), 'Gutachten und Stellungnahmen des Wissenschaftlichen Beirats', https://www.bmvi.de/SharedDocs/DE/Artikel/G/wissenschaftlicher-beirat-gutachten.html.

ENISA (European Union Agency for Cybersecurity) (2021a), 'Methodology for Sectoral Cybersecurity Assessments', https://www.enisa.europa.eu/publications/methodology-for-a-sectoral-cybersecurity-assessment/@@download/fullReport.

ENISA (European Union Agency for Cybersecurity) (2021b), 'European Cybersecurity Certification Schemes – What's in for Conformity Assessment Bodies (CABs)?', https://www.youtube.com/watch?v=vabWKHGrjGM.

ENISA (European Union Agency for Cybersecurity) (2022), 'Certification Schemes and CABs - FAQ', https://www.enisa.europa.eu/topics/standards/certification/certification-schemes-and-cabs.

European Commission (2021), 'Europe's Digital Decade', https://digital-strategy.ec.europa.eu/en/policies/europes-digital-decade.

European Commission (2022), 'Joint Statement: EU and Singapore agree to accelerate steps towards a comprehensive Digital Partnership', 14 February, https://ec.europa.eu/commission/presscorner/detail/en/STATEMENT_22_1024.

European Council (2021), 'Regulation (EU) 2021/887 of the European Parliament and of the Council of 20 May 2021 establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres', PE/28/2021/INIT, 20 May, https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1623160399041&uri=CELEX%3A32021R0887.

Manners, I. (2002), 'Normative Power Europe: A Contradiction in Terms?'. *Journal of Common Market Studies*, 40(2), 235–58.

Meeting the Growing Demand for Cybersecurity Skills and Talent in Europe

Francesca Spidalieri

https://doi.org/10.53121/ELFTPS3 • ISSN (print) 2791-3880 • ISSN (online) 2791-3899

ABSTRACT

This chapter addresses the opportunities and challenges of developing a robust European cybersecurity workforce that can protect digital assets and infrastructure from cyber risk, improve cyber resilience, and support the EU's ambition for strategic autonomy. While there is no single panacea to attract more people to this growing field, this chapter provides a comparative analysis of current initiatives and programmes to grow the cybersecurity pipeline and information and communications technology skills across the EU and the United States, and recommends further expanding and harmonising these efforts. It also offers recommendations to reverse the current under-prioritising and under-funding of cybersecurity R&D, education, and training.

ABOUT THE AUTHOR

Francesca Spidalieri is a cybersecurity and strategy consultant for the World Bank, the International Telecommunications Union, the Global Forum for Cyber Expertise, and other private sector organisations. She is also an Adjunct Professor for cybersecurity policy at Salve Regina University, a Senior Fellow for Cyber Leadership at the Pell Center for International Relations and Public Policy, and the Co-Principal Investigator for the Cyber Readiness Index project at the Potomac Institute for Policy Studies. Francesca holds an MA in International Affairs and Security Studies from Tufts University.

INTRODUCTION

Over the past decade, nations around the world have embarked on a digital transformation journey unmatched in human history. Both advanced and developing economies have increasingly embraced information and communications technologies (ICTs) in their networked environments and infrastructures to improve productivity, efficiency, innovation, and modernisation and to advance human and social development. Countries have prioritised digitisation and connectivity as key enablers of sustainable economic growth and social development, including greater participation in the global economy, improved competitiveness, advanced skills development, and as a means to narrow the 'digital divide' between the connected and unconnected (Hathaway & Spidalieri, 2021). This trend has accelerated in response to the COVID-19 pandemic, as countries have switched to hybrid work environments, automated essential services, and – more recently – ramped up investments in digitisation and technological innovation to relaunch their economies and boost the post-pandemic recovery. The EU has invested nearly €2 billion to advance the digital transition and meet the goals of Europe's Digital Programme (EU, 2021). At the same time, it launched several efforts to establish 'strategic autonomy' in the digital sphere, to reclaim its 'digital sovereignty' in data protection, technology innovation, digital policy, digital taxation, etc., and to forge its own path to data management – one distinct from both the US model of private sector dominance and China's state-controlled approach.

Despite the clear benefits of embedding digital technologies into economies and societies, our increased dependence on ICTs and the expansion of e-services, digital systems, and platforms have

also exposed countries and organisations alike to a growing number of known and unknown vulnerabilities. Europe has been contending with a plethora of threats stemming from the misuse of ICTs, including cyber crime (e.g., phishing, identity theft, internet/email fraud, ransomware attacks, cyber extortion, etc.), data exploitation, critical infrastructure failures, disruptions of essential services, increased surveillance, disinformation, influence operations, foreign interference, etc. – and many of these threats have been exacerbated by the COVID-19 crisis. Most recently, Europe has become a theatre for covert cyber operations and cyberattacks in the midst of the Russia-Ukraine conflict, including phishing campaigns, deployment of wiper malware designed to destroy systems, and ongoing distributed denial of service attacks against Ukrainian financial, government, and defence targets (Fendorf & Miller, 2022). To mitigate the cyber-related risks faced in recent years and further assert EU strategic autonomy, European countries and institutions have developed a broad collection of cybersecurity policies, frameworks, and regulations aimed at protecting digital assets and infrastructure and ensuring the availability, integrity, and confidentiality of data and digital services. But while technology solutions and compliance with internationally recognised standards and EU regulations are certainly important to protecting organisations against cyber threats, those measures alone are insufficient. No matter how advanced, efficient, reliable, and interoperable any particular technical/digital solution is, its capabilities are limited if it is not securely developed ('security-by-design'), properly configured, effectively implemented, and regularly updated by skilled workers who follow well-defined processes. In short, *any technology or process for managing cyber risk is only as good as the people who develop, implement, use, and maintain it* (Spidalieri & Kern, 2014). Technology and policy considerations continue to dominate cybersecurity discussions, often overlooking the fundamental human element at their core.

EU countries, like many other technologically advanced and ICT-dependent nations, have yet to adequately invest in the *development of a robust supply of knowledgeable and experienced IT and cybersecurity professionals* to keep pace with the fast rate of digitisation and parallel proliferation of cyber risks – vulnerability and damage increase when the line of defence is not sufficiently robust. The global capacity shortage (from specialists and throughout the broader workforce) can be felt across all sectors, from national governments to Fortune 500 companies, to international organisations, and academia with potentially negative consequences for national security, the global economy, and people's health and safety. In 2021, over 3.5 million cybersecurity jobs were estimated to be vacant worldwide (Morgan, 2022), with about 500,000 unfilled positions in the United States and over 290,000 in the EU (Leitão Marques, 2021). According to a recent BCG global survey, the gap between demand and supply of cybersecurity professionals grew by 13 per cent between 2020 and 2021. The current workforce of 4.4 million workers would need to grow by 80 per cent right now to meet demand (Chan, 2022).

The importance of cybersecurity knowledge, skills, and capacity is now recognised widely, but the need for its widespread application still depends on the availability of talented professionals. Developing a modern workforce fit for the challenges and opportunities of digital transformation is particularly relevant now as the EU implements its €720 billion Recovery and Resilience Facility plan – the largest stimulus package ever financed on the continent – aimed at 'making Europe greener, more digital, and more resilient'. Member States have already allocated more than 26 per cent of the funds made available to their digital transition – this exceeds the agreed target of 20 per cent for digital spending (EU, 2021). Together with the amounts under the EU long-term budget, these funds should help advance objectives such as fostering the European development of the next generation of digital technologies (i.e., supercomputers, quantum computing, blockchain, etc.); developing capacities in strategic digital value chains, especially microprocessors; speeding up the deployment of high capacity and secure network infrastructure, including fibre and 5G; making use of digital technologies to reach the ambitious environmental goals; upgrading digital capacities in education systems; and *enhancing the EU's ability to protect itself against cyber threats*. However, none of these goals – and especially the last one – can be achieved without appropriate investment in the development of *cybersecurity skills and a professional workforce* equipped with the knowledge and capability to protect digital assets and infrastructure from cyber risk, improve cyber resilience, and leverage digital technologies for strategic advantage.

COMPOUNDING CHALLENGES: CYBERSECURITY WORKFORCE AND SKILL SHORTAGE, GENDER BIAS, AND LACK OF MULTI-DISCIPLINARY EXPERTISE

The tech and cybersecurity industries are among the most in-demand, profitable, and critical fields in modern history. They include a broad range of speciality areas and positions that one can pursue without ever leaving the cyber domain – from software development to network engineering, cryptography, information security, consulting, law and compliance, etc. – all tightly glued together by technology. Although cybersecurity professionals are in great demand and can command impressive salaries, the critical shortage of talent has continued to grow worldwide. In particular, women are a significantly underused source of expertise and makeup an astonishingly low number of the current professionals in the field. In 2021, women accounted for about 25 per cent of cybersecurity positions worldwide (Cybersecurity Ventures, 2021), up from 11 per cent in 2017 ((ISC)², 2017) and only 11 per cent in Europe (Women4Cyber, 2021), despite representing almost half of the global workforce. Various reports, studies, and dedicated initiatives have shed light on the long-standing obstacles and persistent challenges women face when entering and pursuing careers in STEM disciplines, including cybersecurity, due to gender-based discrimination, wage gaps, lower earning potential at every level, missed or delayed promotions, and a much harder path to reach the upper echelons of the corporate world – despite often having higher levels of education and certification than men. 'The under-representation and under-utilisation of female talent is both a critical business issue and a hindrance to the development of world-class cybersecurity organisations and resilient companies, as well as the overall safety and protection of our country' (Terwoerds, 2017).

The shortage of women and minorities in this field has been further exacerbated by a lack of objectivity and consistency in competency models and measurements to ensure men and women are entering and moving up in the industry equally, and by unconscious and conscious biases present all the way through the recruiting and hiring performance evaluations. These endemic aspects are compounded by a lack of clear career paths, job descriptions, certification schemes, and multiple different training and education standards, which in turn make it harder for organisations to properly identify, recruit, place, and retain the cybersecurity workforce they need. Cybersecurity-focused research, education and training programmes have also generally been *under-prioritised* and *underfunded* – especially when compared to other areas of education, training, and R&D, like next-generation pharmaceuticals, life sciences, biomedical engineering, ICT services, electronic products, and automotive products, which are all increasingly dependent on digital systems and, therefore, vulnerable to cyber risks.

> Member States have already allocated more than 26 per cent of the funds made available to their digital transition

The need for cybersecurity capabilities and talent is not limited to technical areas. But many of the existing cybersecurity-related courses and certification programmes were created for the traditional fields of computer science, software engineering, or information assurance, and do not fulfil the need for an inter/multi-disciplinary cybersecurity workforce capable of translating very technical concepts and complex cybersecurity issues into policy, legal, business and governance terms, and incorporating cybersecurity and digital resilience across an entire organisation. Developing effective cybersecurity strategies, policies, and processes requires not only technical expertise but also the ability to synthesise organisation-wide prevention, awareness and mitigation measures, managerial action, and senior-level oversight (rather than just relying on IT professionals or a chief information security officer's team working in a vacuum to 'harden' systems, 'patch' vulnerabilities, or 'fix' a breach after the fact). Addressing these challenges, therefore, calls for a *new generation of cyber-strategic leaders and cyber-policy experts* prepared to tackle the complexities of cyberspace. These individuals do not necessarily need to be trained in engineering or programming, but they must have a deep understanding of the digital environment in which they operate and the most pressing cyber threats affecting their sector or policy areas; an ability to make informed decisions based on cyber risk metrics and potential impacts; and the means to harness the right people, tools, policies, and other measures

Concerns about the widening gap between the demand for a highly trained cybersecurity workforce and the supply of talent have been growing for years

to manage cyber risk (Spidalieri, 2013). While many of these skills, knowledge, and attributes can be acquired by professionals in their respective fields through training and certifications, more efforts are needed to develop, upgrade, and expand educational programmes at the intersection of technology, policy, law, and economics. All these challenges have been widely recognised by experts and acknowledged by non-experts as well (I have personally been writing about these issues for over a decade).

Higher education institutions (HEIs), in particular, play a critical role in educating civilian and military workforces on the unique tenets of cybersecurity and can serve as incubators for the future workforce, bringing together theory with methodology, tools and implementation, and optimising campus-wide resources to combine knowledge, intellectual capacity, and practical skills. Establishing dedicated cybersecurity courses, offering hands-on training such as cyber-range platforms that simulate real-world attack scenarios, and developing multi-disciplinary programmes that incorporate cybersecurity components into existing public policy, international relations, social sciences, and business courses/degrees can help prepare a whole new generation of *cyber-strategic leaders*, researchers, and other professionals in a variety of important research and policy areas, and expose students to the growing array of cyber threats from a governance, legal, and policy perspective.

Finally, another persistent gap is between the *demand* for cyber-policy resources and applied research and the *supply* of high-value, usable information to support more informed cybersecurity policy- and decision-making. Government officials should tap into the extensive expertise that resides in academia, think tanks, and advocacy organisations, while academics and researchers in the cybersecurity field should do a better job of making their work most useful to, and more likely to be consumed and adopted by policy- and decision-makers. A 2017 report from RTI International and the Hewlett Foundation highlighted the disconnect between what government policy-makers need, and what researchers and scholars in the cybersecurity field often want to pursue or produce. The gap between academic research and policymaking has been well-documented in other fields, such as foreign policy and national security. To close this gap, government officials should communicate their needs and share their agency priorities more effectively; engage experts earlier on in the cyber-policy decision-making process; and provide more funding to academia and research centres to conduct the type of cyber-policy research needed. Cyber-policy experts and researchers should make a greater effort to understand the government's specific needs and priorities; identify and engage government stakeholders in their particular areas of expertise; clearly articulate the real-life impacts of cyber *insecurity*, cyber incidents, and vulnerable systems on national security, economic well-being, and critical services (without using too much technical jargon or falling for highly academic and theoretical issues); and provide actionable, objective, and timely information, findings, and recommendations in ways that policy-makers and senior leaders can easily understand and use (Rowe & Sugarman, 2017). Think tanks and other research institutes can also help bridge this gap and play an intermediary role by 'reaching out to industry for data, funding, and collaborative opportunities for their own use and for academics; meanwhile, academics should reach out more directly to industry on the same topics' (RTI International, 2017).

EFFORTS TO GROW THE CYBERSECURITY PIPELINE AND ICT SKILLS ACROSS THE EU AND THE US

Concerns about the widening gap between the demand for a highly trained cybersecurity workforce and the supply of talent have been growing for years as countries and organisations have become increasingly reliant on digital technologies and cyber threats have intensified. As demand continues to outstrip supply, the talent gap has continued to expand. To respond to this growing need, governments have begun to invest in workforce

development initiatives, support the expansion of cybersecurity educational programmes, promote innovation and cyber-R&D efforts, and launch campaigns to raise cybersecurity awareness. Civilian and military HEIs and professional education providers are also working to address the increased skills shortage by developing new academic and certification programmes and partnering with the industry to provide hands-on training activities like hackathons, cyber competitions, and Capture the Flag events.

The European Union Agency for Cybersecurity (ENISA) has launched several initiatives to enhance cybersecurity awareness, promote cybersecurity education, and address the cybersecurity skills shortage (ENISA, 2021). The 2020 EU Cybersecurity Strategy – a key component of the European Digital Strategy – encouraged increasing efforts to attract, train, and retain a professional cybersecurity workforce and invest in cybersecurity research, innovation, and deployment. The European Commission has proposed a number of practical measures to boost the EU's capabilities (e.g., NIS2, Europe Digital Programme, EU research and innovation funding framework programmes, Cyber Diplomacy Toolbox, and 5G Toolbox), improve the overall situation of the EU cybersecurity labour market, and establish cybersecurity competence centres to, among other things, help close the cybersecurity skills gap in the EU and avoid brain drain by ensuring that the best talents have access to large-scale European cybersecurity R&D projects and interesting professional challenges (European Commission, 2021). Three of the established competence centres – Concordia, CyberSec4Europe, and the newly launched European Cybersecurity Industrial, Technology and Research Competence Centre – have been tasked with assessing and helping to reshape the cybersecurity educational ecosystem in the EU and contributing to closing the cybersecurity skills gap, among other things. Nonetheless, several studies about HEIs' cybersecurity programmes have highlighted the still uneven distribution of academic programmes across EU countries and the *lack of common accreditation and minimum curriculum standards*, especially when dealing with the organisational, human, social, and operational aspects of cybersecurity education (Blazic, 2021). The majority of cybersecurity education and workforce development initiatives in Europe are still being pursued in silos and mostly within individual Member States.

In France, the Agence Nationale de la Sécurité des Systémes d'Information (ANSSI) – the country's national competent authority for cybersecurity – has established clear criteria for the accreditation of higher education courses in cybersecurity. The so-called SecNumedu labelling programme intends to assure students and employers that a university degree in cybersecurity meets the required criteria for teaching and training defined by ANSSI in collaboration with industry partners, academia, professional associations, and the Ministry of Education (ANSSI, n.d.). In the United Kingdom, even before Brexit, the National Cyber Security Centre established a process to certify bachelor's, master's, and doctoral degrees as well as apprenticeships in cybersecurity according to a series of requirements and planned activities.

In the United States, by contrast, many of the government initiatives to scale cybersecurity education, training, and workforce development, including the establishment of a National Initiative for Cybersecurity Education (NIST, n.d.) and other government-funded efforts, date back to the 2008 Comprehensive National Cybersecurity Initiative and the money allocated for this initiative (White House, 2009). Since then, various other initiatives and programmes aimed at expanding cybersecurity education and training opportunities, and developing a robust pipeline of cybersecurity professionals have proliferated. The National Security Agency (NSA) and the Department of Homeland Security (DHS) jointly sponsor the National Centers of Academic Excellence in Cybersecurity (NCAE-C) programme, which aims to foster a collaborative cybersecurity educational environment among colleges and universities, establish standards for cybersecurity curricula and academic excellence, and integrate cybersecurity practice within institutions and across academic disciplines (NSA, n.d.). Over 300 top colleges and universities have been designated as Centers of Academic Excellence institutions in one of three specialities – cyber defence, cyber operations, and research – which, in turn, have opened more opportunities for collaboration, additional funding, and an increased number of faculty and students.

Aside from the more advanced technical programmes, several academic institutions in the United States have also started to incorporate courses on emerging and disruptive technologies, cyberspace policy, cyber warfare, and management of cyber risks into traditional degree programmes in public policy, political science, international relations, and business administration, or as part of new multi-disciplinary undergraduate, graduate, and

PhD programmes. Business-oriented courses, for example, now address the opportunities and challenges of digital transformation and the cyber risks emanating from increased dependence on ICTs. Political science and international relations courses often explore the strategic, multi-dimensional power struggles among states over internet governance, the digital economy, and international norms of responsible state behaviour in cyberspace, including how major global powers use cyber capabilities as tools of national power to impose their interests, influence global politics, and conduct military operations and espionage campaigns in and through cyberspace. Private sector companies, such as Microsoft, Google, Amazon, Apple, and IBM, are also partnering with US community colleges and universities to train students in cybersecurity skills and have launched initiatives to teach coding skills to K-12 students.

To better prepare the future workforce for the needs of the cybersecurity labour market and meet the demand for practical skills and knowledge, some EU countries have also started to promote exchanges and collaborations with academia and industry partners. An example of this kind of partnership is the recently inaugurated Cyber Campus in Paris – a hub (similar to Israel's CyberSpark) that brings together national and international cybersecurity players from companies (large groups to small-and-medium businesses), government entities, training organisations, and professional associations to develop more effective cybersecurity solutions and capacity.[1] Its objectives are threefold: developing synergies between public and private actors to guide technological innovation and strengthen its integration into the economy; supporting the training of various audiences (e.g., government employees, students, and professionals) to increase the overall competence of the cybersecurity ecosystem; and providing a physical location for networking, exchanges, and events (RFI, 2022). Germany's federal government, instead, has created a Cybersecurity Innovation Agency, modelled after the US Defense Advanced Research Projects Agency (DARPA), aimed at developing state-of-the-art technologies and innovative cybersecurity solutions with the participation of industry experts (O'Neill, 2018).

Another way to provide hands-on experience and encourage young people to consider careers in cybersecurity is through cybersecurity challenges and exercises. Different organisations in the United States organise cybersecurity and coding challenges

Another way to provide hands-on experience and encourage young people to consider careers in cybersecurity is through cybersecurity challenges and exercises

for elementary, middle-, and high-school students to get them excited about careers in STEM disciplines, including cybersecurity. Programmes like the US CyberPatriot competition or the DefCon for Kids boot camp offer children aged 8 to 16 the opportunity to learn the basics of cybersecurity and cryptography, including how to find vulnerabilities, strengthen network security, and be white-hat hackers by learning reverse engineering and how to responsibly disclose security bugs (r00tz, 2021). DefCon for Kids even includes a 'Meet the Feds' workshop where young students in training can meet representatives of the NSA, DHS, and military investigation agents.

In Europe, ENISA organises an annual European Cyber Security Challenge to encourage the exchange of knowledge and talent across Europe. Individual countries have also launched their own national cyber competitions like Italy's CyberChallenge.IT (similar to the CyberPatriot's National Youth Cyber Defense Competition in the United States). This competition is held in over 40 locations across Italy and aims at promoting the development of cybersecurity skills among 16- to 24-year-olds living in Italy, stimulating their interest in IT and information security, and putting them in direct contact with companies. Its unique approach incorporates gaming as an instrument for attracting young people with multi-disciplinary training on technical, scientific, and ethical issues, alternating theoretical lectures and hands-on experiences on various topics such as cryptography, malware analysis, and web security.

Despite all these commendable initiatives on both sides of the Atlantic, disparate efforts to promote cybersecurity education and training programmes,

establish accreditation schemes for cybersecurity degrees, and develop ad hoc partnerships will not solve the skills shortage alone. More investments, effective coordination mechanisms, and creative solutions are needed to close the growing skills gap and build a robust pipeline of qualified candidates through education, training, and workforce development.

FUTURE CHALLENGES AND OPTIONS TO CLOSE THE WORKFORCE AND SKILL GAP IN EUROPE

The increase in frequency, scope, and severity of cyberattacks in Europe at a time when geopolitical tensions are higher than ever before in the twenty-first century, should prompt European leaders and senior executives in every organisation to prioritise cyber resilience and strengthen cybersecurity capabilities. Developing comprehensive cybersecurity policies, strategies, and security measures fit not only for today's needs but also for tomorrow's uncertainties and future cyber threats, requires bringing diverse perspectives, talents, and backgrounds to problem-solving and innovation. We cannot expect to solve complex problems and close the widening gap between the supply and demand of cybersecurity professionals without including more youth, women, and minorities, so diversity has to be part of the solution (Spidalieri, 2020).

Addressing the critical shortage in the cybersecurity workforce and its gender-based inequity must start at the leadership level. Leaders across society, policy-makers, and decision-makers must recognise, first, that all digital transformation and technological innovations they are promoting today involve a significant cyber risk; and second, that cybersecurity, cyber resilience, and cyber capacity-building should be considered strategic, cross-cutting issues and priorities of all digital development projects, digital strategies, economic/industrial policies, and recovery plans (Hathaway & Spidalieri, 2021). Closing the current workforce/skills and gender gaps requires a strong leadership commitment and significant investments to reverse these trends – from EU policy-makers to government agencies to universities to companies' boardrooms – and a concerted effort to work collaboratively to create the workforce of the future with a diversity of thoughts, genders, experiences, and backgrounds.

While no single panacea exists to attract more people to this growing field and develop a sufficient pool of talent with the requisite skills and interest to succeed in cybersecurity-related professions, starting in middle and high school and sustaining that interest over time; to engage young women and minorities in STEM fields (including cybersecurity) early; to give people with non-traditional backgrounds greater access to cybersecurity roles; and to expand multi-disciplinary programmes at the undergrad and graduate levels that include technology, policy, law, governance, economics, and international relations aspects. National governments, private sector companies, schools and universities, civil society, and individuals can all play a role. For each of these stakeholders, it is important to consider agency- and access-related barriers across an entire career lifecycle. This could result in a broad range of constructive changes: at one end of the spectrum, planning and implementing policies that address gender and racial inequity, at the other, establishing clear career paths that provide real prospects for those entering this ever-expanding profession and reward and retain cyber talents (Spidalieri & Kern, 2014).

In addition to these efforts and initiatives, organisations in both the public and private sectors should focus on developing programmes to further educate and retain their existing workforce and broaden the talent pipeline. This includes ensuring that all staff is regularly trained and tested so that they understand and fully appreciate their role in maintaining a strong cybersecurity posture; promoting tailored programmes for up-skilling and re-skilling in cybersecurity; providing employees with opportunities to connect with mentors and leaders within and outside their organisation to help navigate some of the perceived or actual barriers and further develop their skills; developing internships, traineeships, mentorships, and skill development programmes to help build the pipeline; offering employees other incentives such as opportunities to telework, flexible hours, and paid maternity/paternity leaves (this is not guaranteed in the United States as it is in EU countries); proactively promoting gender diversity in cybersecurity roles; and addressing wage disparity issues by establishing clear pay structures based on merit and movement through the profession.

Other effective mechanisms that can help organisations identify, recruit, and retain cybersecurity professionals, including women and minorities, include: fostering a gender-inclusive workplace; identifying universities that have higher percentages of women and minorities participating in cybersecurity or related programmes and recruiting from these institutions; joining other recruiting alliances that promote workforce diversity; placing increased value on real-world experience and

The current shortage calls for stronger efforts to raise awareness among youth about the opportunities and rewards of cybersecurity careers

aptitude (versus qualifications alone) and being prepared to train or reskill for specific cybersecurity roles; establishing an employee referral programme to recruit talented and trusted cybersecurity professionals from employees' personal networks (e.g., universities, colleges, and professional associations); providing guidance for career advancement and opportunities to reach senior leadership roles in cybersecurity.

POLICY RECOMMENDATIONS FOR EU POLICY-MAKERS

EU policy-makers, representatives of EU bodies, and national leaders should prioritise cybersecurity workforce development and capacity-building as core national and economic security priorities to develop safer and more resilient economies and societies, and meet tomorrow's challenges today. In the short term, all EU countries' national recovery and resilience plans should include a clear commitment to funding cybersecurity workforce development initiatives and promote better coordination among relevant stakeholders to achieve more successful outcomes. In the long term, the EU should continue to strengthen and harmonise its current efforts to grow a robust cybersecurity workforce pipeline and build an EU-wide cybersecurity ecosystem that can support its ambition for strategic autonomy. To support such longer-term efforts, additional recommendations would include:[2]

- Coordinate EU-wide initiatives to establish clearly defined cybersecurity roles and career paths as well as corresponding training and skills development programmes for experts and non-experts in both public and private sectors, including providing executive and operational training, formal internships, and traineeships. Specific training should be developed for EU and national-level actors involved in public policy and digital transition, including regulators and legislators. Training should be complemented with initiatives focused on cyber-policy development and cyber risk management, and with practical exercises within and among EU bodies and Member States and other stakeholders, including drills and simulations.
- Encourage broader and uniform adoption of certification schemes as identified by industry, ENISA, and the EU cybersecurity competence centres and recognised in all EU countries. Developing common accreditation schemes and minimum curriculum standards for cybersecurity degrees and training that follow the knowledge specifications within those certification schemes will facilitate the exchange of experts and mobility of the workforce with standardised levels of cybersecurity skills and knowledge across Europe.
- Facilitate the development, expansion, and *harmonisation* of dedicated school curricula and programmes aimed at accelerating cybersecurity skills development throughout the formal education systems of all EU Member States. While no single educational programme can cover all the specialised skills and sector-specific knowledge required by industry and government, new programmes should be inter/multi-disciplinary and cover not only technical but also non-technical skills and topics, such as digital literacy, public policy, law, governance, economics, risk management, ethics, social sciences, and international relations. Cybersecurity curricula should be developed across primary and secondary schools; dedicated degrees should be promoted and subsidised in all HEIs; and cybersecurity courses should be integrated into all computer science and IT programmes. Key to this effort is encouraging universities, colleges, and other educational institutions to work across departments and with other academic partners (nationally and internationally) to optimise resources and efforts when developing or updating cybersecurity programmes.
- Foster awareness of and stimulate interest in careers in STEM disciplines, including launching an EU-wide campaign to promote cybersecurity career opportunities, for example during the European Cybersecurity Month, which is already dedicated to promoting cybersecurity among EU citizens and organisations (EU, 2021).
- Launch an EU-wide call for cybersecurity talent to increase the supply of qualified cybersecurity professionals and grow the pipeline of future

employees, in particular for the public sector. This effort should include incentive mechanisms, such as grants and scholarships for students to pursue education and training in this field, and additional funds to support relevant apprenticeships/internships and help organisations retain talent.

- Support engagements with academia, the private sector, and civil society to address the ongoing gender gap of cybersecurity professionals in Europe and devise a gender-balanced approach for all skills development and training initiatives in order to better motivate, encourage, and facilitate the participation of women. A key partner in this effort should be Women4Cyber, a preeminent European non-profit organisation dedicated to promoting, encouraging, and supporting the participation of girls and women in the field of cybersecurity (Women4Cyber, 2021). Its broad network of government and industry partners, HEIs, research centres, and mentors, in addition to its active collaboration with the European Commission's DG CONNECT and other EU bodies, would provide invaluable insights and reinforce any new initiative in support of more gender-inclusive policy at the EU and national levels.

All these recommendations should be further studied, expanded, and tailored to the specific needs, resources, and capacities identified by EU agencies and Member States.

CONCLUSIONS

This chapter identified creative solutions and incentives to address the shortage of both technical and non-technical cybersecurity experts across public and private sector organisations and harmonise academic, research, and training efforts across EU Member States. The intent of this chapter is to catalyse further discussions among EU policymakers, representatives of EU bodies, as well as other Member States' organisations and academic institutions working on cyber capacity-building and cybersecurity skills development, including education, training, and workforce development initiatives.

Europe's ability to protect its security, economic prosperity, and societal development, ensure its resilience in times of crises, and build more secure digital societies hinges on its ability to prepare its leaders and future workforce for the challenges of the digital age. Attempts to use cyberspace and digital technologies for malicious purposes have matured in scope and sophistication over the past two decades; these threats will only intensify as criminals continue to embrace the low cost of entry/high-reward ratio and countries continue to use cyber instruments as offensive weapons and tools of national power. Meeting these challenges in both the public and private sectors requires careful planning and consideration and should focus on technical solutions and regulations as much as on developing a knowledgeable, capable, and diverse workforce.

NOTES

1. https://campuscyber.fr/en/.
2. Many of these recommendations have been drawn and adapted from the 'Guide to Developing a National Cybersecurity Strategy', https://ncsguide.org/the-guide/.

REFERENCES

ANSSI (Agence Nationale de la Sécurité des Systémes d'Information) (n.d.), 'SecNumedu, Labeling of Higher Education Courses in Cybersecurity', https://www.ssi.gouv.fr/en/cybersecurity-in-france/formations/secnumedu-labeling-of-higher-education-courses-in-cybersecurity.

Blazic, B.J. (2021), 'The Cybersecurity Labour Shortage in Europe: Moving to a New Concept for Education and Training'. *Technology in Society* 67, https://doi.org/10.1016/j.techsoc.2021.101769.

Chan, S. (2022), 'The Future of Women in Cybersecurity', *The Edge*, 3 March, https://www.theedgesingapore.com/views/environmental-social-and-governance/future-women-cybersecurity.

Cybersecurity Ventures (2021), 'Women Hold 25% of Cybersecurity Jobs Globally in 2021', 20 April, https://cybersecurityventures.com/women-hold-25-percent-of-cybersecurity-jobs-globally-in-2021.

ENISA (2021), 'Cybersecurity Education', https://www.enisa.europa.eu/topics/cybersecurity-education.

European Commission (n.d.). 'Recovery and Resilience Facility', https://ec.europa.eu/info/business-economy-euro/recovery-coronavirus/recovery-and-resilience-facility_en.

European Commission (2021), 'Commission to Invest Nearly €2 Billion from the Digital Europe Programme to Advance on the Digital Transition', 10 November, https://ec.europa.eu/commission/presscorner/detail/en/ip_21_5863.

European Commission (2022), 'European Cybersecurity Competence Network and Centre', 24 February, https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-competence-centre.

EU (European Union) (2021), 'European Cybersecurity Month', https://cybersecuritymonth.eu.

(ISC)² & EWF (2017), '2017 Global Information Security Workforce Study: Women in Cybersecurity', Executive Women's Forum on Information Security, Risk Management and Privacy, 15 March, https://www.ewf-usa.com/page/WomenInCybersecurity.

Fendorf, K., & Miller, J. (2022), 'Tracking Cyber Operations and Actors in the Russia-Ukraine War'. Council on Foreign Relations, 24 March, https://www.cfr.org/blog/tracking-cyber-operations-and-actors-russia-ukraine-war.

Hathaway, M., & Spidalieri, F. (2021), 'Integrating Cyber Capacity into the Digital Development Agenda', Global Forum on Cyber Expertise, November,https://thegfce.org/wp-content/uploads/2021/11/Integrating-Cybersecurity-into-Digital-Development_compressed.pdf.

Leitão Marques, M. (2021), 'Agencia de Notícias de Portugal', 28 April, https://www.lusa.pt/ppue2021/1661/article/31367168/eu-presidency-europe-has-290-000-unfilled-cybersecurity-jobs-mep.
Morgan, S. (2022), 'Cybersecurity Jobs Report: 3.5 Million Openings in 2025', *Cybersecurity Ventures*, 9 November, https://cybersecurityventures.com/jobs.
NIST (National Institute of Standards and Technologies) (n.d.), 'National Initiative for Cybersecurity Education – About', https://www.nist.gov/itl/applied-cybersecurity/nice/about.
NSA (National Security Agency) (n.d.), 'National Centers of Academic Excellence in Cybersecurity', https://www.nsa.gov/Academics/Centers-of-Academic-Excellence.
O'Neill, P. (2018), 'Germany Launches New Cybersecurity Research Agency Modeled After DARPA', *CyberScoop*, 30 August, https://www.cyberscoop.com/germany-cybersecurity-research-agency-modeled-after-darpa.
Rowe, B., & Sugarman, E. (2017), 'Cyber Officials Need Help, But Are Experts up to the Task?', *War on the Rocks*, 30 May, https://warontherocks.com/2017/05/cyber-officials-need-help-but-are-experts-up-to-the-task.
RFI (2022), 'France Launches "Cyber City" to Pool Resources for Better Digital Security', 16 February, https://www.rfi.fr/en/france/20220216-france-launches-cyber-city-to-pool-resources-for-better-digital-security.
R00tz (2021), 'A Place Where Kids Learn White-Hat Hacking to Better the World', https://r00tz.org.
RTI International (2017), 'Understanding Demand for Cyber Policy Resources', RTI Report for Hewlett Foundation's Cyber Initiative, https://www.rti.org/sites/default/files/resources/14759228_RTI_Cyber_Policy_Demand_Report_Final.pdf.
Spidalieri, F. (2013), 'One Leader at a Time: The Failure to Educate Future Leaders for an Age of Persistent Cyber Threat', Pell Center for International Relations and Public Policy, https://salve.edu/sites/default/files/filesfield/documents/pell_center_one_leader_time_13.pdf.
Spidalieri, F., & Kern, S. (2014), 'Professionalizing Cybersecurity: A Path to Universal Standards and Status', Pell Center Report, https://salve.edu/sites/default/files/filesfield/documents/Professionalizing-Cybersecurity.pdf.
Spidalieri, F. (2020), 'More Minority and Women Needed to Close the Cybersecurity Workforce & Skill Gap', Pell Center for International Relations and Public Policy, 8 May, https://www.pellcenter.org/more-women-needed-to-close-the-cybersecurity-workforce-gap-picks-of-the-week.
Terwoerds, L. (2017), 'Research Shows Women in Cybersecurity Face Under-representation, Discrimination and Stagnating Careers', Alta Associates, 15 May, https://www.altaassociates.com/research-shows-women-in-cybersecurity-face-under-representation-discrimination-and-stagnating-careers.
US CyberPatriot (2021), 'What is CyberPatriot?', US Air Force Association, https://www.uscyberpatriot.org/Pages/About/What-is-CyberPatriot.aspx.
White House (2009), 'The Comprehensive National Cybersecurity Initiative', https://obamawhitehouse.archives.gov/issues/foreign-policy/cybersecurity/national-initiative.
Women4Cyber (2021), 'Hacking Gender Barriers: Europe's Top Cyber Women', https://women4cyber.eu/roadmap-of-actions/100-women-in-cybersecurity-book.

Cyber Governance in the EU

Bushra Al Blooshi and Angelika Eksteen

https://doi.org/10.53121/ELFTPS3 • ISSN (print) 2791-3880 • ISSN (online) 2791-3899

ABSTRACT

Cyber governance is an increasingly important topic, and needs to be addressed mainly on the political rather than technical level. This chapter therefore analyses the process of creation, implementation, and measurement of individual cybersecurity strategies to achieve a better understanding of the levels of governance in the Member States. The authors conclude that there are striking similarities across the Member States and that, while there is a need for more EU governance, the right balance must be struck. The chapter uses the governance situation in Dubai to extrapolate useful insights and develop ad hoc policy recommendations that fit the EU context.

ABOUT THE AUTHORS

Bushra Al Blooshi is head of research and innovation at the Dubai Electronic Security Center (DESC), the first Arab member of the World Economic Forum's Global Future Council, and the chair of the Dubai Digital Authority's Digital Skills Committee. She leads many strategic initiatives in Dubai related to cybersecurity.

Angelika Eksteen worked with the DESC before becoming CEO of AI Directions, a company empowering organisations to transform AI advantages into innovation and success. Eksteen is editor of the ISO/IEC 27001 and many other international standards. She has a PhD in Mathematics.

INTRODUCTION

In recent years, a number of trends have changed our world and created new needs. The COVID-19 pandemic brought about a situation wherein more digital means of communication were used than ever before, creating the need to secure such communication, and all information thus exchanged and processed. At the same time, more and more sophisticated cyberattacks appeared, not only targeting large international companies, but also using the same or similar attack vectors across countries, attacking country-sensitive information, and using blackmail to exploit the dependence of organisations on their information.

This situation creates a need for effective cybersecurity standards, policies, overall governance, and cross-border thinking, applying protections as far-reaching as the attacks themselves. Cyber governance has thus become an international issue, with the involvement of various stakeholders from the public and private sectors, creating interesting challenges for harmonisation in the EU.

The problem involves all countries across the globe, but this chapter will focus on the EU, the situation there, and possible ways ahead. The EU plays an important role in this changing world, and it needs to have sufficient EU-wide cyber governance strategies, policies, and initiatives in place to play this role successfully. To understand more of the cybersecurity governance activities in the EU, we consider the different cybersecurity strategies in various EU countries, and their creation and implementation, as all this speaks to overall governance.

EUROPEAN PILLARS FOR A RESILIENT NATIONAL CYBERSECURITY STRATEGY

In 2018, the European Union Agency for Cybersecurity (ENISA) published a 'Guide to Develop a National Cybersecurity Strategy' (ENISA, 2016). This guide aimed to provide:

> a useful, flexible and user-friendly framework to set the context of a country's socio-economic vision and current security posture and to assist policy-makers in the development of a Strategy that takes into consideration a country's specific situation, cultural and societal values, and that encourages the pursuit of secure, resilient, ICT-enhanced and connected societies.

The ENISA guide distinguishes the 'process' that will be adopted by countries during the lifecycle of a National Cybersecurity Strategy (initiation, stock-taking and analysis, production, implementation, reviews) from the 'content', the actual text that would appear in a National Cybersecurity Strategy document. Elements of both speak towards achieving governance – the process of strategy development needs to be reliable, following typical criteria for such processes, as identified by ENISA and the International Telecommunications Union (ITU) (the ITU developed a similar guide on the development of strategies for an international audience), and true governance is only achieved if the strategy is implemented, and the success of this implementation is measured (ITU, 2018).

We do not necessarily know the process by which each of the strategies we will compare here was created, but there are some signs of a successful strategy, such as the achievements during its implementation. It is by now safe to assume that a cybersecurity strategy had a predecessor, therefore, the implementation of the respective predecessor can be measured. This is one of the first aspects we will consider. Another important aspect is how the implementation of the strategy is monitored, and whether and how success is measured.

The indicative criteria applied when looking at the different national cybersecurity strategies are listed below. They are based on the issues that have been addressed and the overall impression of the individual method of addressing them.

- Does the strategy contain references to the achievements that were made when implementing its predecessor, and what conclusions can be drawn from these references?

The Estonian Cybersecurity Strategy lists planned activities under the headings 'We prevent', 'We protect', and 'We develop'

- Does the strategy contain general principles, information about its development, or a plan for its implementation?
- Does the strategy refer to the process of monitoring and measuring its implementation, and what would define success in this process?

Finally, the national cybersecurity strategies describe the initiatives they are planning – these activities and their contribution to enhancing governance will be the basis of the fourth section of this chapter.

COMPARING NATIONAL EUROPEAN STRATEGIES

This chapter considers a number of the most recent national cybersecurity strategies, applying the criteria described above. We chose strategies that were in operation for no more than three years, avoiding any that might already be in their review cycle.

Estonia

This is already the third strategy for Estonia (Republic of Estonia, 2019), and states clearly in the introduction that it is based on the previous ones (2008–13 and 2014–17) and the lessons learnt from them. The strategy starts by highlighting the key impacts of implementing the previous strategies, and the objectives resulting from the implementation of their latest predecessor.

The Estonian Cybersecurity Strategy also lists planned activities under the headings 'We prevent', 'We protect', and 'We develop'. After discussing the current situation, including the latest threats, the Estonian Cybersecurity Strategy elaborates on Estonia's strengths and challenges. This is followed by an explanation of how the strategy links to other national and international strategies.

There are also several parts of the strategy that directly address governance:

- As a contributor to achieving the objective of a sustainable digital society (in the 2018 strategy): 'Fostering comprehensive governance and development of a cohesive cybersecurity community'.
- The E-Governance Academy has been founded to promote collaboration with like-minded countries, making active use of cyber-defence exercises, international discussion forums, and research studies offered by the centre.
- The strategy also refers to creating an EU cyber assistance network, including governance (discussed in the following section).

In summary, the Estonian Cybersecurity Strategy, its history as a follower of the previous strategies, and all the activities around it lean heavily towards achieving governance.

Finland

The establishment of Finland's Cybersecurity Strategy (Security Committee, 2019) followed a well-defined process, which is described in a document associated with the strategy (Cederberg, 2020), and includes a country analysis, vision and strategy, and implementation plan, with progress being monitored.

This strategy focuses on the main points that are to be achieved. Other typical contents, like a more detailed analysis of the country's situation, benefits of previous implementations, and plans for new initiatives are not contained in the document, but are partly available in others.

In summary, the Finnish Cybersecurity Strategy does not focus on governance as much as other strategies do, but some of the thought behind the contents reveals that governance has been considered:

> The role of the Cyber Security Director is to ensure the coordination of the development, planning and preparedness of cybersecurity in society. … Under his or her leadership, the overall picture and development programme of cybersecurity will be developed, drawing on the expertise of ministries, the Security Committee and cybersecurity actors. (Security Committee, 2019)

Spain

Spain's 2019 National Cybersecurity Strategy (National Security Council, 2019) is based on its 2013 strategy, which already 'designed the governance model for national cybersecurity'. The 2019 strategy 'boosts initiatives that complement further progress in the national governance model with European policies'.

The Spanish cybersecurity strategy describes actions to achieve its goals and details measures that will support the implementation of these actions. Finally, the strategy describes how the different responsibilities for cybersecurity are allocated in the National Security System.

In summary, the overall construction, the information presented, and the style of presentation clearly show that cyber governance is the aim of this strategy. Even the final words, which summarise the change from the 2013 to the 2019 strategy by including a set of actions to allow responses to rapidly changing threats, clearly base all the activities on a considerably mature governance model.

Luxembourg

Luxembourg's fourth National Cybersecurity Strategy (Government of the Grand Duchy of Luxembourg, 2021) has been built on the previous three strategies and includes multiple concrete and measurable actions that are set out in an internal monitoring table (available upon request).

The strategy makes several clear statements about governance, such as: 'The governance framework for the use of public cloud services at the state level or in the provision of public services will be defined', and:

> The identification and exchange of relevant risk scenarios and metrics is a collective activity that will be coordinated at State level and documented in the Risk Scenario Sharing Platform (MOSP). This will be accessible as a public service, which in the medium term will substantially contribute to increasing the quality of governance (informed governance) and resilience.

In addition, Luxembourg's strategy defines the National Cybersecurity Governance Framework in a dedicated chapter, detailing:

- The inter-ministerial cyber prevention and cybersecurity coordination committee
- Key state entities involved in national cybersecurity governance
- Initiatives, such as Cybersecurity Luxembourg, Bee Secure Government, and the overall cybersecurity ecosystem in Luxembourg

In summary, the Luxembourg strategy clearly refers to the governance activities that are either in place

or will be undertaken to ensure a well-governed cybersecurity ecosystem in Luxembourg.

Germany

For the development of Germany's Cybersecurity Strategy 2021, the current state of cybersecurity was analysed, and then the objectives for the new strategy were established. Together with this, the implementation and review were institutionalised: 'As a further significant innovation in relation to the latest cybersecurity strategy, the implementation of the strategy should be continuously monitored and reviewed. To this end, all strategic objectives are defined with defined indicators, on the basis of which the success of the strategy can be traceably controlled'. Section 9 of the strategy details these thoughts further.

The German Cybersecurity Strategy 2021 is written in a considerably different way than the other strategies considered. It identifies a large number (44) of cybersecurity topics to be addressed, and then for each of these topics, consider the following:

- Is this goal relevant?
  - Where do we stand?
  - What do we want to achieve?
- What effects do we expect?
  - Why do we let ourselves be measured?

One particular aim also addresses governance directly: 'Strengthen international law and the normative framework for cyberspace and influence responsible governance'.

In summary, the way the German Cybersecurity Strategy 2021 is structured and the shift of emphasis from statements of what needs to be done to a complete framework of activities speaks strongly of governance.

INITIATIVES TO MEET THE ESTABLISHED GOALS

The individual countries' strategies highlight several important initiatives, which are listed below:

Estonia

Estonia's Cybersecurity Strategy plans implementation of several activities, including one that addresses governance, among other issues:

> 'Estonia makes a leading contribution to ensuring competitive and sustainable cyber capability in partner countries and takes part in creating an EU cyber assistance network'.
>
> The objective of the activity is to ensure that Estonia would be able, if necessary, to promote a competitive and sustainable cyber capability in partner countries. Estonia can share its experiences with other countries, by taking part in EU, NATO, and other international projects. In addition, specific fields that are within Estonia's capabilities and necessary for Estonia must be defined in international digital and cyber cooperation – for example, planning of policies and strategies in the cybersecurity field, e-governance, a certain geographic focus, countries in other regions, etc. ... Being involved in international standardization and certification processes is also important. (Cybersecurity Strategy of Estonia).

Finland

Another document from Finland associates the strategic objectives with companies in Finland offering cybersecurity services and solutions (Business Finland, 2020). The listed companies address governance in their company programmes; details can be found in the document.

In these cases, the companies' business models are to apply cybersecurity technology to gain further insights to support governance.

Spain

Goal V of Spain's Cybersecurity Strategy, the 'International Cyberspace Security', makes several references to governance, including a statement that the strengthening of the Internet together with European partners can only happen on a governance basis, and the active role Spain will take in different interest groups, such as the Internet Governance Forum.

This goal is supported by 'Line of Action 6', which addresses the contribution to international activities to secure cyberspace. This is supported by six detailed measures that will all work towards achieving more governance.

Luxembourg

The Luxembourg strategy defines an action plan for the overall implementation of the strategy, but unfortunately, this document is not publicly available.

Germany

In Germany's strategy, every one of the cybersecurity topics identified contains a section called 'What do we want to achieve' – these are the initiatives

There is still a lack of understanding of cyber governance, considerably more than in other areas

that are put in place to implement the strategy. In the area of governance, this translates to an international framework for harmonised standardisation of practices and a common framework for cybersecurity legislation.

GAPS, CHALLENGES, AND OPTIONS

Cybersecurity and cyber governance are not only technical but also political issues; therefore, the challenges and opportunities considered also focus on the political level. Despite the differences among EU Member States, of which they are proud and which they wish to maintain, there should be common ground in establishing cyber governance, and cross-border issues should be addressed at the EU level. The challenge here is to strike the right balance between providing EU-wide policies or standards, while leaving enough space for country-specific implementation.

Another challenge is communication in case of problems. The EU has already taken significant steps to establish strategies, protect critical infrastructure, increasingly regulate the single digital market, and fight cybercrime. But there is still a great need for more information exchange, not only between the Member States but also between the private and the public sector. This results from the traditional reluctance to share information about the cybersecurity incidents that we still see around the world. It is important to overcome this inhibition, as sharing such information will ultimately help all.

Looking at the bigger picture internationally, recent changes have made conversations between different countries more difficult in some cases, and further fragmentation can happen any day because of overriding issues, such as supply chain disruptions, or attacks with unclear origins. The EU needs to support its Member States and present a united front to strengthen its position.

Finally, there is still a lack of understanding of cyber governance, considerably more than in other areas, because of the technical nature of many cybersecurity questions. This lack of understanding may well lead to a lack of execution and omitting necessary activities will not improve overall security.

DUBAI'S SITUATION

History

Dubai has a well-established cybersecurity governance model, an effort that started in 2012 with a committee formulated from across critical infrastructure entities under Resolution No 13 of 2012 to define the cybersecurity model and governance framework for the city. The committee's work was finalised with the Information Security Regulation (ISR) and the work was handed over to the newly established Dubai Electronic Security Center (DESC). The main objective of the centre is to govern, regulate, and monitor cybersecurity in Dubai.

About the ISR

The ISR's main purpose is to provide Critical Information Infrastructures entities in Dubai with the right controls to ensure the resilience of critical services and minimise information security-related risks and damage by preventing and/or minimising information security incidents. The regulation consists of 13 main domains that are grouped into three main categories: governance, operations, and assurance. Governance sets the high-level requirements for structuring and managing information security, while the operation domains set the technical controls that might be used based on risk-assessment results. The assurance domains set the resilience and quality controls. Table 1 shows the ISR's main domains and their categories.

About the governance model

The main objectives of the governance domain are:

- Aligning Information security with the entity's strategic direction
- Ensuring information security objectives are achieved
- Managing risks appropriately
- Using the entity's resources responsibly
- Continuous monitoring of the information security programme

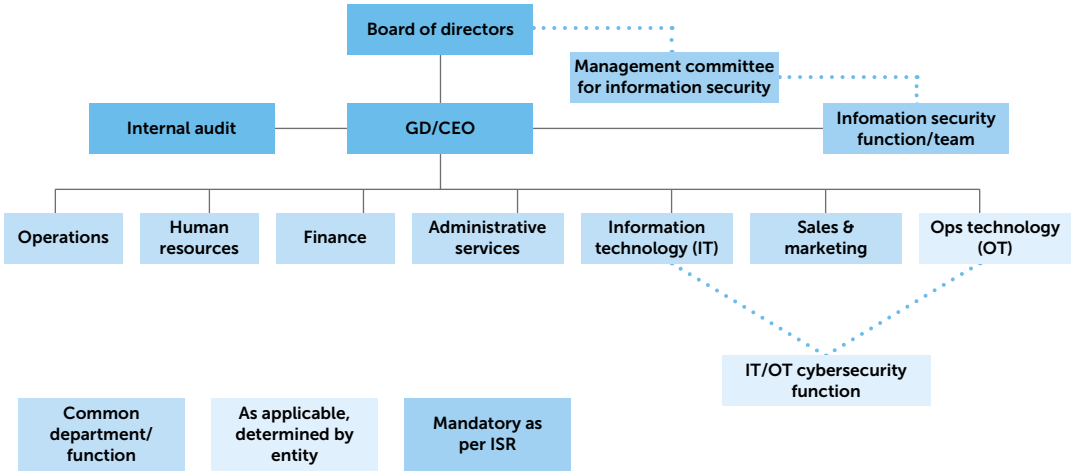
The governance model in ISR requests all CII entities to identify their information security functionaries, who should report to the top management and not IT departments. This functionary is responsible

TABLE 1: **Information security regulation domains and classes**

Domains		Classes		
		Governance	**Operation**	**Assurance**
	**Domain 1 – Information Security Management and Governance**	✓		
	**Domain 2 – Information and information Asset Management**	✓	✓	
	**Domain 3 – Information Security Risk Management**	✓	✓	
	**Domain 4 – Incident and Problem Management**		✓	
	**Domain 5 – Access Control**		✓	
	**Domain 6 – Operations, Systems and Communication Management**		✓	
	**Domain 7 – Business Continuity Planning**	✓	✓	
	**Domain 8 – Information Systems Acquisition, Development and Management**		✓	
	**Domain 9 – Environmental and Physical Security**		✓	
	**Domain 10 – Roles and Responsiblities of Human Resources**	✓	✓	
	**Domain 11 – Compliance and Audit**	✓		✓
	**Domain 12 – Information Security Assurance and Performance Assessment**	✓		✓
	**Domain 13 – Cloud Security**	✓		✓

Source: ISR

FIGURE 1: **Managerial structure of ISR**



Source: DESC

for overall information security within the entity. Moreover, it also requires establishing an information security management committee that is led by the entity's CEO (see Figure 1).

Information security function responsibilities

A CII entity allocates the responsibility for information security to a capable and independent position, reporting to the top management or to the steering committee, while considering the segregation of duties and omitting the conflicts of interests. The information security position is assigned the following responsibilities:

- Plan, implement, and maintain an information security programme/management system that is integrated with the whole entity's processes.
- Coordinate with the senior management on the identification, development, secure handling, and management of entity-wide information assets.
- Plan, develop, and maintain an organisation-wide information security risk-assessment methodology in coordination with the entity's senior management.
- Ensure that appropriate operational controls are selected and implemented according to the results of the risk assessment.
- Develop the required policies and procedures based on the results of the risk assessment.
- Ensure organisation-wide compliance with the information security programme/management system and report on ISR implementation status to the information security steering committee.
- Assist and support senior management in their information security responsibilities.
- Plan and conduct periodic information security awareness education and training for the entity's staff and applicable external parties.

Information security steering committee

An information security steering committee, headed by the director general or their deputy, must be established and should include the heads of each division in the entity. The steering committee should have the following roles and responsibilities:

- Supervise and ensure the implementation of an information security management system and its controls across the entity.
- Conduct periodical reviews on the implementation of the ISR and any information security controls and objectives.
- Review and approve periodically the information security policies and procedures for implementation within the entity.
- Promote information security culture within the entity.
- Ensure that relevant information security methodologies are part of all business processes and new initiatives or projects across all the entity departments or functions.
- Follow up and review both internal and external audit results for the effectiveness of ISR

implementation and ensure necessary and timely corrective action.
- Review and approve the information security risk-assessment methodology and risk assessment-related results that are used across the entity.
- Ensure that adequate resources are provided to implement, support, and operate the information security management system.
- Make recommendations for both corrective and preventive action based on the risk-assessment approach.
- Review information security incidents and the responses to them.
- Ensure that recommendations approved by the committee are implemented.
- Ensure that Information Security requirements are integrated as part of contractual requirements in their respective project management activities.

Multi-tier assurance process

ISR implementation is audited internally by the information security functionary of the entity. After that, it is also audited by the audit team in DESC. This multi-tier audit and assurance has created well-defined governance at the entity, sector, and city levels.

CONCLUSIONS AND USEFUL INSIGHTS FOR POLICY-MAKERS

The assessment of the current EU situation and the EU's governance activities clearly shows that the Member States:

- are putting cyber governance in place in different ways, but their overall aims are comparable.
- have expressed the need for cross-border solutions, in addition to the efforts made in the state itself.

The EU is in a position to support such governance actions and do the following:

- Establish an EU-wide governance framework that helps harmonise the actions of individual states. This can, for example, start off with an update/expansion of the current ENISA strategy development document (ENISA, 2016) to include general EU governance goals and how to achieve them. A particular emphasis should be placed on the distinction between overarching governance elements that need EU guidance and harmonisation and those that should remain up to individual Member States.
- Identify a common approach that supports local needs while driving harmonisation at the EU and international levels. International governance frameworks such as the ISO 38000 or ISO 39000 series can be used to support this effort.
- Help garner resources for the establishment and maintenance of cyber governance, which, like any other activity, needs resources. It is a well-known fact that there is a shortage of resources in the field of cybersecurity as a whole, and of people with deep knowledge of cyber governance in particular. The EU should, together with the Member States, implement a suite of programmes to decrease this shortage (for more information on this topic, please refer to [Chapter 4]).
- Work with the private sector and groups such as the Institute of Directors to create awareness and understanding of what cyber governance is, and what it is not. Cyber governance and cybersecurity management, such as ISO/IEC 27001, are still commonly confused. EU Member States should also be encouraged to do the same. In turn, this would make the private sector's cybersecurity talents, services, and solutions more accessible.

REFERENCES

Business Finland (2020), 'Cybersecurity from Finland', 3 July, https://www.businessfinland.fi/49ed06/contentassets/9d10aa6fff2c469d905e61b3507dd6f0/finnish_solutions_for_cyber_security_web.pdf.

Cederberg, A. (2020), 'A Comprehensive Cybersecurity Approach – The Finnish Model', https://www.cyberwatchfinland.fi/wp-content/uploads/2020/07/A-COMPREHENSIVE-CYBER-SECURITY-APPROACH---THE-FINNISH-MODEL.pdf.

ENISA (European Union Agency for Cybersecurity) (2016), 'National Cyber Security Strategy Good Practice Guide – Designing and Implementing National Cyber Security Strategies', 14 November, https://www.enisa.europa.eu/publications/ncss-good-practice-guide.

Government of the Grand Duchy of Luxembourg (2021), 'National Cybersecurity Strategy IV', https://hcpn.gouvernement.lu/dam-assets/fr/publications/brochure-livre/strategie-nationale-cybersecurite-4/National-Cybersecurity-Strategy-IV.pdf.

ITU (International Telecommunications Union) (2018), 'Guide to Developing a National Cybersecurity Strategy – Strategic Engagement in Cybersecurity', https://www.itu.int/pub/D-STR-CYB_GUIDE.01.

National Security Council (2019), 'National Cybersecurity Strategy 2019', Government of Spain, https://www.ccn-cert.cni.es/en/about-us/spanish-cybersecurity-strategy-2013.html.

Republic of Estonia (2019), 'Cybersecurity Strategy 2019–2022', July, https://dea.digar.ee/cgi-bin/dea?a=d&d=JVestinformsyst201907.2.7.3&e=-------et-25--1--txt-txIN%7ctxTI%7ctxAU%7ctxTA----------.

Security Committee (2019), 'Finland's Cybersecurity Strategy 2019', https://turvallisuuskomitea.fi/en/finlands-cyber-security-strategy-2019.

Europe's Digital Discontent

Lior Tabansky

https://doi.org/10.53121/ELFTPS3 • ISSN (print) 2791-3880 • ISSN (online) 2791-3899

ABSTRACT

Can the EU innovate its way into a leadership position in the technological race? All the EU's plans to reduce digital dependency imply that it needs to innovate better, faster, and more effectively. This chapter explores two major moves towards digital sovereignty: those in cloud computing and chip-making. It argues that the EU has ample fiscal and human capital for disruptive innovation. The problem is, therefore, that the political structure prevents the EU from attempting moon shots. The longer the EU avoids acknowledging its structural impediments to innovation, the deeper China's and the United States' advantage over Europe will grow.

ABOUT THE AUTHOR

Lior Tabansky of Tel Aviv University is the Head of Research Development at Blavatnik Interdisciplinary Cyber Research Center and the Academic Director of the 'Effective Cybersecurity' Executive Education programme. Tabansky studies the intersection of technology and power, including defence innovation; small states' national security strategies; hostile influence operations via social media; and cyber capability maturity. Lior offers a unique grasp of cybersecurity, combining academic research in security studies with 15 years of professional IT work and business experience in formulating cyber strategies.

DIGITAL DEPENDENCY: DATA, CLOUD, CHIPS

This first section exposes the relevance of the topic in the context of EU strategic autonomy and assesses the EU situation.

The EU's Lisbon agenda aimed for it to become the most competitive and most dynamic knowledge-based economy in the world by 2010. French President Emmanuel Macron said in a marathon speech at the Sorbonne in Paris in 2017:

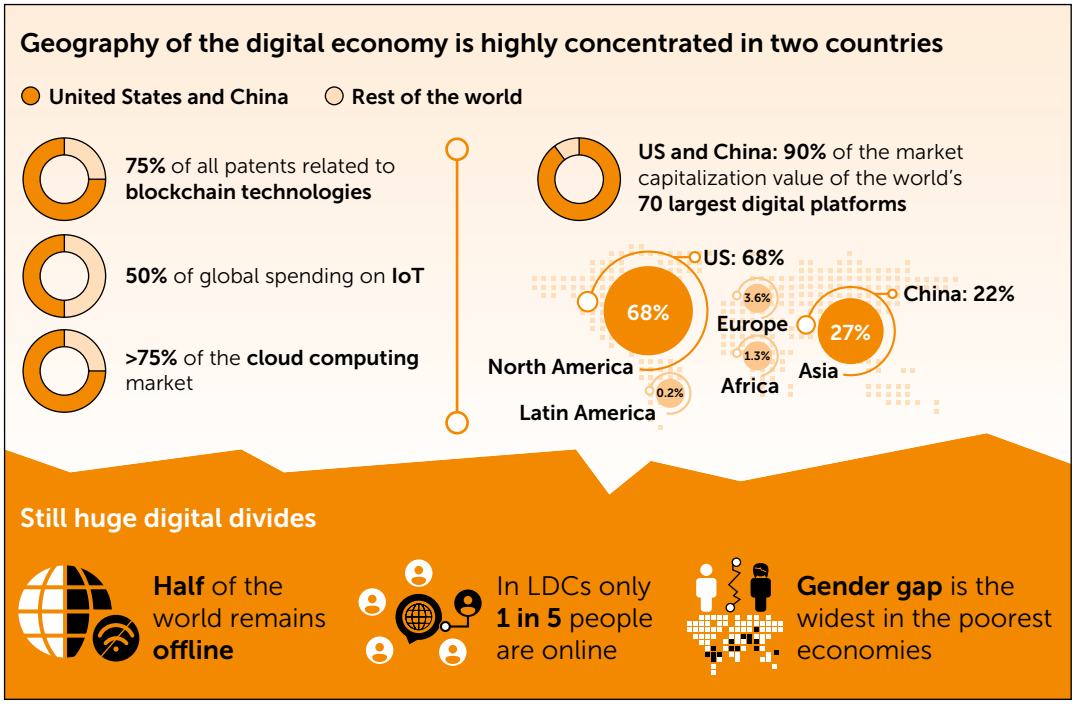
> The Europe we know is too weak, too slow, too inefficient, but only Europe gives us the capacity to act on the world stage in the face of the big, contemporary challenges. (Macron, 2022)

Yet, a decade later, Europe's overall competitive position has not improved. Across the board, digital technological capabilities increasingly underpin all instruments of power: diplomacy, information, military, and economy. Reluctantly, the EU has acknowledged that for most things digital, Europe depends strongly on US technology, infrastructure, and businesses. From a realistic international relations (IR) perspective, the dependency on the United States means grave geopolitical risks for the EU, some of which are already looming.

The United States and China hold over 90 per cent of the 70 largest digital platforms' market value and control over 75 per cent of the cloud computing market (UNCTAD, 2019).

US cloud service providers dominate Europe in terms of both business volume and the rate of technological improvements. Domestic providers – Deutsche Telekom, Orange, and OVHcloud – often simply resell the services of US companies such as Google and IBM. Data from the EU mostly flows to the United States and the UK (European Commission, n.d.).

FIGURE 1:



Source: UNCTAD, 2019

Chips and microprocessors are critical components of not only clouds but practically every electronic product. The main steps in producing microchips are designing, manufacturing, assembling, testing, and packaging. They represent the pinnacle of scientific-technological progress by combining hundreds of highly specialised cutting-edge innovations in chemistry, quantum physics, materials, and algorithms. Intel (US) and Samsung (South Korea) are among the few companies that cover all three steps – design, manufacture, and assembly – by themselves. Most others specialise in design (ARM, UK) or manufacturing (TSMC, Taiwan). The European semiconductor industry has plunged from a 40 per cent market share in the 1990s to 10 per cent today (European Commission, 2021b). As a result, European producers and consumers depend entirely on US and Asian firms for microchips.

Both the United States and China leverage digital technologies and supply chains for the geopolitical contest. It is better late than never for the EU to come to terms with the problem. Recently, the EU has officially acknowledged that Europe needs digital sovereignty and strategic autonomy: both for internal reasons, namely closer and deeper integration of the Member States, and for external reasons, namely to wrest back global power. The EU has put forth a strategy to counter digital dependency: to innovate better, faster, and more effectively.

Let us examine two major innovation efforts towards digital sovereignty: cloud computing and chip-making.

GAIA-X WILL THRIVE ON THE EUROPEAN REGULATION

Current EU initiatives

In September 2012, the European Commission adopted the first 'European Cloud Computing Strategy', which called upon Member States to embrace the potential of the cloud. The recent European Data Strategy bluntly states that the EU needs to reduce its dependency on foreign cloud infrastructure and cloud providers. As of 2019, the EU intends to invest €2 billion via the European Data Strategy in a European High Impact Project that will federate energy-efficient and trustworthy cloud infrastructures and related services. In addition, cloud technologies developed within Horizon 2020-funded research and market actors will be

deployed via the Connecting Europe Facility 2 (for cloud infrastructures interconnection) and Digital Europe programme (for cloud-to-edge services and cloud marketplaces).

France recognised and acted upon the cloud risk early, launching the Andromède sovereign cloud project back in 2009. Despite the advantages of the language barrier, market access, policy support, and over €150 million in state-funded investment in capable French IT and telecommunications firms, France has not been able to sustain the initiative. Notably, the EU has not supported this early attempt to advance the foundations for technological sovereignty.

In October 2019, France and Germany announced GAIA-X: the basis for an open-data infrastructure that represents 'European values' and will interconnect cloud providers around Europe. The Gaia-X architecture is based on the principles of federation, distributed consensus, decentralisation, and regulation by automation (GAIA, 2021). As of early 2022, The GAIA-X international alliance counts 1,800 participants from over 500 institutions as members. No non-EU firms have applied to join (GAIA, n.d.).

An earlier relevant EU response was to introduce data regulations and localisation requirements. Europe's General Data Protection Regulation (GDPR) imposed data localisation de facto (European Council, 2016a; GDPR.EU, n.d.; Cory & Dascoli, 2021). The later EU Cybersecurity Act, the regulation on the free flow of non-personal data, the European Data Strategy, regulations on facial recognition in the EU and other more obscure principles, guidelines, and directives have further tightened restrictions on data use.[1] The EU justified these in terms of privacy protections, law enforcement, and broader moral arguments. The United States and other observers often see these as market protection instead. Intentionally or not, these and other regulations support the commercial case for an EU cloud.

Will the GAIA-X federated cloud computing infrastructure work? Yes. GAIA-X can grow into a commercially sustainable and profitable proposition. The reasons for this optimism are the combination of mature distributed computing technologies, dedicated public funding, and tailored regulatory support. GAIA-X and its participants will enjoy a de facto locked customer base of the market. European public agencies are the most likely and loyal customers. These may suffice to establish the critical mass and drive efficiencies. As the global business trend of moving from on-premises to cloud services will continue, Europe's private corporations will consume more and more cloud services. All of them will be nudged along with the political incentive to consume cloud services from GAIA-X. Foreign firms with operations in the EU are likely to decide based on the same set of incentives: European regulatory risks, nudging, and costs comparable to the US providers across most standard offerings.

BUT REGULATING DATA IS AN ILLUSION OF CONTROL

Data regulations cannot impose sovereign control. Regulators face two nearly impossible tasks: exclude access to data and detect misuse. The obstacles stem from the type of economic creature that data is. Enter the 2018 Nobel Prize in Economic Sciences. The work of Paul Michael Romer (and William Nordhaus) received the highest honour for demonstrating how the conventional forces of production fail to explain modern economic growth and how data, information, and ideas drive long-term economic growth. Moreover, Romer's 'new growth theory', first presented in 'Endogenous Technological Change' (Romer, 1990) stresses how data, information, knowledge, and wisdom differ from traditional goods (see Table 1).

One may share data, information, ideas, algorithms, and software, but unlike when one shares a loaf of bread, one's own share never diminishes as a result. Consider software code: makers, hackers, and large firms can reliably reuse and modify it, patents and other protections notwithstanding. A sovereign may outlaw pirated copies, but cannot directly obstruct the functionality of software.

How would one control the use of data as an input, and for what purposes? Is it possible to distinguish

TABLE 1: **Differences Between Traditional Goods and Data, Information and Knowledge**

Traditional goods	Data and knowledge goods
Tangible physical object	Largely intangible
Rivalrous, excludable	Non-rivalrous, partially excludable
Often perishable	Durable

Source: Author's elaboration based on Romer (1990)

A radical innovation in chips is risky, but success will reap great benefits: it may render obsolete entire classes of products and services

original from copied data? After all, no matter how, how often, when, and where data is being used, data itself will remain intact. Unlike a half-eaten slice of bread, no evidence of consumption remains. Compliance depends on the cooperation of those who use data: foreign and domestic companies. Google, Facebook, and others profit from matching targeted ads with potential buyers. They innovate tracking and partially give up on cookies. However, in other use cases, each could reliably present answers to explain *'Why am I seeing this ad?'*.

Data does not lend itself to controls fit for tangible goods. Those who had succeeded in detecting past abuses have enjoyed privileged access to people, infrastructure, or databases and usually act after the abuse and the damage caused. When dealing with non-rivalrous, largely intangible, durable, and only partially excludable goods, data regulation will leave the EU lagging behind the United States and China in the digital economy.

EUROPE CAN DOUBLE ITS MARKET SHARE IN ADVANCED SEMICONDUCTORS

EU current initiatives

The response? 'Europe's Digital Decade: Digital Targets for 2030' – the EU sets a goal to double the EU's share of global production of the most advanced semiconductors between 2nm and 5nm (Breton, 2021).

Europe's pockets of competitiveness in academia are the Inter-university Micro Electronics Center in Belgium, the Laboratory of Electronics and Information Technology in France, and the Fraunhofer Institute in Germany. Europe's pockets of competitiveness in the industry are the Germany-based Infineon, the Netherlands-based ASML (which makes Extreme Ultra-Violet lithography systems), and NXP Semiconductors, also based in the Netherlands. Designing and making a chip requires a complex combination of hundreds of highly specialised cutting-edge innovations in chemistry, quantum physics, materials, and algorithms. It is also a capital-intensive industry. In 2022 alone, massive capital expenditure is planned: Intel expects to spend $28 billion, TSMC $44 billion, and Samsung $33 billion (Economist, 2022). These are cushioned by public money in the form of subsidies and incentives. The US Department of Commerce has urged Congress to pass a bill that includes $52 billion in handouts to chipmakers (*The Economist*, 2022).

Europe too can afford to spend tens of billions of euros from public and private sources. It is likely that by 2030 European firms will design, manufacture, and package far more semiconductors and gain 20 per cent of the market. However, these will be competing with offers from incumbents.

BUT CARVING OUT A SHARE IN THE SILICON-BASED SEMICONDUCTORS MARKET WILL TRAP EUROPE AS AN ALSO-RAN

The silicon-based improvement in computing power is based on semiconductor miniaturisation. It is nearing its end: physically, there is not much more room left (Leiserson et al., 2020). At 5nm, the scale is already too close to the size of an atom. Some of the directions for improvements in computing power are:

- Materials: graphene, black phosphorus, transition metal dichalcogenides, boron nitride nanosheets, and carbon nanotubes. Intel and other tech giants are not the only investors in these innovations. The US Defense Advanced Research Projects Agency alone has committed grants of $300 million per year for basic research into new designs and materials for chips (Service, 2018).
- Hardware architecture simplification: replace a large and complex processing core with several simpler cores, each with a lower transistor count and less complex architecture. Many processor cores running in parallel can perform some tasks much faster and more efficiently (e.g., GPUs).
- Domain specialisation: customise chip hardware for a particular application domain (e.g., network controllers, AI processors, SSD controllers).

The global incumbents are investing in these directions. Amazon acquired Israel's Annapurna Labs for an estimated $370 million in 2015 (Janakiram, 2019). NVidia acquired Israel's Mellanox, which specialises

in network controllers and interconnect solutions, for $7 billion (NVIDIA, 2020). Intel acquired the Israeli start-up Habana Labs, which designs custom chips for deep learning, for $2 billion in 2019 (Scheer & Rabinovitch, 2019; Intel, 2019). The radical directions for breakthroughs in computing are:

- Biological computers using molecules to perform computations.
- Quantum computers harnessing the collective properties of quantum states, such as superposition, interference, and entanglement, to perform calculations (Nellis, 2021).

Both face fundamental scientific challenges – biology, genetics, and quantum mechanics; designing a new class of software; and creating tailored materials. However, as the scientific-technical foundations for biological and quantum computers are embryonic, business research and development (R&D) is not there yet. Moreover, the incumbents are unlikely to undermine their prosperous lines of business.

A radical innovation in chips is risky, but success will reap great benefits: it may render obsolete entire classes of products and services. Even if a quantum or biological computing class coexists with silicon-based integrated circuits, radical innovation will gain a first-comer's advantage in the high-end niches of the markets and secure outsized premiums, margin, and profits. However, the current EU plans, which probably came to life through a consensus – do not aim too high. 'Europe's Digital Decade: Digital Targets for 2030' includes a chapter on quantum computing. The EU has launched the Future and Emerging Technology Flagship – Quantum, with an investment of €1 billion from various sources over several years. A radical innovation demands much higher ambitions and risks. Giving up on carving out a larger slice of the current silicon-based pie would free up more resources for such ambitious initiatives.

A SENSIBLE HORIZON?

Further challenges and options

Public policy and funding are essential for basic science.[2] Scientific development, funded by the state, precedes current commercial applications, often by decades.[3] Business R&D builds upon the fruits of basic science. Europe has a broad and solid academic base with the best universities and research institutions globally, an educated and skilled workforce, policies to support entrepreneurship, a large industrial base, and very innovative companies. Why the lack of breakthrough innovation? In the same 2017 speech, Macron said that one of the six keys to European sovereignty, namely a 'Europe of innovation and regulation adapted to the digital world', meant that:

> Europe must lead rather than undergo this transformation, by promoting its model within globalisation, a model combining innovation and regulation. It must have an agency for breakthrough innovation, jointly financing new research fields, such as artificial intelligence, or unexplored fields. It must guarantee equity and trust in the digital transformation, by reviewing its fiscal systems [taxing digital technology corporations] and by regulating the major platforms (Elysée, 2017).

The EU possesses an enviable war chest, chiefly the nine European Framework Programmes for Research and Innovation (FPs) of the magnitude of tens of billions of euros annually (Abbott, 2019). The Horizon 2020 mechanism attempts to direct innovation towards the seven societal challenges listed and the areas of activity that cut across several societal challenges, such as digitisation.

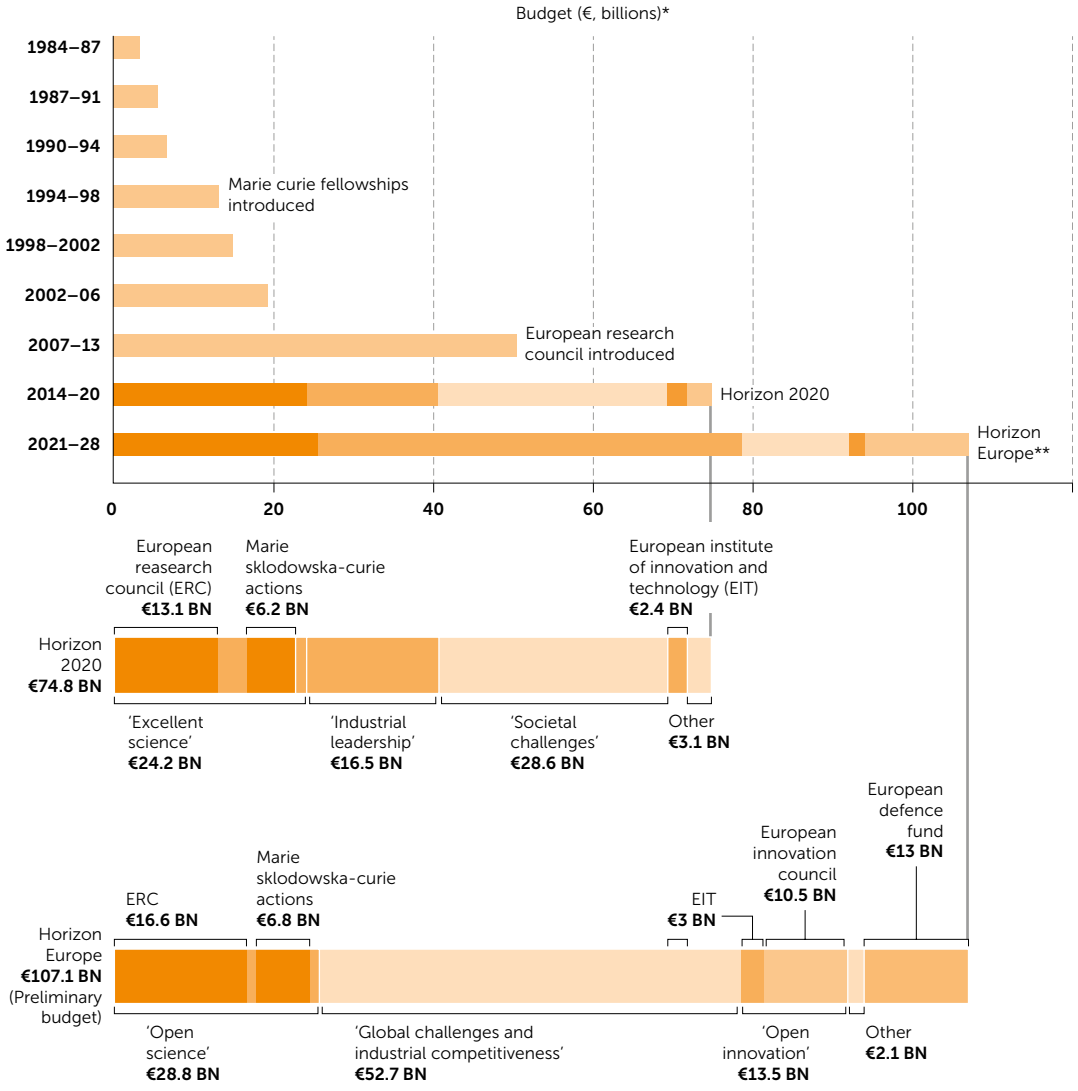
Having distributed €60 billion to 150,000 participants across 27 Member States and more than a dozen other countries, including research-intensive nations such as Israel and Switzerland (Nature, 2019), even the foremost European innovation guru Mazzucato admits that Horizon 2020 'has stopped short of delivering broad societal impact' (Mazzucato, 2018). I leave it to the reader to examine the 15 success stories in the Director General for Research and Innovation report for the EU (European Commission, 2019a).

Horizon Europe has a budget of €95.5 billion for the 2021–2027 period, of which €15.3 billion is dedicated to the 'digital, industry and space' challenge. Its three pillars – excellent science, global challenges and European industrial competitiveness, and innovative Europe – sound perfect. The EU says that Horizon Europe incorporates lessons learned in Horizon 2020, including increasing support for breakthrough innovation. Despite the lack of disruptive innovations that came to life via FPs, the EU Institutions are content: these added high EU value,[4] and the implementation of the Horizon 2020 has largely been a success (European Commission, 2018). This fascinating lack of critique deserves a dedicated study.

FIGURE 2: **Research projects under Horizon Europe**

RISING RESEARCH CASH

The European Union has steadily increased the value of its large framework reasearch programmes.



*In current €.

**Horizon europe budget yet to be finalized; assumes 27 member states after brexit.

Source: Nature 2019

EU'S SELF-IMPOSED OBSTACLE TO INNOVATION: CONSENSUS AND RADICAL INNOVATION ARE MUTUALLY EXCLUSIVE

Despite having ample financial capital, human capital, and national innovation systems, the EU is not aiming for disruptive innovation, including in the two major efforts towards digital sovereignty. In both cloud computing and chip-making, the EU will achieve the modest goals it has declared. But in the global technological race, Europe will, unfortunately, remain an also-ran. The very essence of the Union is the main obstacle to innovation. To understand why, let us start with why innovation always meets resistance.

Further challenges and options

Innovation, especially radical, is about uncertainty, risk, and facing active resistance. Radical innovation defies the current interests, norms, and order of things. Innovators face two classes of obstacles: passive and active.

To innovate is to threaten the current structure of power. Until the mid-nineteenth century in Europe, making such threats to the established order meant facing implicit resistance but also explicit threat of punishment.

Radical innovation must overcome numerous obstacles to succeed. After all, radical innovation is merely a vision that outsiders develop. Clearly, promises have not yet been realised: if they were, then it would not be an innovation.

Nowadays, disruptors no longer face institutionalised punishment. Still, innovation remains unpleasant for the challengers, for at least two reasons: all innovations face broad resistance, and nearly all innovations will fail.

In contrast, sustaining or incremental innovations offer improvements along previously established performance trajectories (Dombrowski & Gholz, 2009; Christensen, 2003). In other words, market leaders (think Kodak) will naturally resist disruptive innovations (digital photography, displayed rather than printed). This finding and the underlying reasons echo Kuhn: people trained within the prevalent paradigm will be largely unable and often not interested in exploring a radical diversion from the norm, let alone adopting it (Kuhn, 1962).

Scientific obstacles are tremendous but passive: metals, genes, or electrons do not actively resist. People and institutions do. Way before digital technology, Machiavelli warned about the dire consequences of innovation:

> There is nothing more difficult to plan, more doubtful of success, nor more dangerous to manage than a new system. For the initiator has the enmity of all who would profit by the preservation of the old institution and merely lukewarm defenders in those who gain by the new ones. (Machiavelli, 2010 [1550])

Human nature remains the same: people enjoying the benefits of the current order will resist the threat to their lifeline – even if others are certain that this would be a 'creative destruction' (Schumpeter, 1934). Innovation is exhaustingly hard, just as it was when Machiavelli wrote *Il Principe*.

The EU's political structure amplifies the predicament. The institutionalised consensus-based policy process structurally limits the EU's ability to take risky decisions. Rather than delving into the flourishing European studies scholarship, my argument is straightforward. Betting on a radical innovation will almost certainly result in failure. The promised thing will not work, will overrun costs and schedules, will fail to win over customers and compete with incumbents, and so on. A sovereign government usually places such bets only within the defence realm. A deliberation between numerous Member States will be unlikely to reach an agreement on such high risks. As with any negotiation, each party typically gets only some of what it wants. In political bargaining, the lower the level of commitment, the higher the likelihood of getting to a 'yes'. Consensus-building is a fundamental constraint to risk appetite. Moon shots, with their undeniable risks of resounding failure, are structurally opposed to consensus-building.

A simple example is the pattern in play in Europe in the realm of defence and strategic autonomy. Every state remains sovereign; Member States differ in interests and preferences, and compete within the EU. Smaller states may have outsized power in EU governance and repeatedly exercise it and exploit linkages in issues of 'low politics'. The process to craft a common policy across the 27 Member States, even if it demands a qualified majority rather than unanimity, is necessarily longer and more expensive than in more hierarchical governance. The notion that the need for unanimity structurally impedes the EU from taking on more ambitious military missions has long been present in the IR and political science literature (Howorth & Menon, 2009). Some scholars have been brave enough to argue that the European Union is unable to deliver the foreign and security policies expected due to

Acknowledging that the EU will never be able to spur breakthrough innovation, the decision to scale back the EU resources earmarked for it makes a lot of sense

decision-making procedures incapable of overcoming dissent (Toje, 2008).

This consensual style of governance will stay. The process is vital for the core political goal of the EU: preventing hostilities between Europeans through profound integration.

THREE POLICY RECOMMENDATIONS

Given that structural choice and its constraint to radical innovation, Europeans should acknowledge that the EU is the wrong vehicle for breakthrough innovation. I suggest three recommendations to the EU on the two major policies on digital sovereignty, cloud computing and chip-making.

Policy recommendation A: Continue both cloud computing and chip-making efforts

First, both large-scale initiatives are nearly impossible to cancel. Second, completing these can create some value for Europe. Some of the countries involved will benefit from increased public spending and commercial investments. The EU political institutions will present another self-serving accomplishment and use it to further cement the Brussels-based mechanisms. However, in geopolitical competition, both the commercial and the political achievements will fall short of the grandeur of official EU documents.

Policy recommendation B: Seize funding innovation through the EU

Accepting reality will spark disputes and debates, but eventually will lead to the adaptation of a more effective innovation policy for Europe. Stating that the EU is clearly the wrong vehicle for breakthrough innovation is understandably hard. It undermines much of the prior promises the EU institutions made. It certainly shakes the very foundations of the power of technocrats, experts, and public officials. Leaders of Member States may also prefer to continue shifting the blame to Brussels rather to have to make hard choices about risky long-term initiatives. Acknowledging that the EU will never be able to spur breakthrough innovation, the decision to scale back the vast EU resources earmarked for it makes a lot of sense. These billions could well be invested in numerous other ways to promote political, economic, and cultural integration.

Policy recommendation C: Focus EU funding on incremental innovation

Acknowledging that the EU will never be able to spur breakthrough innovation can lead to another rational decision: shift budgets to incremental innovation. With all due respect to the digital hype, the real economy is here to stay. Europe is home to a vast tapestry of strong and robust industries. Food, fashion, machinery, financial services, biomed, and so on – all could do well in the future. The EU should relinquish the grand visions that permeate its declarations and policies, and instead, dive deeper into more mundane challenges that concern competitiveness across the board in manufacturing, agriculture, and services. Such a strategy will help concentrate incremental innovation efforts on well-defined, narrow-focused areas.

The longer the gap between reality and aspiration lingers, the greater China's and the United States' advantage over Europe will grow. The EU will continue to disappoint itself until it acknowledges this structural issue.

NOTES

1. See, for example: European Council, 2016b; guidance on mixed datasets; European Commission, 2019b; European Commission, 2021a.
2. Research into how states enter new, high-technology markets demonstrates that peripheral agencies with few hard resources and little political prestige are more likely to spur radical innovation (Breznitz & Ornston, 2013). The argument is supported by a within-case analysis of Finland and Israel, two historically low-technology economies that successfully promoted rapid innovation-based growth. (Breznitz, Ornston, & Samford, 2018).
3. For the technologies that an iPhone combines, see Mazzucato, 2013.
4. The European Commission introduced the concept of the European added value (EAV) in 2014. EAV is 'the value resulting from an EU intervention which is additional to the value that would have been otherwise created by Member States alone' (SEC(2011) 867 final).

REFERENCES

Abbott, A.S.Q. (2019), 'How European Scientists will Spend €100 Billion'. *Nature,* 569(7757), 472–75.

Breton, T. (2021) 'Inside the Future: Europe's Plan to Thrive in the Global Microchip Race', 21 May, https://ec.europa.eu/commission/commissioners/2019-2024/breton/announcements/inside-future-europes-plan-thrive-global-microchip-race_en.

Breznitz, D., & Ornston, D. (2013), 'The Revolutionary Power of Peripheral Agencies: Explaining Radical Policy Innovation in Finland and Israel'. *Comparative Political Studies,* 46(10), 1219–45, https://doi.org/10.1177/0010414012472466.

Breznitz, D., Ornston, D., & Samford, S. (2018), 'Mission Critical: The Ends, Means, and Design of Innovation Agencies', *Industrial and Corporate Change*, 27(5), 883–96, https://doi.org/10.1093/icc/dty027.

Christensen, C.M.R.M.E. (2003). *The Innovator's Solution: Creating and Sustaining Successful Growth*. Boston: Harvard Business School Press.

Cory, N., & Dascoli, L. (2021) 'How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them', ITIF, July, https://itif.org/sites/default/files/2021-data-localization.pdf.

Dombrowski, P., & Gholz, E. (2009), 'Identifying Disruptive Innovation: Innovation Theory and the Defense Industry', *Innovations*, 4(2), 101–17.

The Economist (2022) 'When Will the Semiconductor Cycle Peak?', 29 January, https://www.economist.com/business/2022/01/29/when-will-the-semiconductor-cycle-peak.

Elysée (2017), 'President Macron Gives Speech on New Initiative for Europe', 26 September, https://www.elysee.fr/en/emmanuel-macron/2017/09/26/president-macron-gives-speech-on-new-initiative-for-europe.

European Commission (n.d.), 'The European Data Flow Monitoring', https://digital-strategy.ec.europa.eu/en/policies/european-data-flow-monitoring

European Commission (2018), 'A New Horizon for Europe: Impact Assessment of the 9th EU Framework Programme for Research and Innovation', Directorate General for Research and Innovation.

European Commission (2019a), 'Assessment of the Union Added Value and the Economic Impact of the EU Framework Programmes: Final Report', Directorate-General for Research and Innovation.

European Commission (2019b), 'Practical Guidance for Businesses on How to Process Mixed Datasets', 29 May, https://digital-strategy.ec.europa.eu/en/library/practical-guidance-businesses-how-process-mixed-datasets.

European Commission (2021a) 'Cloud Computing', https://digital-strategy.ec.europa.eu/en/policies/cloud-computing.

European Commission (2021b) 'Inside the Future: Eurpe's Plan to Thrive in the Global Microchip Race', 22 May, https://ec.europa.eu/commission/commissioners/2019-2024/breton/announcements/inside-future-europes-plan-thrive-global-microchip-race_en.

European Council (2016a) '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’, 27 April, https://eur-lex.europa.eu/legal-content/EN/AUTO/?uri=CELEX:02016R0679-20160504&qid=1532348683434.

European Council (2016b) 'Directive (EU) 2016/680 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 by Competent Authorities for the Purposes of the Prevention, Investigation, Detection or Prosecution of Criminal Offences or the Execution of Criminal Penalties, and on the Free Movement of Such Data, and Repealing Council Framework Decision 2008/977/JHA', 27 April, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2016.119.01.0089.01.ENG&toc=OJ%3AL%3A2016%3A119%3ATO.

GAIA (2021) 'GAIA-X Architecture Document', 21 December, https://gaia-x.eu/sites/default/files/2022-01/Gaia-X_Architecture_Document_2112.pdf.

GAIA (n.d.) 'FAQ', https://gaia-x.eu/faq.

GDPR.EU (n.d.) 'FAQ', https://gdpr.eu/faq.

Howorth, J., & Menon, A. (2009), 'Still Not Pushing Back: Why the European Union is Not Balancing the United States', *Journal of Conflict Resolution*, 53(5), 727–44.

Intel (2019) 'Intel Acquires Artificial Intelligence Chipmaker Habana Labs', Intel Newsroom, 16 December, https://newsroom.intel.com/news-releases/intel-ai-acquisition/#gs.5437jj.

Janakiram, M. S. V. (2019) 'How an Acquisition Made by Amazon in 2016 Became Company's Secret Sauce', *Forbes*, 10 March, https://www.forbes.com/sites/janakirammsv/2019/03/10/how-an-acquisition-made-by-amazon-in-2016-became-companys-secret-sauce.

Kuhn, T.S. (1962). *The Structure of Scientific Revolutions*. Chicago: University of Chicago Press.

Leiserson, C.E., Thompson, N.C., Emer, J.S., Kuszmaul, B.C., Lampson, B.W., Sanchez, D., & Schardl, T.B. (2020), 'There's Plenty of Room at the Top: What Will Drive Computer Performance after Moore's Law?', *Science*, 368(6495), eaam9744, https://doi.org/10.1126/science.aam9744.

Macron, Emmanuel (2022), Speech at the Closing Ceremony of the Confernece on the Future of Europe, https://presidence-francaise.consilium.europa.eu/en/news/speech-by-emmanuel-macron-at-the-closing-ceremony-of-the-conference-on-the-future-of-europe/.

Machiavelli, N. (2010 [1550]). *Il principe* [*The Prince*]. London : Penguin.

Mazzucato, M. (2013). *The Entrepreneurial State: Debunking Public Vs. Private Sector Myths*. London: Anthem Press.

Mazzucato, M. (2018), 'Mission-Oriented Research and Innovation in the European Union', European Commission, https://op.europa.eu/en/publication-detail/-/publication/5b2811d1-16be-11e8-9253-01aa75ed71a1/language-en.

Nature (2019), 'How European Scientists Will Spend €100 Billion', 29 May, https://www.nature.com/articles/d41586-019-01566-z.

Nellis, S. (2021) 'IBM Says Quantum Chip Could Beat Standard Chips in Two Years', *Reuters*, 15 November, https://www.reuters.com/technology/ibm-says-quantum-chip-could-beat-standard-chips-two-years-2021-11-15.

NVIDIA (2020) 'NVIDIA Completes Acquisition of Mellanox, Creating Major Force Driving Next-Gen Data Centers', 27 April, https://nvidianews.nvidia.com/news/nvidia-completes-acquisition-of-mellanox-creating-major-force-driving-next-gen-data-centers.

Romer, Paul M., 1990, Endogenous Technological Change, The Journal of Political Economy, Vol. 98, No. 5, Part 2: The Problem of Development: A Conference of the Institute for the Study of Free Enterprise Systems. (Oct., 1990), pp. S71–S102.

Scheer, S. & Rabinovitch, A. (2019) 'Intel Buys Israeli AI Startup Habana Labs for $2 Billion', *Reuters*, 16 December, https://www.reuters.com/article/us-habana-labs-m-a-intel-idCAKBN1YK1BU.

Schumpeter, J.A. (1934). *The Theory of Economic Development; An Inquiry into Profits, Capital, Credit, Interest, and the Business Cycle*. New York and London: Oxford University Press.

Service, R. F. (2018) 'Chipmakers Look Past Moore's Law, and Silicon', *Science*, 27 July, https://www.science.org/doi/10.1126/science.361.6400.321.
Toje, A. (2008), 'The Consensus—Expectations Gap: Explaining Europe's Ineffective Foreign Policy'. *Security Dialogue*, 39(1), 121–41, https://doi.org/10.1177/0967010607086826.
UNCTAD (UN Conference on Trade and Development) (2019), 'Digital Economy Report 2019', https://unctad.org/system/files/official-document/der2019_en.pdf.

The Normative Landscape in Security and Resilience: The Future of Critical Infrastructures and Essential Services in the EU

Martina Castiglioni and Alessandro Lazari[1]

https://doi.org/10.53121/ELFTPS3 • ISSN (print) 2791-3880 • ISSN (online) 2791-3899

ABSTRACT

Critical entities and essential services are experiencing a new normal in which their stability is being challenged by a blend of recurring disturbances and alternating crises. This situation calls for improved build adaptation plans to properly address and mitigate existing risks along with emerging ones such as hybrid threats and the escalating threat of climate change. This chapter analyses the EU security agenda's milestones and upcoming initiatives to answer to the question, *'Is the EU's Critical Infrastructure safe and secure?'* and providing recommendations to policymakers and security experts on key activities to maximise the results of future collaboration.

ABOUT THE AUTHORS

Alessandro Lazari is Senior Key Account Manager at F24 AG. He holds an MA in Law (University of Bologna) and PhD in Computer Engineering, Multimedia, and Telecommunications (University of Florence). Between 2010 and 2019, he worked at the European Commission's Joint Research Centre on policy support for the European Programme for Critical Infrastructure Protection (EPCIP).

Martina Castiglioni is Capacity Building Manager at Cyber 4.0 (Italy). She holds a BSc in International Relations (University of Padua) and an MSc in Security Policies (University Cattolica Milan).

INTRODUCTION

Today, society relies on a variety of critical public and private infrastructure and other essential services, which are presumed to be safe from all hazards. However, there are many factors that contribute to the instability of these infrastructure services thanks to the ever-changing environment in which these businesses operate and deliver their services. We do not only observe the edges blurring between the physical and digital domains of security but also the emergence of a multitude of new hazards and threats (e.g., pandemics, hybrid warfare, wars, lack of primary resources, and malicious mergers and acquisitions) whose magnitude and complexity are constantly a challenge and that very often decrease the general level of safety and security of critical infrastructure and essential services.

Modern security and resilience programmes cannot reach the goal of ensuring the stability of vital businesses without considering current and future challenges to be assessed and addressed in their adaptation plans. Failing to correctly and comprehensively adapt to current and upcoming issues may cause major disruptions (e.g., electricity, water, healthcare, and transport) because of the impossibility of dealing with the many negative events that may unfold and threaten the stability, continuity, and prompt recovery of vital businesses.

As this chapter aims to demonstrate, critical entities and essential services are experiencing a new normal in which their stability is being challenged by a blend of recurring disturbances and alternating crises. To better frame the context and future challenges, a high-level analysis of the pillars of the EU security agenda will be provided with the intention

of responding to the question: *'Is the EU's critical infrastructure safe and secure?'*. Finally, some policy recommendations will be provided as food for thought for policymakers and security experts.

TEMPORARY DISTURBANCE VS ENDURING CRISES: A NEW NORMAL FOR CRITICAL INFRASTRUCTURE?

The COVID-19 pandemic that began in late 2019, followed by the overlapping invasion of Ukraine – in early 2022 – has dragged critical infrastructure and essential services at the global, national, regional, and local levels into an enduring crisis that doesn't fit the definition of 'temporary disturbance' any longer. In the last three years, in fact, every business had to put in an unprecedented effort to adapt and respond to the pandemic, circumstances that implied the deep redesign of many policies, processes, and mitigation measures, including physical access to specific assets and buildings for operations and maintenance. Under these new circumstances, infrastructure and services have become even more exposed and vulnerable. This situation has brought intense stress in many dimensions, including the technological one, which has suffered many disruptions caused by the intensification of cyberattacks. Threat actors (e.g., state-sponsored hackers, cybercriminals, hacktivists) have exploited the uncertainty caused by the new normal to intensify their cyber operations.[2] This is highlighted by renowned reports and studies (e.g., the World Economic Forum's global risks report)[3] that confirm the proliferation of cyberattacks in the near future.

Between late 2021 and early 2022, when all businesses had finally reached a good level of maturity in handling the disturbances caused by the pandemic, and the pressure on them was decreasing thanks to the virus' partial regression, the tension around Ukraine followed by the sudden invasion have brought a new crisis that is leading to new impacts on critical infrastructure and essential services, reducing their overall safety and security.

Along with a new wave of sophisticated and targeted cyberattacks, critical infrastructure and essential services have had to deal with a newly mutated context characterised by severe disturbances of the supply chain in strategic sectors (mainly in energy) as a consequence of the sanctions, embargoes, and bans enforced by international, European, and national institutions against Russia.

The gas sector has been deeply affected by the Ukraine crisis, with the impact spreading throughout its entire business, operational lifecycle, and supply chain. In response, the European Commission has proposed accelerating the EU's readiness for any scenario by reaching 'independence from Russian gas well before the end of the decade' (European Commission, 2022). The fact that the EU currently imports 40 per cent of its total gas consumption from Russia has led to the call for measures aimed at the diversification of the supply chain together with additional actions to prepare for next winter (2022–23). A Communication from the Commission proposes that gas storage filling across the EU should start in March 2022 to have sufficient volume and to absorb future supply shocks. In parallel, transmission system operators have been asked 'to coordinate measures to optimise capacities available in the network in case of reduced or no flows and pressure from the East'. The prevision of potential retaliation in response to these protective measures, as anticipated, not only foresee supply shocks but also the recrudescence of targeted cyberattacks against the energy sector.[4]

Therefore, the energy sector is becoming, more than others, a geopolitical battlefield whose disruption could have a significant impact on citizens' lives.

Given the way recent events unfolded, it seems that the phases of 'peace time' and 'war time' in the lifecycle of critical infrastructure are undergoing a paradigm change in the way they occur. The impression is that they do not seem as distinct as in the past and that critical infrastructure is getting used to a more hybrid normality characterised by constant pressure on some dimensions (e.g., cybersecurity) together with more often recurring and increasing crises caused by economic, industrial, geopolitical, societal, and environmental factors (e.g., disruption of the supply chain, unavailability of human resources because of pandemics, severe weather events, and climate change).

The growing complexity of modern society means that the safety and security of essential services will likely face increasing challenges in the near future.

We may also predict that specific events and trends will have an impact on critical infrastructure. To name a few: the shift from surface-based to satellite-based communication services, the adoption of artificial intelligence, and hybrid threats.

Finally, climate change is also expected to have a broad impact on the lifecycle of critical infrastructure with consequences that may span from light-medium (non-lethal) issues to the partial or complete unavailability or annihilation of infrastructure and the services provided. At the same time, we

shouldn't underestimate the impact on the constellation of small and medium enterprises (SMEs) that are part of the operators' business and production lifecycle. Companies all along the supply chain have different resilience capabilities and some of them can be crippled if severely impacted, with limited possibility of bouncing back to an adequate level of service.

IS THE EU'S CRITICAL INFRASTRUCTURE SAFE AND SECURE?

Since the early years of the new millennium, the European Union has been steadily pushing forward the discussion about enhancing the protection of critical infrastructure. Between 2004 and 2016, in fact, the Union progressively deployed an unprecedented effort to design and enforce a 'shield' for critical infrastructure and essential services in the EU. This framework, which has started by focusing on the protection of critical infrastructure against terrorism (see European Commission, 2004), has progressively embraced protection from all hazards (the European Programme on Critical Infrastructure Protection and the Directive on European Critical Infrastructures) (see European Commission, 2006), followed by a full-fledged approach to dealing with network and information security (the NIS Directive; see European Council, 2016) in the context of operators of essential services.

Together with these milestones, mainly aimed at addressing the cyber/physical protection of critical infrastructure, the Seveso Directives also shouldn't be forgotten (see European Council, 2012), since they constitute the absolute reference in the field of health, safety, and environmental protection in establishments in which dangerous substances may be present (e.g., during processing or storage) in quantities exceeding certain thresholds.

Since the embryonic stages of the joint European journey on critical infrastructure, regulations, directives, and policies have pointed out the need to perform risk analyses in order to prioritise and mitigate risks, and this approach is still being endorsed.

In the last three decades, operators of critical infrastructure in the EU, thanks to the common normative and policy baseline, have drastically improved the way they initialise, manage, and maintain projects in the areas of health, safety, security (including cybersecurity), and the environment, which, as a result, has allowed companies to put in place permanent and graded measures to deal with potential issues that may arise (e.g. terrorism, cyberattacks, industrial accidents, and severe weather).

Companies all along the supply chain have different resilience capabilities and some of them can be crippled if severely impacted

Therefore, operators are constantly engaged in the protection and resilience of their businesses. However, the efforts in these areas are often finite and triggered by the need to comply with directives and regulations, risk-driven decisions, and the availability of budget and qualified human resources, circumstances that imply that adaptation strategies and tactics to deal with new risks and sudden changes of scenario may take quite some time to be properly formalised and implemented.

An adequate level of maturity in the execution and monitoring of security measures cannot be reached overnight; it implies a continuous improvement process. Risk-driven security plans, in particular, to have a good degree of accuracy, efficiency, and impact, need to have access to scenarios, statistics, redefinition of the criticalities of assets under different conditions, up-to-date risk methodologies, and proportionate and comprehensive frameworks of security controls to be implemented to mitigate emerging risks.

The hard work of the last 30 years has allowed critical infrastructure and essential services in the EU to reach an overall adequate level of safety and security. This is indeed true if we consider situations in which these businesses are operating in their comfort zones. As anticipated above, future scenarios can be expected to push European companies outside their comfort zones because of the need to respond to hybrid threats, shortage of supplies, and severe environmental modifications as a consequence of climate change. Given their magnitude and scale, these challenges will require efforts that cannot be sustained only by operators of critical infrastructure. While conventional threats and crises may be dealt with by the prompt activation of the latter and coordination with public

authorities, the response to emerging scenarios will require an unprecedented joint effort in which the public sector will have to play a major role at all levels. Dealing with increasingly complex geopolitical scenarios with the aim of assuring continuous access to vital supplies and technologies, gathering and sharing wide-scale intelligence, monitoring and coordinating to counter hybrid threats, as well as deepening the awareness and understanding of the local impact of climate change are areas in which European institutions, national governments, and authorities will have to be the first in line to ensure political cohesion, availability of budgets and resources, execution of joint tests and exercises, and timely and secure information-sharing. Silo approaches from the past will have to leave room for the establishment of a European shield that operates across all sectors of critical infrastructure and essential services with a holistic, participatory approach.

THE EU'S CONTINUOUS IMPROVEMENT LIFECYCLE IN THE PROTECTION AND RESILIENCE OF CRITICAL ENTITIES AND ESSENTIAL SERVICES

We may well remember 16 December 2020 as a key turning point in the EU's recent history in security, resilience, and cooperation. On this date, the Commission published two proposals for new directives. With the experiences of almost three decades behind it, the EU initiated a new policy cycle aimed at further improving security and resilience in both the physical and cyber domains of critical infrastructure and essential services. First, the Commission submitted a proposal to the European Parliament and the Council to repeal the NIS Directive and adopt an updated version (NIS 2.0) (European Commission, 2016b), with improvements, especially in cooperation. Second, it put forward a proposal for a directive on the resilience of critical entities that focused on physical security (European Commission, 2020), to replace that enforced by the ECI Directive of 2008 (European Council, 2008), now considered obsolete in respect of modern challenges. With this double proposal, the Commission sought to harmonise its actions and bring together the physical and cyber dimensions by dealing with them using coordinated, collaborative mechanisms and procedures. The EU's will to change is exemplified in the Member States' strong commitment to amending the NIS Directive, which was only promulgated in 2016.[5] This was achieved at remarkable speed, and the new directive is considered among

> The hard work of the last 30 years has allowed critical infrastructure and essential services in the EU to reach an overall adequate level of safety and security

the most impactful measures of the EU security agenda, since it has led to the following (Kaspersky, 2020):

- Established a basis for an increased common level of cyber resilience in Europe
- Created national strategies that have led to increased cooperation between Member States
- Increased awareness of the cybersecurity needs of organisations and critical infrastructure, to the effect that cybersecurity has become a political priority.

With the upcoming promulgation of NIS 2.0 and the critical entity resilience directives, expected in late 2022 or early 2023, the EU will have established a full-fledged, inclusive framework that will prepare the Member States to face the challenges of the years to come.

The work on the cyber and physical pillars will also pave the way for preparation for and response to hybrid threats, which is among the EU's priorities.[6]

POLICY RECOMMENDATIONS

The developments described in this chapter provide a high-level snapshot of the current state of European policies and practices. Consistent with its continuous improvement approach, since the embryonic stages of the security agenda, the EU has pursued incremental changes, allowing Member States adequate time to adopt and implement each improvement at their respective national levels. The joint actions have ensured a trusted environment in which each critical infrastructure stakeholder has been enabled to discuss important matters, share information, become more familiar with the security

and resilience efforts of other Member States and within other sectors, get access to best practices, and initiate bilateral or multilateral consultations as necessary.

The EU's security and resilience framework puts the Union and its Member States in a strong position to deter, prevent, reduce the consequences of, respond to, and recover from a broad array of threats to critical entities and essential services in the years to come. In this context, we offer three recommendations to serve as food for thought for policymakers and security experts alike.

Avoid the risk of over-regulation

Given the good overall maturity of the EU's framework in the areas of security and resilience, in the years to come, European institutions should reduce regulation efforts in favour of a more hands-on approach aimed at ensuring that every Member State reaches an adequate level of compliance and alignment with the Union's objectives. Over-regulating a field that now stands on a very solid and comprehensive baseline would prevent every involved stakeholder from focusing on the activities needed to produce results. In this crucial phase of the Union, the primary target should be maximising the outputs of the main nodes of the EU's security and resilience. These nodes include the network of CSIRTs, the NIS Cooperation Group (in charge of strategic cooperation and the exchange of information among Member States to develop trust and confidence) the European Cyber Crises Liaison Organisation Network (in charge of the coordinated management of large-scale cybersecurity incidents), and the Critical Entities Resilience Group (in charge of strategic cooperation and the exchange of information).

Consider the whole lifeline of critical infrastructure and essential services

Thinking about critical infrastructure and essential services very often brings to mind the picture of huge, widespread, and complex organisations relying on high numbers of people, establishments (e.g., offices, plants, storage, logistics, and production sites), and technologies (e.g., IT, OT, IoT, sensors, robotics, biometrics, video surveillance, etc.). This is indeed true for many of them. At the same time, recent projects – aimed at the identification and designation of operators of essential services under the national transpositions of the NIS Directive – have shown that Member States, regions, metropolitan cities, and communities rely on many SMEs. These companies, which fully belong to the lifeline of national security and resilience, often rely on smaller budgets and finite resources while dealing with the same issues faced by large organisations. This phenomenon is very often accompanied by the fact that companies that fly 'below the radar' are not properly involved in the consultation and exercises that could be pivotal for the development of their security and resilience programmes and for their inclusion in exchange networks. Since cyber-attacks disregard companies' size and will increase in the future, national governments and authorities cannot afford to leave anyone behind and they should take immediate measures to consider the whole national lifeline of critical infrastructure and essential services in their strategies, operations, capacity-building projects, and funding opportunities. A proper national security plan cannot reach the expected objectives if such features are missing, especially considering that many of these 'smaller' operators are also very often in charge of trans-boundary essential services that are vital for neighbouring countries as well.

Narrow down knowledge to enable prompt and effective decision-making in critical infrastructure and essential services

As anticipated, during the last 30 years, operators have been actively driven to put together strategies and programmes for the protection and resilience of their infrastructure and services. However, some modern threats cannot be properly addressed by them as phenomena like hybrid threats and climate change, among others, require the wider and deeper involvement of public authorities, agencies, academia, and research centres to enable decision-making. These entities should put together joint efforts to narrow down the expected scenarios triggered by newly emerging risks, to characterise with improved granularity how certain events could unfold in specific areas and regions. Such activity would allow the potentially impacted operators to perform gap analyses to evaluate whether running security and resilience plans need amendment to extend coverage to new events that they may face.

This practical approach would definitely help operators prioritise and select mitigation measures, well before this knowledge is consolidated in security frameworks and standards.

NOTES

1. Both authors are writing in a strictly personal capacity and the views expressed in this chapter should not be associated with any of their professional or academic affiliations.
2. For a full-fledged snapshot and analysis of the evolution of the phenomenon, see ENISA (2021).
3. The Global Risks Report series tracks global risks perception among risk experts and world leaders in business, government, and civil society. It examines risks across five categories: economic, environmental, geopolitical, societal, and technological. See WEF, 2022.
4. According to the experts of the European Council on Foreign Relations, energy infrastructure is highly vulnerable to cyberattacks and the EU should address this vulnerability as part of its defence against Russian aggression (Romero & Nelson, 2022).
5. On the contrary, the ECI Directive 114/08/EC has been in force for more than 14 years.
6. On the topic of hybrid threats in the EU, see European Commission, 2018; European Commission, 2016a.

REFERENCES

ENISA (European Union Agency for Cybersecurity) (2021), 'Threat Landscape 2021', 27 October, https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021.

European Commission (2004), 'Critical Infrastructure Protection in the Fight Against Terrorism', https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52004DC0702&from=EN.

European Commission (2006), 'A European Programme for Critical Infrastructure Protection', 12 December, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52006DC0786&from=EN.

European Commission (2016a), 'Increasing Resilience and Bolstering Capabilities to Address Hybrid Threats', 6 April, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52016JC0018.

European Commission (2016b), 'Proposal for a Directive of the European Parliament and of the Council on Measures for a High Common Level of Cybersecurity Across the Union', https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52020PC0823&from=EN.

European Commission (2018), 'Joint Framework on Countering Hybrid Threats', 13 June, https://eur-lex.europa.eu/legal-content/GA/TXT/?uri=CELEX:52018JC0016.

European Commission (2020), 'Proposal for a Directive of the European Parliament and of the Council on the Resilience of Critical Entities', 16 December, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52020PC0829&from=EN.

European Commission (2022), 'REPowerEU: Joint European Action for More Affordable, Secure and Sustainable Energy', 8 March, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52022DC0108&from=EN.

European Council (2008), 'Directive 2008/114/EC of 8 December 2008 on the Identification and Designation of European Critical Infrastructures and the Assessment of the Need to Improve Their Protection', 8 December, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32008L0114&from=en.

European Council (2012), 'Directive 2012/18/EU of the European Parliament and of the Council of 4 July 2012 on the Control of Major-Accident Hazards Involving Dangerous Substances', 4 July, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32012L0018&from=EN.

European Council (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', 6 July https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016L1148&from=EN.

Kaspersky (2020), 'Review of the NIS Directive: Key Takeaways', 21 September, https://www.kaspersky.com/about/policy-blog/general-cybersecurity/review-of-the-nis-directive.

Romero, A. & Nelson, J. (2022), 'Why Europe's Energy Industry is Vulnerable to Cyber-Attacks', European Council of Foreign Affair Relations, 7 March, https://ecfr.eu/article/why-europes-energy-industry-is-vulnerable-to-cyber-attacks.

WEF (World Economic Forum) (2022), 'Global Risks Report 2022', 11 January, https://www.weforum.org/reports/global-risks-report-2022.

The Security of Space Systems: A European Perspective

Marco Lisi

https://doi.org/10.53121/ELFTPS3 • ISSN (print) 2791-3880 • ISSN (online) 2791-3899

ABSTRACT

Space technologies, given their role in localisation and timing, remote sensing, and communications, are essential for the provision of worldwide digital services and the performance and survival of our critical infrastructures. Since they are closely integrated into the critical infrastructures of our society, space systems need to be protected against intentional and non-intentional attacks, in terms of confidentiality, availability, integrity, continuity, and quality of service. The convergence between defence and space has been among the most debated issues across the world and is central to the agenda of the European Commission. The war in Ukraine has confirmed that security concerns and provisions need to be extended to all space assets and that Europe must be strategically autonomous in terms of technologies and access to space. There is a widespread perception that space risks becoming the battleground of a future war, if it has not already done so.

ABOUT THE AUTHOR

Marco Lisi is a former special advisor to the European Space Agency and the European Commission. Following a 'summa cum laude' for his PhD in Engineering, he worked in the aerospace and telecommunications sectors, holding managerial positions in R&D, engineering, and programmes, both in industry and in institutional organisations. He is now an independent consultant and visiting professor. Lisi holds five international patents and has authored more than 200 technical papers.

INTRODUCTION

The present phase of the world's industrial and technological development is characterised by the convergence of space-based and ground-based infrastructure, all driven by three main technological trends: ubiquitous localisation and timing, ubiquitous sensing, and ubiquitous connectivity.

Given their role in localisation and timing, remote sensing, and communications, space technologies are essential for the provision of worldwide digital services. For example, the pervasive connectivity required by the Internet of Things (IoT), despite the wide diffusion of broadband wireless networks (5G and, soon, 6G), can never be fully achieved without the support of satellite mobile communications. A seamless integration of space and ground systems is required: satellite communications, in particular, need to be fully interoperable with terrestrial networks.

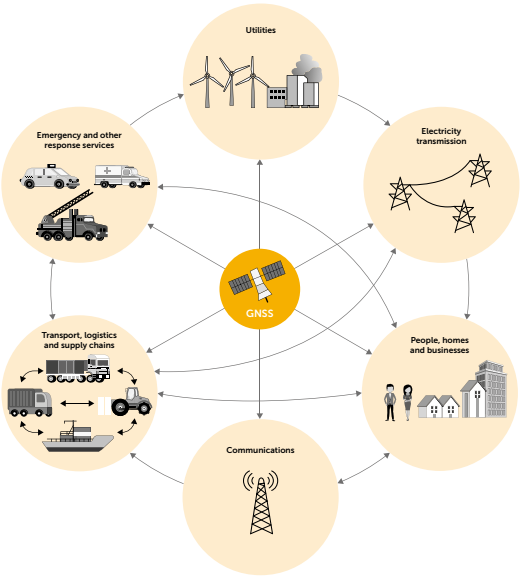
The value-added applications made possible by integrating satellites in the 5G network architecture range from assets management (car maintenance, fleet management, container tracking, tracking of consumer devices), to high-speed platforms (cars, trains, aeroplanes, unmanned aerial vehicles), and highly reliable and secure communications (industry automation, eHealth, remote control, facility management).

The traditional weaknesses of satellite communications – cost and latency – are being brought down on the one hand by the introduction of very High Throughput Satellites and on the other by non-geostationary such as Low Earth Orbit (LEO) or Medium Earth orbit (MEO) constellations.

Global Navigation Satellite Systems (GNSSs), such as GPS, GLONASS, Galileo, and Beidou, together constitute a potentially interoperable infrastructure,

FIGURE 1: **The European Space Agency's European Space Security and Education Centre at Redu, Belgium. This is the European centre of excellence for space security services**

FIGURE 2: **GNSS critical dependencies**



providing vital support to most industrial and economic aspects of our society (Figure 2).

GNSSs are nowadays considered a worldwide utility, tightly interconnected with all other critical infrastructure, from electric power distribution systems to air traffic management systems, and from railways to water and oil piping networks.

In the perception of the average user, the main contribution of GNSSs, their true 'raison d'être', is in providing one's accurate position and allowing reliable navigation, be it by car, aeroplane, train, or boat. Precise timing is understood as at most an enabling feature of GNSSs and a very useful by-product, but only after positioning and navigation. The reality, as shown by studies performed in the United States and Europe, is that timing is the most strategic and essential service offered by GNSSs, and the one that affects all critical infrastructure of our society the most. The main sectors relying on GNSSs for timing are communications (e.g., Internet, cellular, and satellite networks), energy, financial services, and transportation systems. In the least obvious of these, financial services, transactions are time-stamped using atomic clocks, but GNSS is used as a secondary timing source and for synchronisation.

In the realm of remote sensing, Earth Observation (EO) satellites provide continuous and ever-more detailed monitoring of our environment with passive (optical cameras, radiometers) and active (Synthetic Aperture Radars) sensors. These data will be soon integrated with real-time data collected by billions of 'in situ' ground sensors, the miniaturised integrated circuits of the IoT. The IoT envisions many billions of Internet-connected objects or 'things' that can sense, communicate, compute, and potentially actuate, as well as have intelligence, multimodal interfaces, physical/virtual identities, and attributes. The integration and fusion of remote sensing data, georeferenced by GNSS, exchanged via global communication networks, and eventually processed in large computing facilities, power most, if not all, industrial applications and welfare services.

The convergence of space-based and ground-based systems and how space assets are vital for the performance and survival of our critical infrastructure is thus evident.

Space systems, being highly integrated into the critical infrastructure of our society, need to be guaranteed and protected against intentional and non-intentional attacks, in terms of confidentiality, availability, integrity, continuity, and quality of service. Moreover, the convergence between defence and space is among the most debated issues around the world. This issue is a prominent part of the agenda of European Commissioner Thierry Breton of France, who is responsible for the Directorate General for the Defense and Space Industry of the European Commission.

Increasing importance will be given to security aspects of all space systems, both for their potential strategic value and for the essential role they play in guaranteeing the survival of critical infrastructure, in the case of intentional and unintentional

FIGURE 3: **The European Union Space programme**

threats of any kind. The commonly shared perception is that space risks becoming the battleground of a future war, if it has not already become one.

SPACE SECURITY AND EU STRATEGIC AUTONOMY

A good understanding of the present European Union plan to achieve strategic autonomy in space can be gained from the pillars of the European space programme, being pursued by the European Commission through the European Union Space Programme Agency (EUSPA) (Figure 3):

- Galileo global positioning, navigation, and time reference system: This system is the backbone of all critical infrastructure, and also provides an encrypted signal resistant to jamming and spoofing to governmental and security/safety-related services, such as the Search and Rescue service and the Public Regulated Service (PRS). At the European regional level, Galileo is complemented by the European Geostationary Navigation Overlay Service, a satellite-based augmentation system used to improve the performance of Galileo and GPS.
- Copernicus integrated EO 'system-of-systems': This will play an important role in environmental monitoring (climatic changes, pollution), management of emergencies (natural disasters such as earthquakes, wildfires, and floods), and border/coastal surveillance. Copernicus consists of a complex set of systems that collect data from multiple sources: EO satellites, in situ sensors such as ground stations, and airborne and sea-borne sensors.
- European satellite telecommunication system for governmental use (GOVSATCOM): part of the more ambitious Secure Connectivity Initiative, GOVSATCOM will provide assured, secure, cost-efficient communication capabilities for security and safety-critical missions and operations, adopting quantum technologies for encryption. The GOVSATCOM system will also pay special attention to providing connectivity to the Arctic region, whose strategic importance is growing.
- Space Situational Awareness (SSA): A system for the surveillance of objects in orbit, SSA also monitors the peaceful use of outer space, as required by international treaties (UN, 1967).

It is evident that the strategic objective pursued by the EU in developing its space programme has resulted in the need to strengthen the security and resilience of its space-based and ground-based assets against cyber and physical attacks.

EUROPEAN SPACE INFRASTRUCTURE: THE PRESENT SCENARIO

The world's critical infrastructures rely to a large extent on space systems (i.e., assets existing in sub-orbital or outer space), including their ground control systems and launch facilities. Satellites are an important delivery platform for information society services. They are often key elements of an information and communication technology system architecture, both as sensors and as components of the telecommunications network architecture.

Satellite security has been in the past erroneously limited to encryption and anti-jamming technologies. In reality, satellites are part of hybrid systems, which incorporate both space and terrestrial components; their ground segments are therefore exposed to the same types of threats (viruses, worms, Trojan horses, denial-of-service attacks, exploited vulnerabilities, etc.) typically experienced by terrestrial information systems. Space systems vulnerabilities can be exploited by focusing attacks on any one of the three segments that make up the space capability (Figure 4):

- Space segment: the satellite or satellite constellation, including payloads

FIGURE 4: **Space, ground, and user segments of a satellite system**

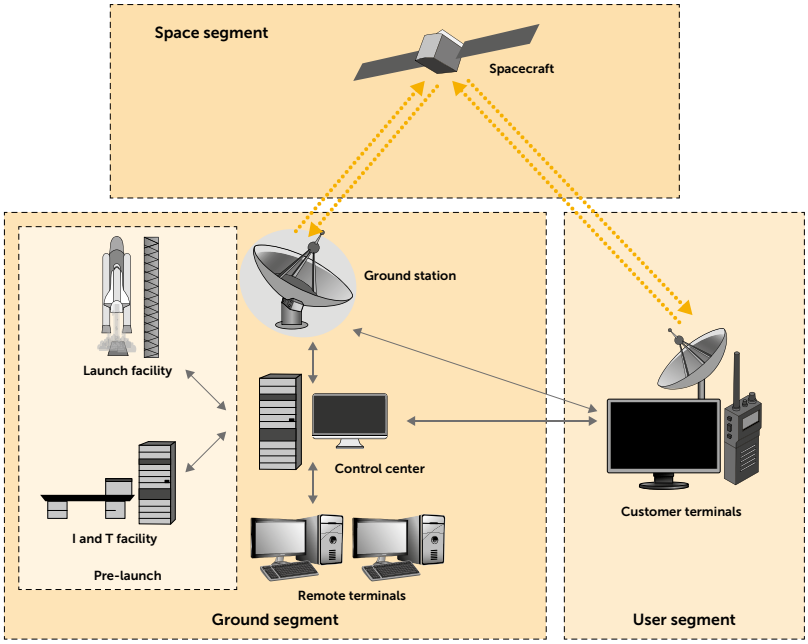


TABLE 1: **Unintentional threats to satellite systems**

Types of threat	Vulnerable satellite system components
Ground-based:	
Natural occurrences (including earthquakes and floods; adverse temperature environments) power outages	Ground stations: TT&C and data links
Space-based:	
Space environment (solar, cosmic radiation; temperature variations) Space objects (including debris)	Satellites; TT&C and data links
Interference-oriented:	
Solar activity; atmospheric and solar disturbances Unintentional human interference (caused by terrestrial and space-based wireless systems)	Satellites; TT&C and data links

Source: DOD and GAO analysis.

- Ground segment: all the hardware and software facilities that allow the space assets to be successfully controlled and operated, from launch to disposal. Typical elements of a ground segment are control centres (mission control centre and dedicated operational centres) and ground station networks
- User segment: corporate and individual users, including their equipment and software applications

Moreover, space systems, such as satellites and their control segments, typically adopt sophisticated technologies for their communications, radiation hardening, and computing requirements.

The growing concern of governments and space companies about the risk of cybernetic attacks on their terrestrial and in-orbit infrastructures is well known and evidenced. But other threats loom over space and its peaceful use, as shown in tables 1 and 2.

In addition to cyberattacks, which are mainly directed against ground segment infrastructure (control centres, control ground stations, launch facilities), a number of physical threats are nowadays

TABLE 2: **Intentional threats to satellite systems**

Types of threat	Vulnerable satellite system components
Ground-based:	
Physical destruction	Ground stations: Communications networks
Sabotage	All systems
Space-based (anti-satellite):	
Interceptors (space mines and space-to-space missiles)	Satellites
Directed-energy weapons (laser energy, electromagnetic pulse)	Satellites; TT&C and data links
Interference and content-oriented:	
Cyber attacks (malicious software, denial of service, spoofing, data interception, and so forth)	All systems and communications networks
Jamming	All systems

Source: GAO analysis.

possible, from kinetic energy anti-satellite weapons to direct-energy weapons and radiofrequency jamming.

A kinetic anti-satellite weapon can be a missile launched from earth into space until it intercepts a satellite already in orbit and destroys it by impact, or it can be a 'killer' satellite that is put into orbit and remains there waiting to be used by modifying its orbit. In both cases, a 'kinetic energy' attack, based on physical impact with a target satellite causing its destruction, is also followed by the inevitable consequence of the production of debris, which continues to remain in orbit, increasing the already worrying quantity of space debris around earth.

Direct-energy weapons are usually directed against assets in orbit and can be realised as high-energy laser or radiofrequency beams generated on the ground, able to 'blind' satellites and damage their electronic equipment. Very damaging 'flashes' of radiofrequency energy can also be generated by exploding small nuclear bombs in the ionosphere (Electro-Magnetic Pulse or EMP).

The vulnerabilities of GNSSs such as Galileo are worth examining separately. The vulnerabilities of these systems are essentially of three types: 'jamming', 'spoofing', and cyberattacks. Jamming means interference, intentional or unintentional, that can overwhelm the GNSS signals and prevent proper reception. Possible causes of such disruption can be man-made but unintentional, such as overpowering radio emissions in nearby bands, or natural, such as space weather events (e.g., solar flare eruptions).

GNSS signals are particularly vulnerable to jamming as they are extremely weak, both because they are transmitted by satellites travelling at an altitude of about 20,000 kilometres, and due to regulatory limitations. Jamming, both in the military and civilian fields, is the simplest, cheapest, and at the same time most effective means of preventing the use of GNSS systems in limited geographical areas (from a few square kilometres to entire regions). Due to the proliferation of commercially available jamming equipment, it is also relatively inexpensive yet very sophisticated (Figure 5).

Spoofing is a more sophisticated and slightly more difficult form of attacking the functionality of GNSS systems (and certainly an intentional and malicious one). The threat is based on the possibility of generating, through relatively inexpensive and technologically simple equipment, fake replicas of GNSS signals. In this way, it is possible to provide the attacked user or infrastructure inaccurate information about both location and time, so as, for example, to divert a plane or a ship from their course. The countermeasure adopted in

FIGURE 5: **Commercially available GNSS jamming equipment**

military and government applications is to encrypt the codes of GNSS signals, making it impossible to falsify them. In the civil field, it is worth highlighting the European Commission initiative to introduce civil signal authentication in the Galileo system, the so-called Open Service Authentication (OS-NMA).

The third area of vulnerability, cyberattacks, derives from the technology of the terrestrial segment of GNSS systems, typically based on very complex software programmes, data processing centres, and data communication lines. The possibility of internal and external cyberattacks is, as with all large IT architecture of this type, very high.

For all the security threats discussed so far, proper mitigation strategies and specific countermeasures can be put in place, as summarised in Table 3.

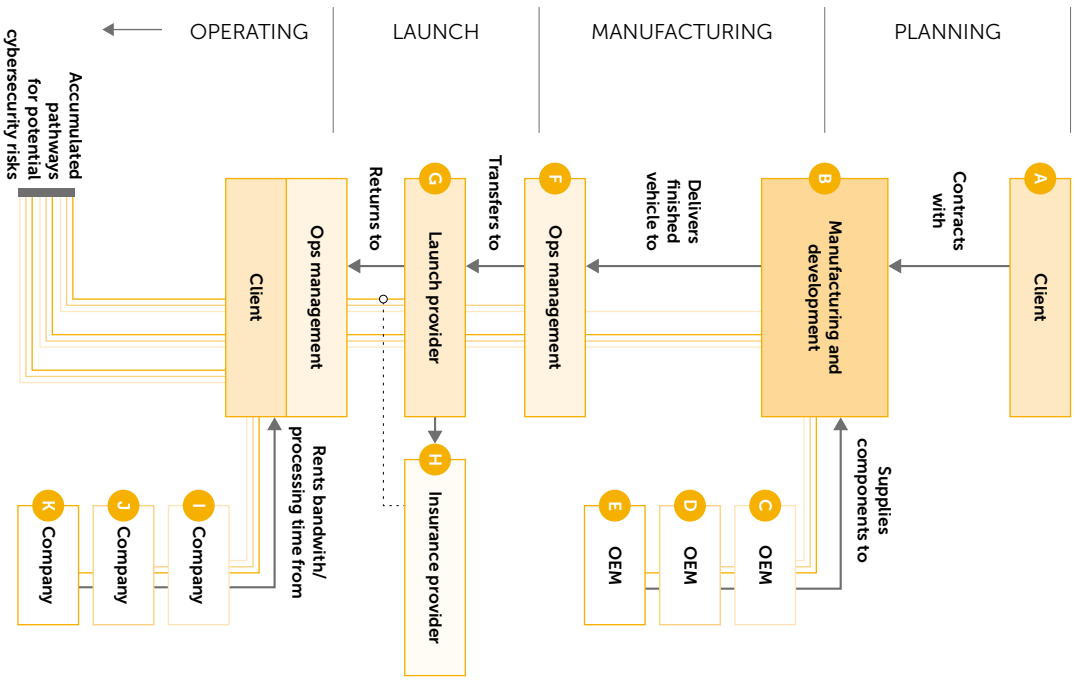
Finally, an often underestimated vulnerability deserves mention: the supply chain. The complexity of the supply chain required to create these systems makes them attractive to hackers (Figure 6).

Most satellite systems require multiple manufacturers with various specialities to develop all the components to be eventually integrated by a system integrator. Each such vendor provides an access point for an attacker into a satellite production line. Each additional vendor provides an additional opportunity to compromise a satellite, either by injecting malicious software or by introducing malicious hardware (hardware Trojans). For these highly complicated supply chains and production organisations, one might assume that stringent security protocols are in place, but this is seldom true, especially in commercial industries.

Despite the many potential threats described, for many years security standards for space assets, especially commercial ones, have not been regulated by any institutional body. Until recently, there were no national or international agencies restricting the use of satellites and monitoring their actual usage, except for the UN Office for Outer Space Affairs (UNOOSA), which has a mandate of protecting space from military uses, and the International Telecommunications Union (ITU), which mostly coordinates satellites' orbits and radiofrequency spectrum utilisation in order to avoid interference.

The lack of security regulations implies that satellites lack common cybersecurity standards and might be used for cyberattacks with impunity and anonymity unless commercial companies and government agencies take steps to secure these systems.

FIGURE 6: **Pathways for potential security attacks in a satellite life cycle**



This situation is becoming even more serious due to the proliferation of low-cost, very small satellites (1 to 20 kg) using commercial off-the-shelf technology. These micro- or pico-satellites, called 'CubeSats', can be developed and put into orbit at very affordable costs (a few hundred thousand euros) and are therefore very attractive to small entrepreneurs, research institutions, and academies. The negative side of the coin is that security controls and standards for this class of satellites are practically non-existent. The risk then would be that they can be hacked by malicious actors, to be used as weapons against larger and more vital assets in space.

In Europe, there are four classes of space asset organisations, i.e., organisations that build, operate, maintain, or own space systems:

1. Commercial operators, offering B2B and B2C services after procuring satellites from European and non-European satellite manufacturers (e.g., Eutelsat, SES Astra, Inmarsat). Security requirements apply to them to some extent, but without their having to comply with standards or official certification processes.

2. National space agencies (e.g., CNES in France, DLR in Germany, ASI in Italy), promoting and funding satellite programmes mostly for military, governmental, or 'dual-use' applications (telecommunications, EO, spectrum monitoring, intelligence). These agencies apply security standards and certification or accreditation processes in cooperation with their national security agencies.

3. The European Space Agency (ESA), an intergovernmental organisation including 22 Member States, not all belonging to the EU (e.g., the UK). The ESA's objectives are:

- **a**. to promote, for exclusively peaceful purposes, space research and technology, and their applications;
- **b**. to manage specific satellite missions carried on by European space industries;
- **c**. to support satellite operations through its ground control infrastructure, including a network of monitoring ground stations;
- **d**. to guarantee European countries access to space, maintaining a major spaceport, the Guiana Space Centre at Kourou, French Guiana, operating the fleet of European launch vehicles in cooperation with Arianespace (Ariane, Vega), and developing new launch capabilities;
- **e**. to support at technical and procurement levels the space programmes developed by the European Commission;
- **f**. to promote cooperation with agencies and institutional organisations at the national and international levels (e.g., with NASA on the International Space Station or ISS).

> The world's critical infrastructures rely to a large extent on space systems (i.e., assets existing in suborbital or outer space), including their ground control systems and launch facilities

As far as security is concerned, the ESA has recently been developing a coordinated European approach to space security, mainly in cooperation with the European Commission and EUSPA.

4. The EUSPA, which is responsible for the development and operation of the EU common space infrastructure. In addition, through the funding of the Horizon programme, EUSPA promotes commercial downstream applications based on its systems, such as Galileo or Copernicus. EUSPA is also responsible for the security certification and accreditation of its space assets, in cooperation with the ESA and the national security agencies of the EU Member States.

EUROPEAN SPACE SECURITY INITIATIVES AT THE INSTITUTIONAL LEVEL

The only two European initiatives in space security at the institutional level are from the ESA and EUSPA. The ESA is creating a new centre for cybersecurity that will safeguard all agency systems against outside interference, extending from ESA ground infrastructure around the globe to satellites in orbit. Beginning operations in 2024, the ESA's new Cyber-Security Operations Centre (C-SOC) will provide agency-wide cyber-monitoring and management capability under the technical responsibility of the ESA's Security Office. The C-SOC represents

a unique capability in Europe, reinforcing the ESA's preventative-reactive security measures.

Operating on a distributed architecture basis, the C-SOC will be able to provide resilient and redundant security coverage to the entire ESA infrastructure, monitoring and managing its vulnerabilities 24 hours a day and 365 days a year. Its capabilities will also be available to ESA Member States and international partners. C-SOC will have nodes and interconnections distributed across all main ESA sites, and to allow widespread coverage across European territory, mobile C-SOC stations (Cyber Portable Operational Platforms) will be deployed as needed, in principle extending protection to partners involved in ESA missions.

The centre is being established in parallel with other cybersecurity measures, including the Security Centre of Excellence, the sites working together to complement the capabilities of the ESA's state-of-the-art Computer and Communications Emergency Response Team.

The space security activities of the EUSPA and European Commission are performed mainly by the Security Accreditation Board (SAB). The SAB is the security accreditation authority for all the EU space programme's components and is completely independent in its decision-making. The SAB is composed of a representative of each Member State, a representative from the Commission and a representative from the High Representative for the Union for Foreign Affairs and Security Policy. Where appropriate, representatives of ESA and the agency not involved in security accreditation may be invited to attend SAB meetings as observers. On an exceptional basis, representatives of other EU institutions, third countries, or international organisations may also be invited as observers. The chairperson of the SAB is responsible for representing the EUSPA on security accreditation matters. The SAB ensures that systems comply with the relevant security requirements and provides statements of approval for systems and services to operate.

The SAB makes its decisions based on local evaluations by the competent national security accreditation authorities, verification by EUSPA's Security Accreditation Department, and the recommendations of its technical subordinate panel and bodies. These decisions include:

- Defining and Approving security accreditation strategies
- Approving satellites launches
- Authorising the operation of systems in different configurations and the various services they provide
- Authorising the operation of ground stations
- Authorising bodies to develop or manufacture sensitive PRS technologies, PRS receivers, or PRS security modules
- Endorsing the selection of approved products
- Approving interconnections between systems

To reduce the vulnerabilities of critical infrastructure, the European Commission has launched the European Programme for Critical Infrastructure Protection. The European Joint Research Centre (JRC) provides technical support and carries out different research activities, including detection and mitigation of radio frequency threats that could jam or spoof GPS and Galileo, as well as unintentional interference from space weather events, such as solar storms. JRC is also testing a broad range of commercial GNSS timing receivers to assess their resilience to various types of interference scenarios.

THE WAR IN UKRAINE AND ITS CONSEQUENCES

The war in Ukraine is proof that security concerns have to be extended to all space assets, as cyberattacks, often combined with physical ones, target all digital infrastructure, on the ground and in space, well knowing their interdependencies. It has also demonstrated the importance and vulnerability of space infrastructure and the urgent need to provide for their defence in a broader framework, which obviously includes all critical European infrastructure.

In the early days of the war, distributed denial-of-service attacks tried to degrade Ukrainian internet access and communications. The Ukrainian government asked Elon Musk to provide the country with ground stations of his Starlink satellite communications systems. Incidentally, this request was criticised by the Russian government as violating the official neutrality of the United States on the basis of the United Nations Outer Space Treaty, which forbids the use of space assets in war conflicts and places international responsibility and requirements for authorisation and continued supervision of non-governmental space activities (such as those of Musk's Spacelink) on the state. Almost in response, cyberattacks disrupted worldwide user terminals of the satellite internet and TV provider Viasat. Viasat operates as a defence contractor for the US government in addition to selling retail services; the

FIGURE 7: **Jamming of GPS signals detected by the Hawkeye 360 satellite in Ukraine**

company also worked with the Ukrainian military and police.

As far as satellite positioning systems are concerned, European aviation authorities reported a sudden increase in interference with GPS signals in places as far away as Finland, the Mediterranean, and Iraq since Russia invaded Ukraine, forcing aircraft to reroute or change their destination (Figure 7).

The indirect consequences of the war were also very serious, such as Russia's decision to stop cooperation in space programmes with Western nations, including the ISS and the launches of European satellites with Russian launchers. The suspension of Soyuz launches from the European launch base in French Guiana, with the return of Russian engineers and technicians who supported those launches, could have serious consequences for the European space programme, for example by delaying the originally planned launch of the two Galileo satellites at the end of 2022.

The lesson we should learn from the war in Europe is that security provisions need to be extended to all space assets and that it is strategically important for Europe to be autonomous in terms of technologies and access to space. It is equally evident that the convergence between defence and space must be approached with a sense of realism.

CONCLUSIONS AND RECOMMENDATIONS

Space security has grown from a governmental or military problem to an issue affecting all critical infrastructure, down to individual users. From a network-centric perspective, satellite systems need to incorporate standardised and certifiable approaches to physical and cybersecurity. Until recently, however, space security has been perceived as a customised add-on, leading to a variety of security requirements and a number of proprietary solutions adopted by space agencies and industries, often on a goodwill basis.

The first important recommendation, therefore, is to take a holistic view of security, recognising that space assets are an integral and vital part of our society. In Europe, the ESA and EUSPA must continue in their coordinated effort to establish a common European approach to space security, adopting existing standards and good practices wherever available, but developing ad hoc new standards for space systems where needed.

The objective of institutional organisations must also be to foster a security culture in the industrial and research sectors, looking at security as an integral part of systems engineering. European policymakers should recognise the strategic importance of autonomy in certain technological areas, such as space components and integrated circuits: Europe is much too dependent on foreign countries and the security risks deriving from this situation are unacceptably high.

Finally, as far as the European GNSS, Galileo, is concerned, Europe has to broaden its view and recognise the need for more robust and resilient Positioning, Navigation, and Timing (PNT) infrastructure. The interoperability of Galileo with other GNSS (GPS and, to some extent, GLONASS and Beidou) in a multi-constellation scenario has already proved to be a safeguard against massive outages of one constellation. However, Europe also must work towards a PNT system-of-systems, including GNSS and non-GNSS (e.g., eLoran) infrastructure. At the user level, a fusion of data from different systems and platforms will guarantee a high degree of availability and continuity.

The integrity of time and position data will be more easily assessed by the user themselves, comparing different sources and spotting discrepancies. Jamming and spoofing will be more difficult to pull off and easier to detect, as the user will no longer be reliant on a single source of information.

The development of non-GNSS solutions and of complementary autonomous platforms and technologies will be a step towards a resilient, more versatile PNT infrastructure, able to fix, to a large extent, all present limitations and vulnerabilities. European governments should seriously consider this possibility.

REFERENCES

Manulis, M., Bridges, C. P., Harrison, R., Sekar, V., & Davis, A. (2021), 'Cyber Security in New Space'. *International Journal of Information Security*, 20, 287–311. https://doi.org/10.1007/s10207-020-00503-w.

Al-Kusayer, T. A. (1992), 'The Susceptibility of Communication Satellites to the Nuclear Electromagnetic Pulse'. *Journal of King Saud University – Engineering Sciences*, 4(2), 229–37.

Eutelsat Communications (2013). 'Satellite Interference: An Operator's Perspective', ITU presentation, 10 June, https://www.itu.int/en/ITU-R/space/workshops/2013-interference-geneva/Pages/workshopPresentations.aspx.

Falco, G. (2018), 'The Vacuum of Space Cybersecurity', AIAA Space Forum, 17–19 September, https://doi.org/10.2514/6.2018-5275.

Nightingale, E., Lal, B., Weeden, B., Picard, A., & A. Eisenstadt (2016), 'Evaluating Options for Civil Space Situational Awareness (SSA)', IDA Paper NS P-8038, August, https://www.ida.org/-/media/feature/publications/e/ev/evaluating-options-for-civil-space-situational-awareness-ssa/p-8038.ashx.

Chow, B. (2017), 'Stalkers in Space: Defeating the Threat'. *Strategic Studies Quarterly*, Summer, 82–116, https://www.airuniversity.af.edu/Portals/10/SSQ/documents/Volume-11_Issue-2/Chow.pdf.

Gleason, M., & Hays, P. (2020), 'A Roadmap for Assessing Space Weapons', Center for Space Policy and Strategy, October, https://aerospace.org/sites/default/files/2020-10/Gleason-Hays_SpaceWeapons_20201005_1.pdf.

Rajagopalan, R. (2010), 'Electronic and Cyber Warfare in Outer Space', UNIDIR Space Dossier, May, https://unidir.org/publication/electronic-and-cyber-warfare-outer-space.

Livingstone, D., & Lewis, P. (2016), 'Space, the Final Frontier for Cybersecurity?', Chatham House, the Royal Institute of International Affairs, September, https://www.chathamhouse.org/2016/09/space-final-frontier-cybersecurity.

European Space Policy Institute (2018), 'Security in Outer Space: Rising Stakes for Europe', Report 64, August, https://espi.or.at/publications/espi-public-reports/send/2-public-espi-reports/371-security-in-outer-space-rising-stakes-for-europe.

Harrison, T., Johnson, K., & Roberts, T. (2019), 'Space Threat Assessment 2019', CSIS Aerospace Security Project, April, https://www.csis.org/analysis/space-threat-assessment-2019.

Cristini, F. (2010), 'Satellite Networks: Solutions Against Emerging Space Threats'. *IFAC Proceedings Volumes*, 43(15), 380–85, https://doi.org/10.3182/20100906-5-JP-2022.00065.

Holmes, M. (2019), 'The Growing Risk of a Major Satellite Cyber Attack', *Via Satellite*, November, https://interactive.satellitetoday.com/the-growing-risk-of-a-major-satellite-cyber-attack.

Jasani B. (2016), 'Space Assets and Emerging Threats', Department of War Studies King's College London, Presentation to UNOOSA, September, http://www.unoosa.org/pdf/SLW2016/Panel2/1_Jasani_-_Space_assets_and_threats_06082016.pdf.

U.S. Defense Intelligence Agency (2019), 'Challenges to Security in Space', Report, https://www.dia.mil/Portals/110/Images/News/Military_Powers_Publications/Space_Threat_V14_020119_sm.pdf.

United States General Accounting Office (2002), 'Critical Infrastructure Protection: Commercial Satellite Security Should Be More Fully Addressed', Study Report, August, https://www.gao.gov/products/gao-02-781.

De Faakto (2019), 'Attacking Military & Civilian Satellite Systems: An Open Source Intelligence Study', September, https://defaakto.com/2019/09/14/attacking-military-civilian-satellite-systems-an-open-source-intelligence-study.

Papadimitriou, A., Adriaensen, M., Antoni, N., & Giannopapa, C. (2019), 'Perspective on Space and Security Policy, Programmes and Governance in Europe'. *Acta Astronautica*, 161 (August), 183–91, https://doi.org/10.1016/j.actaastro.2019.05.015.

Lisi, M. (2007), 'Security Certification of Complex, "Network Centric" Satellite Systems', AIAA-2007-3192, Proceedings of the 25th AIAA International Communications Satellite Systems Conference, Seoul, Korea, 10–13 April, https://doi.org/10.2514/6.2007-3215.

Lisi, M. (2007), 'Security Aspects of the Galileo Satellite Navigation System', Atti dell'Istituto Italiano di Navigazione, no. 186, June.

Lisi, M. (2007), 'Security Certification of Dual Use Satellite Systems', Proceedings of the 13th Ka and Broadband Communications Conference 2007, Torino, September.

United Nation (1967), Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies, RES 2222 (XXI).

The Unchecked Proliferation of Offensive Cyber Capabilities (OCC): A Dangerous New Reality?

Arthur de Liedekerke and Maarten Toelen[1]

https://doi.org/10.53121/ELFTPS3 • ISSN (print) 2791-3880 • ISSN (online) 2791-3899

ABSTRACT

While the Pegasus saga is a damning and evident indictment of the international community's inability to effectively regulate the proliferation of offensive cyber capabilities, it is by no means a standalone incident. The current laissez-faire regulatory approach to OCC proliferation has left a dangerous grey zone from which unscrupulous actors are only too keen to benefit. Given the destructive potential and easy diffusion of OCC – as well as the possible impact on people's security and the prosperity of economies worldwide – it is reasonable to search for ways to limit its reach and (ab)use by unscrupulous actors. This chapter puts forward recommendations for policymakers and security experts alike.

ABOUT THE AUTHORS

Arthur de Liedekerke is a project manager and advisor at Rasmussen Global and a non-resident fellow at the Institute for Security Policy at Kiel University. He holds MAs in International Relations from the University of Maastricht and Geopolitics from King's College London.

Maarten Toelen is a strategy consultant with experience in the Cyber and Hybrid Working Parties of the Council of the EU. He holds an LLM in European Law from Leiden University, MAs in EU External Relations and Security Policy from the Vrije Universiteit Brussel and International Security and Contemporary War from King's College London.

PEGASUS: JUST ANOTHER EXAMPLE OF THE SYSTEMIC PROBLEM OF OCC PROLIFERATION

Much ink has already been spilt on the weaponisation of cyberspace – and how international (humanitarian) law should evolve in response. Recent incidents, such as the SolarWinds campaign or the ransomware attack on Colonial Pipeline, have yet again illustrated the far-reaching impact that malicious cyber operations can have on private organisations and individuals alike (Kaspersky, 2021).

One incident, however, should have set far more alarm bells ringing than it did: Pegasus. In the summer of 2021, an international collective of investigative journalists publicly disclosed that the Israel-based NSO Group had been offering the Pegasus spyware to its governmental clients – which included authoritarian regimes – for years (OCCRP, 2021).

Living up to the Greek mythological roots of its name, this military-grade trojan horse enabled those who purchased it to surreptitiously infiltrate mobile devices and exfiltrate sensitive data, such as location and messaging history. Pegasus was subsequently used to facilitate human-rights violations around the world on a massive scale, including – as has recently surfaced – in Israel itself (OCCRP, 2021).

Pegasus is a damning and evident indictment of the international community's inability to effectively regulate the proliferation of OCC, but it is by no means a standalone incident. Back in 2014, DarkMatter, a cybersecurity firm based in the United Arab Emirates, hired 'contractors' to infiltrate the lives of political opponents, journalists, and government critics on behalf of the monarchy, a business deal that would become known as the Raven Project (Spencer, 2021). Optimistic as one might be, all indications suggest that the problem of OCC

proliferation is likely to get worse before it gets any better.

As this contribution aims to demonstrate, there is a growing concern that the international community's inertia in convincingly addressing OCC proliferation has left a dangerous grey zone from which unscrupulous actors are only too keen to benefit. After all, advanced vulnerabilities and tools – once intended for state actors – are increasingly being bought and sold to the highest bidder, ushering in a dangerous new reality through the spread of OCC. This could – if left unchecked – gradually culminate in a techno-dystopian commercial environment, where cyber vulnerabilities and intrusive tools are developed by private organisations, to be sold to and exploited by private organisations.

THE COMMODIFICATION OF OCC: A REMOTE POSSIBILITY OR A PLAUSIBLE THREAT?

While many open-source intrusion tools are readily found on code-sharing sites or public internet fora – made available by hackers (ethical or otherwise) or cybersecurity researchers – more sophisticated and advanced hacking tools can be purchased by governmental agencies (at a hefty premium) from specialised vendors. Due to the absence of market scrutiny or regulatory oversight into the customers of these vendors, there is however no conclusive way to ascertain in whose 'arsenals' such tools eventually wind up.

Underground marketplaces, such as DarkMarket, TheWhiteHouse, or DarkFoxA – where customers can purchase a wide variety of spyware, phone exploits, ransomware source codes, and Advanced Persistent Threats (APT) tools – are inherently difficult to monitor or regulate. As a consequence, there is no evident and all-encompassing solution to effectively address the issue. OCC can and should be developed and/or deployed by government agencies for legitimate security uses, with robust democratic controls to limit their indiscriminate use. For example, former Australian Prime Minister Malcolm Turnbull explained back in 2017 how Australia's OCC were being used to 'help target, disrupt and defeat terrorist organizations', while ensuring that the use of these capabilities was 'subject to stringent legal oversight and consistent with obligations under international law' (Turnbull, 2017).

The most pressing issue, however, involves the manufacturing, commodification, and monetisation of OCC at the business-to-business (B2B) level. Assessing the post-incident impact of Pegasus for example, a senior defence correspondent for *Israel Hayom* – Israel's most widely-read newspaper – noted that 'as a rule of thumb, (cyber) weapons can only be sold to government agencies, not to private elements that could exploit them commercially'. (Limor, 2021). Noble as such statements might be, the validity of this 'rule of thumb' seems questionable in the light of (recent) evolutions in the OCC domain.

After all, OCC was being used for commercial interests as far back 2015, as the recent indictment of a Mexican citizen – the head of a company called Elite by Carga – who used 'an interception device' to tap into the phone calls of 'a business competitor', goes to show. In another instance, 'one or more "Elite by Carga" employees compromised and infiltrated the phone and email accounts of a Florida-based competitor, in exchange for [an] approximately $25,000 cash payment from the Mexican business' (Franceschi-Bicchierai, 2022).

In the context of corporate espionage, the absence of established rules and norms – that should codify red lines and responsible behaviour – exacerbates the confusion about what is legitimate or illegitimate behaviour (Hoffman & Maurer, 2019). The standard line taken by cyberweapons manufacturers has long been that they exclusively offer their products or services to governmental clients and law enforcement agencies. As the convoluted Pegasus saga demonstrates, however, such good-faith statements should be taken with a pinch of salt. By way of further example, NSO had stated that Pegasus could not be used to track Israeli citizens, but the company is currently under investigation by a national commission for infiltrating the phones of a dozen Israeli nationals (BBC, 2022).

As Nicole Perlroth highlighted in her bestseller *This Is How They Tell Me the World Ends: The Cyberweapons Arms Race*, the current laissez-faire approach to OCC has resulted in an ecosystem of unacceptable risk (Perlroth, 2021). Whereas the for-profit development of other instruments of warfare – be they conventional, nuclear, biological, or chemical – has been rightfully circumscribed in the past, this does not (yet) seem to be the case with OCC. In that same context, there appears to be a pattern of lies and deceit from numerous actors involved in the niche OCC field. For instance, there are strong indications that the Italian-based firm Hacking Team negotiated with a third-party reseller to export its malware to Nigeria to bypass Italian export controls (Hern, 2015). Moreover, back in 2019, a probe was launched into FinFisher – a German spyware maker that was accused of

Many open-source intrusion tools are readily found on code-sharing sites or public internet fora – made available by hackers

'exporting powerful spying software without a permit' (Deutsche Welle, 2019).

Worse still, the number of legally established companies that are dodging transparency and scrutiny is steadily increasing. In the words of Shalev Hulio, co-founder and CEO of NSO, 'the industry is going away from regulation [with]companies trying to hide activity and hide what they're doing'. (O'Neill, 2020). All this should add to the sense of urgency to develop rules of the road for truly bona fide organisations (O'Donnell, 2021). If not, an already shadowy world will simply get darker.

TOO LITTLE, TOO LATE? ASSESSING THE EU'S ACTION IN THIS FIELD

While the recent ENISA Threat Landscape Report paints a grim picture of the various sophisticated cyberattacks that the EU might face in the foreseeable future (ENISA, 2021), the Global Risk Report 2022 from the World Economic Forum (WEF) provides us with some staggering context against which to assess OCC proliferation (WEF, 2022). The report indicates that malware intrusions grew by 358 per cent in 2020, while ransomware infections grew by 435 per cent. A contemporary example is the more than 100 Log4j intrusion attempts detected every minute in December 2021, shortly after the flaw in the software library was discovered.

In the light of these observations, one could reasonably conclude that malicious cyber activity will continue to rise in the near future – facilitated by, among others, vulnerabilities and tools that exploit the complex digital (eco-)systems that have come to characterise our societies. While most private organisations that have built business models around the acquisition and commercialisation of weaponised zero-days vulnerabilities (i.e, a vulnerability in a system or a devices that has been disclosed but not patched) and intrusion tools – including the Malta-based ReVuln or the US-based Zerodium – are located in the United States or the EU, some of them are based in countries where human rights and due diligence processes are not considered important (Kesan & Hayes, 2016).

Even when these bona fide organisations are headquartered in the EU or United States though, according to a recent report from the Atlantic Council, several of them are 'irresponsible proliferators' as a result of 'their willingness to market outside their continents to non-allied governments' (Atlantic Council, 2021). This is all clear evidence that – for all intent and purposes – the predominant logic behind OCC proliferation will remain commercial. As such, one may rightfully ask what is to stop these actors from developing or acquiring OCC systems and selling them (for a hefty premium) to dubious individuals or unscrupulous companies. In short, what is to stop OCC commodification from materialising?

Given the impact that unchecked OCC might have on people's security and the prosperity of its economies, the proliferation and commodification of OCC by and for private organisations is a defining battle that the EU must take head on. As suggested by a recent European Policy Centre report, 'the EU will, after all, fail to advance towards strategic autonomy if it is not at the forefront of technological innovation and efforts to regulate emerging technologies' (Grevi, 2021).

While the EU has shown genuine ambition and progress in regulating various emerging and disruptive technologies – ensuring that they work for and are deployed in the interest of the Union and its citizens – most EU policy discussions and (regulatory) actions on OCC are focused on industrial policy, critical infrastructure protection, and responsible state behaviour in cyberspace. As such, far too little is being done to prevent private organisations from manufacturing and commercialising OCC in the grey or black market, be it in a business-to-business or business-to-consumer setting. As highlighted above, this constitutes a regulatory limbo that is incentivising private organisations to either enter the OCC market or expand their existing footprints in it.

Though commendable, previous efforts to introduce additional scrutiny to this space – for example, the EU's attempt to regulate the export of OCC (EU, 2021) or non-binding norms such as the UN Guiding Principles on Business and Human Rights (UNHRC, 2011) and the OECD Due Diligence Guidelines (OECD, 2018) – have had a rather limited

Far too little is being done to prevent private organisations from manufacturing and commercialising OCC in the grey or black market

impact. The most ambitious initiative to date, the EU's reform of its Dual Use Regulation, still falls short of placing explicit and legally binding conditions on Member States and private exporters alike. Be that as it may, the European Commission work programme for 2022 does include a proposal on a European Cybersecurity Resilience Act, which aims to establish common standards for cybersecurity products and could be a promising vehicle to address this issue.

While concrete details on the exact scope of this initiative are still scarce, Commissioner Thierry Breton clearly indicated the ambition to establish a specific European Cyber Capability Plan – integrating both civilian and military needs – as well as a genuine EU cyber doctrine that includes operational and defensive cyber capabilities. As such, one might reasonably conclude that the Cybersecurity Resilience Act will at least touch upon dual-use cyber products and might even go further. Spurred by the political controversy around Pegasus, the European Data Protection Supervisor also supported a 'ban on the development and deployment of spyware with the capability of Pegasus in the EU' (EDPS, 2022). These policy developments will certainly put extra pressure on EU Member States to take OCC commodification seriously. Leaving questions on the legality – under EU law – of such policy initiatives aside, the forthcoming negotiations on the Cybersecurity Resilience Act may – or may not – lay the foundation for a new chapter in OCC non-proliferation.

OCC PROLIFERATION: LIKELY TO GET WORSE BEFORE IT GETS ANY BETTER

As indicated above, cyberattacks are on the rise. While sophisticated, OCC-enabled attacks have traditionally been regarded as a natural extension of nation-states' geopolitical agendas, this is no longer the exclusive rationale behind them. After all, the cyber threat landscape is rapidly changing and increasingly putting private organisations and individuals at risk (WEF, 2021). While the intentions of hacker collectives and organised cybercrime are known to most, states are also increasingly shifting their modus operandi in cyberspace. In the light of this evolving threat landscape – characterised by various malicious actors with disparate motivations – zero-day vulnerabilities and more advanced intrusion tools could more easily find their way into the already existing grey and black markets for OCC.

It is against this backdrop that all indications suggest that the problem of OCC proliferation is likely to get worse before it gets any better. To better understand this phenomenon, reference can be made to the concept of 'offence-defence balance', a concept borrowed from the traditional study of war (Glaser & Kaufmann, 1998). In essence, the offence-defence balance approach assesses strategies, tactics, and technologies for their offensive or defensive added value, and thereby shapes a nation-state's foreign or defence policy. Unfortunately, most experts agree that the offence-defence balance in cyberspace is decidedly tipped in the favour of offence at the moment of writing. While there are several reasons for this trend – such as the ease of access to offensive technology versus the high costs of complex defensive controls as well as a chronic underinvestment in cyber defence – the ease of access to vulnerabilities and OCC capabilities is also certainly a contributing factor.

Moreover, regardless of the EU's normative and economic power, getting Member States to agree on the importance of OCC proliferation and the need for a (binding) regulatory framework will be no easy feat. After all, the EU still lacks a common position on many of the more sensitive cybersecurity or technology issues, including a shared understanding of the strategic importance of digital technologies like artificial intelligence. In a sector thought to be worth over $12 billion (Cyber Peace Institute, 2021) – and one that is so closely tied to national defence interests – reluctance to restrict national champions or trusted suppliers with further red tape will be particularly hard to overcome.

CHALLENGES AND AVENUES TO STRENGTHEN OCC NON-PROLIFERATION

Given the destructive potential and easy diffusion of cyberweaponry, it is reasonable to search for ways to limit its reach and (ab)use by unscrupulous actors. Therefore, one might reasonably wonder

whether an international non-proliferation agreement could be the way forward. If the last twenty years are anything to go by, this is likely to be a lost cause – particularly if such an agreement were to be modelled on nuclear-era disarmament treaties. After all, historic disarmament agreements defined how nation-states managed exclusive, expensive, and evident weapon systems. OCC, meanwhile, can be as basic and elusive as a few lines of obscure code purchased by any individual or organisation on the dark web. In other words, to recall Abraham Lincoln's words *'the dogmas of the past are clearly inadequate for the stormy present'*.

In this context, three recommendations are put forward to serve as food for thought for policymakers and security experts alike:

1. A truly multi-stakeholder approach to revive the spirit of the Wassenaar Arrangement

Given the prominent role of private organisations and individuals in OCC proliferation, policymakers should move away from the traditional state-centric, humanitarian, or national security-driven approaches to disarmament theory and rather embrace a whole-of-society method.

While the existing Wassenaar Arrangement on dual-use technologies and conventional weapon exports is far from an ideal framework in this regard – given its voluntary nature and absence of monitoring and enforcement measures – its signatory members could still use the existing framework as a platform to strengthen OCC norm-setting in cyberspace. The Pegasus saga could (and should) be the latest incident that spurs the necessary international momentum to (re)vitalise earlier attempts to capitalise on the framework offered by the Wassenaar Arrangement (Ruohonen & Kimppa, 2019).

By upholding a genuine multi-stakeholder approach and reformulating the issue of cyber-weaponry as one of prohibited and restricted goods, the private market for OCC might finally be incentivised to self-regulate. As nothing good ever comes easy, the first step in addressing cyber proliferation and commercialisation is recognising that it exists.

2. Moving from a geopolitical to an industrial-technical rationale

By moving away from a political-military and capability-driven standpoint on OCC towards a more industrial-technical rationale, policymakers could part from the narrow definition of cyber-weaponry and instead focus on the underlying set of capabilities that make up OCC systems.

While not all organisations within the OCC development chain necessarily partake in the proliferation process, focusing non-proliferation efforts on identifying and curbing the specific capabilities and actors that do so – such as exploit vendors or access-as-a-service providers – could result in the development of market regulation or industry standards to address such illicit activities.

The Atlantic Council has been doing excellent work in this regard, with the release of a March 2021 report entitled 'A Primer on the Proliferation of Offensive Cyber Capabilities' providing a more granular framework within which to craft technically feasible counterproliferation policies that do not harm valuable elements of the cybersecurity industry (Atlantic Council, 2021).

3. Leading by example

A world where private sector organisations can manufacture and sell cyberweapons to interested (non-state) parties is dangerous for everyone – be they ordinary citizens, private organisations, or even governments – and poses significant risks to international stability.

It will take courage and leadership to get the ball moving on this sensitive topic, in the same way all previous disarmament discussions did. Nations who stand to lose the most – i.e., those with many OCC organisations – are simultaneously those who will have to lead by example if this process is to gain any traction. Following their support for the Paris Call for Trust and Security in Cyberspace and the promising vehicle that is the EU-US Trade and Technology Council, the United States should seek to align its efforts with its European allies and partners to counter the private proliferation of OCC systems and look to non-traditional partners – such as China or India – who may prove to be willing to work on this specific issue. Preventing OCC commercialisation and proliferation from becoming completely out of control is in the interest of all major powers and could provide the foundation for future agreements on other cyber issues.

NOTES

1. Both authors are writing in a strictly personal capacity and the views expressed in this contribution should not be construed as representing those of any of the professional or academic institutions with which they are affiliated.

REFERENCES

Atlantic Council (2021) A Primer on the Proliferation of Offensive Cyber Capabilities, Report.

BBC (2022), 'NSO Group: Israel Launches Inquiry into Police Hacking Claims', *BBC News*, 7 February, https://www.bbc.com/news/world-middle-east-60287161.
Cyber Peace Institute (2021), 'How the Mercenaries Selling Cyber-Surveillance Software are a Threat to Cyberpeace', 12 March, https://cyberpeaceinstitute.org/news/how-the-mercenaries-selling-cyber-surveillance-software-are-a-threat-to-cyberpeace.
Deutsche Welle (2019), 'German Prosecutors Investigate Spyware Maker Finfisher', 5 September, https://www.dw.com/en/german-prosecutors-investigate-spyware-maker-finfisher/a-50293812.
EDPS (European Data Protection Supervisor) (2022), 'Preliminary Remarks on Modern Spyware', 15 February, https://edps.europa.eu/system/files/2022-02/22-02-15_edps_preliminary_remarks_on_modern_spyware_en.pdf.
ENISA (2021) ENISA Threat Landscape 2021, Report, ISBN: 978-92-9204-536-4 – DOI: 10.2824/324797.
EU (European Union) (2021). 'Regulation of the European Parliament and Council on Setting up a Union Regime for the Control of Exports, Brokering, Technical Assistance, Transit and Transfer of Dual-Use Items', 21 April, https://data.consilium.europa.eu/doc/document/PE-54-2020-INIT/en/pdf.
Franceschi-Bicchierai, L. (2022), 'The US Crackdown on Spyware Vendors is Only Beginning', *VICE*, 18 February, https://www.vice.com/en/article/jgmbag/the-us-crackdown-on-spyware-vendors-is-only-beginning.
Glaser, C., & Kaufmann, C. (1998), 'What is the Offense-Defense Balance and Can We Measure It?', *International Security*, 22(4), 44–82, https://doi.org/10.1162/isec.22.4.44.
Grevi, G. (2019), Strategic autonomy for European choices: The key to Europe's shaping power, European Policy Centre.
Hern, A. (2015), 'Hacking Team Hacked: Firm Sold Spying Tools to Repressive Regimes, Documents Claim', *The Guardian*, 6 July, https://www.theguardian.com/technology/2015/jul/06/hacking-team-hacked-firm-sold-spying-tools-to-repressive-regimes-documents-claim.
Hoffman, W., & Maurer, T. (2019), 'The Privatization of Security and the Market for Cyber Tools and Services', Carnegie Endowment for International Peace, Geneva Centre for Security Sector Governance, https://www.dcaf.ch/sites/default/files/publications/documents/Carnegie_MaurerHoffmann_July2019.pdf.
Kaspersky (2021), 'DarkChronicles: The Consequences of the Colonial Pipeline Attack', 21 May, https://ics-cert.kaspersky.com/publications/reports/2021/05/21/darkchronicles-the-consequences-of-the-colonial-pipeline-attack/#_Toc72509158.
Kesan J., & Hayes, C. (2016), 'Bugs in the Market: Creating a Legitimate, Transparent and Vendor-focused Market for Software Vulnerabilities'. *Arizona Law Review*, 58, 753–830, https://arizonalawreview.org/pdf/58-3/58arizlrev753.pdf.
Limor, Y. (2021), 'The Hackers: A Closer Look at the Shadowy World of Offensive Cyber', *Israel Hayom*, 13 August, https://www.israelhayom.com/2021/08/13/the-hackers-a-closer-look-at-the-shadowy-world-of-offensive-cyber.
Turnbull, M. (2017), 'Offensive Cyber Capability to Fight Cyber Criminals', Government of Australia, 30 June, https://www.malcolmturnbull.com.au/media/offensive-cyber-capability-to-fight-cyber-criminals.
O'Donnell, L. (2021), 'Europol Reveals Dismantling of "Largest" Underground Marketplace', 12 January, https://threatpost.com/europol-dismantling-underground-marketplace/162949.
O'Neill, P. H. (2020), 'The Man Who Built a Spyware Empire Says It's Time to Come Out of the Shadows', *MIT Technology Review*, 19 August https://www.technologyreview.com/2020/08/19/1007337/shalev-hulio-nso-group-spyware-interview.
OECD (Organisation for Economic Co-operation and Development) (2018), 'OECD Due Diligence Guidance for Responsible Business Conduct', https://www.oecd.org/investment/due-diligence-guidance-for-responsible-business-conduct.htm.
OCCRP (Organized Crime and Corruption Reporting Project) (2021), 'The Pegasus Project', https://www.occrp.org/en/the-pegasus-project.
Perlroth, N. (2021). *This Is How They Tell Me the World Ends: The Cyberweapons Arms Race*. New York: Bloomsbury.
Ruohonen, Jukka & Kimppa, Kai. (2019) Updating the Wassenaar debate once again: Surveillance, intrusion software, and ambiguity. Journal of Information Technology & Politics. 16. 1-18. 10.1080/19331681.2019.1616646.
UNHRC (United Nations Human Right Council) (2011), 'UN Guiding Principles on Business & Human Rights (UNGPs)', https://www.business-humanrights.org/en/big-issues/un-guiding-principles-on-business-human-rights/un-guiding-principles-the-next-decade.
World Economic Forum (2022) Global Cybersecurity Outlook, Insight Report, WEF.

Cybersecurity in the Age of Artificial Intelligence: Secured by Design or We Are Too Late

Marco Ciappelli and Sean Martin

https://doi.org/10.53121/ELFTPS3 • ISSN (print) 2791-3880 • ISSN (online) 2791-3899

ABSTRACT

The EU Artificial Intelligence Act aims to foster AI innovation while controlling it with regulations. Although that balance could eventually be achieved in the long run, relegating cybersecurity to a secondary role or an 'afterthought' will create a security gap that could create more problems than expected. Ethics and security are two sides of the same AI coin. One cannot exist without the other. This chapter contends that European measures and regulations currently lack detailed guidance for effective methods to handle malicious or accidental cyber activities and guard against the potential impact that compromised AI can have on society.

ABOUT THE AUTHORS

Marco Ciappelli is co-founder and podcast host at ITSPmagazine, with experience in digital branding and marketing. Marco has a PhD in Political Science from the University of Florence.

Sean Martin is an information security and technology veteran and a six-term Certified Information Systems Security Professional. Martin is the co-founder and director of operations and programming at ITSPmagazine, and is also an adjunct professor at the Graziadio Business School, serving on its Cyber Risk Professional Advisory Board.

CYBERSECURITY IN THE AGE OF ARTIFICIAL INTELLIGENCE: SECURED BY DESIGN OR WE ARE TOO LATE

The continuum between a utopian – 'modeled on or aiming for a state in which everything is perfect; idealistic'[1] – and a dystopian – 'relating to or denoting an imagined state or society where there is great suffering or injustice'[2] – future can be deceptive. Where we make our stand today will be our legacy to future generations who will thrive or wither because of these very decisions.

Cybersecurity is an important topic that continues to get a lot of attention: 'As many as 87% of executives are planning to improve cyber resilience at their organisation by strengthening resilience policies, processes, and standards for how to engage and manage third parties' (WEF, 2022).

Investments in artificial intelligence (AI) continue to skyrocket: 'our average simulation shows around 70 percent of companies adopting at least one of these types of AI technologies by 2030, and less than half of large companies may be using the full range of AI technologies across their organizations … AI could potentially deliver additional economic output of around $13 trillion by 2030, boosting global GDP by about 1.2 percent a year' (Bughin et al., 2018).

With the increased use of AI and the growing risk of cyberattacks, we must explore the world where these two factors collide. We must ensure that we have a vision for a future that supports the ethical use of AI in society, taking into account the cyber risks involved. The topic of cybersecurity is of utmost importance and this exploration could serve as a suggestion for EU policymakers in their effort

to build a more resilient and stronger cybersecurity infrastructure.

At this time, most countries seriously involved in developing and deploying AI systems of all sorts have been wise enough to realise that the incredible potential of AI can be harnessed and used for good only by developing sets of ethical rules that require such technology to operate in the interest of people's wellbeing, with respect to human rights, and to prevent all those outcomes that may negatively impact human lives (Jobin, et al., 2019).

In the sections that follow, we will provide examples of both bad and good uses of AI and how the technology can be subverted through methods of malicious and accidental cyber activities as a means to illustrate the potential impact that compromised AI can have on society.

Moreover, even if we don't directly answer them, this paper attempts to explore the following research questions:

1. What is the possibility that the proposed ideal balance between regulation and innovation may be too good to be true and impossible to achieve?
2. Is it possible to foster AI innovation while controlling it with heavy regulations that may not keep up with its pace?
3. Will cybersecurity be able to keep up with unrestrained and obviously unethical cybercriminals' innovation?

THE CYBERSECURITY IN AI PROBLEM

As with most things in life, including those created through innovation and technology, the more we do, the more we expose ourselves to risk. Consider:

- a bicycle that encounters risk at every turn (Hambleton, 2017)
- a personal powerboat where inaction can create a dangerous situation (California Casualty, 2020)
- a small civilian helicopter or plane that could go down at any moment (Lange, 2020)

Each of these machines can be a lot of fun, but they also bring with them a lot of risk (even if measured). This holds true for AI-enabled systems; the more the algorithms and systems ingest, analyse, and perform, the more they open themselves up to failure, misuse, and abuse, which introduces a lack of trust in the system that must be addressed (Jacovi et al., 2021).

The more the algorithms and systems ingest, analyse, and perform, the more they open themselves up to failure, misuse, and abuse

Examine any situation in life and you can find both the good and the bad. The same holds true for the state of cybersecurity for AI systems: 'In the continuous shift from analogue to digital, the potential for the malicious use of new technologies is also exposed' (Trend Micro Research, 2020).

To help illustrate these points of concern, let's apply this apparent lack of cybersecurity maturity to a few scenarios where AI may be used to make things better. First, the scenarios that could benefit from an AI system:

1. to reduce traffic and make highway travel more desirable, tolerable, and affordable (Kanowitz, 2020)
2. to make the supply chain more efficient (Alicke et al., 2021)
3. to raise the quality and shorten the time to market for new products (Newton, 2022)

It doesn't take much thought to jump from how things can go from 'we're making life better' to 'things just got a whole lot worse than they ever were'.

Let's look at each of these same three scenarios through this lens.

In the first example, the AI-enabled highway, consider a compromised and abused AI algorithm that could cause traffic flow to slow down or perhaps even come to a complete standstill (Comiter, 2019).

For the next example, the supply chain, picture some malformed data being fed into the system that could redirect supply-chain components to the wrong place at the wrong time, disrupting delivery and having a significant impact on the economy (Bonderud, 2021).

Finally, for the third example representing product development and manufacturing, the exposure

of the intricate (and private) manufacturing details could introduce a flaw in the product that could cause harm to the users (Micro.ai, 2022).

Insights from Michael C. Harasimowicz, Director of AI Innovations, Lockheed Martin, described the realities of these scenarios quite well: 'AI is a product of its environment; how is it built, trained, and deployed? AI applications will have to be secured where the data is collected, processed, and stored'.[3]

A 360-degree approach can help prevent many possible issues. Keeping one step ahead in cybersecurity is always the best move because by the time something happens, in most cases, it is simply too late. It is crucial that strong cybersecurity initiatives be pushed earlier in the AI lifecycle than later. It is also crucial that the definition of 'risk' be clear, including for the rankings of high, medium, and low. These points are explained with economics and philosophy in the article 'AI and the Paperclip Problem' (Gans, 2018).

Ultimately, cybersecurity is about protecting the decisions and actions initiated by AI, which means protecting the integrity of the AI data itself and the supply chain of the data and related activities (ETSI, 2021). Data integrity is only one aspect that needs to be evaluated as data confidentiality and availability must also be maintained. AI decisions extend beyond the data as well, so systems and algorithms must also be protected against a cyber attack that could disrupt the AI decision-making process.

While there are already many analyses, critiques, and suggestions to improve the Act (some important ones can be found on the Future of Life Institute website, which we invite you to read),[4] we still wondered: Is there enough being done in the EU AI Act to account for the potential cyber risks to society beyond the language that focuses so much on AI ethics? Does the EU AI Act do enough to address the unfortunate reality of the risks associated with cybersecurity in AI?

> [The European Community Artificial Intelligence Act] is a proposed European law on AI – the first law on AI by a major regulator anywhere. The law assigns applications of AI to three risk categories. First, applications and systems that create an unacceptable risk, such as government-run social scoring of the type used in China, are banned. Second, high-risk applications, such as a CV-scanning tool that ranks job applicants, are subject to specific legal requirements. Lastly, applications not explicitly banned or listed as high-risk are largely left unregulated.[5]

Although that balance could eventually be achieved in the long run, relegating cybersecurity to a secondary role or an 'afterthought' will create a security gap that could create more problems than expected. Ethics and security are two sides of the same AI coin. One cannot exist without the other.

METHODOLOGY

In pursuing our investigation of the EU AI Act, both qualitative and quantitative approaches have been employed, making liberal use of semi-structured interviews with top experts in the fields of AI, cybersecurity, and ethics.

The research considered the expert opinions of those intimately involved in current AI initiatives.[6] What was learned brought to light two key aspects of the challenge in securing AI systems: architecture and design of AI systems, and the human element involved in AI systems.

Through the use of these semi-structured interviews, AI risks were analysed and clarified. Based on this research, we make recommendations for how to implement cybersecurity by design as proposed for the enhancement of AI development.

THE STATE OF CYBERSECURITY IN AI IN THE EU

Although cybersecurity is a topic to which the EU AI Act draws attention, the debate is still in its infancy in this specific context and not enough is being invested in this area in terms of dedicated research, communication, development, and governance connecting AI, ethics, and cybersecurity together in the same conversations, policies, and actions.[7]

As Dr Ingrid Vasiliu-Feltes put it: 'The current state of cybersecurity as critical infrastructure in the context of AI mirrors the global cybersecurity landscape by being suboptimal, incongruent, and inconsistent'.[8]

The EU AI Act was the most prominent public document from the European Union with the greatest focus on AI and ethics, hence our selection of this piece of legislation to which we applied our focus.[9]

Cybersecurity in AI and its potential impact on society are not entirely absent. The EU AI Act does describe the result we are hoping to avoid: a serious incident. The Act states:

> 'Serious incident' means any incident that directly or indirectly leads, might have led or might lead to any of the following: (a) the death of a person or serious damage to a person's health, to property

The EU Artificial Intelligence Act proposes an ideal balance that aims to foster AI innovation while controlling it with regulations that may not keep up with its pace

or the environment, (b) a serious and irreversible disruption of the management and operation of critical infrastructure (EUR-Lex, 2021).

However, the devil is in the details – or the lack thereof – and a lot needs to happen if we are to avoid a 'serious incident'. Stephan Jou describes some of these details: 'AI is subject to attack methods and surfaces that are distinct. Adversaries can attack AI methods, and machine learning methods have unique weaknesses, with unique techniques and tactics (such as model stealing and threshold poisoning)'.[10]

Once we uncover and analyse the details, Keenan Skelly's perspective points to the need for concrete action: 'While the EU AI Act contains a few hard lines on AI development, such as banning the use of biometrics in AI research, it falls short of highlighting specific examples of "misuse" and the processes that must be created to avoid the use of AI for social, economic, and population control'.[11]

Concrete action is best defined early on in the AI lifecycle, which is where we head next in this article.

ARCHITECTURE AND DESIGN OF AI SYSTEMS PROTECTION

It took decades for organisations and governments to take cybersecurity seriously (White House, 2021). And, although the cybersecurity industry has matured, there are still many gaps when it comes to maturity in cybersecurity programmes in the commercial space, including the prediction from some analysts that, by 2025, cyberattackers will have weaponised operational technology environments to successfully harm or kill humans (Gartner, 2021).

Matthew Rosenquist points to this reality, noting that while advancements have been made in cybersecurity, connecting these dots to other programmes can be challenging: 'Cybersecurity is no further advanced than the AI it must eventually protect'.[12]

Add an advanced technology like AI to the mix and things get even more challenging to secure and regulate (Weissinger, 2021). This idea is supported by Dr Ingrid Vasiliu-Feltes: 'The complex portfolio of AI tools has the potential to greatly contribute, augment, and amplify the existing cybersecurity efforts'.[13]

Further to the point of complexity, Dr Macnish was involved in crafting a report called 'Security Issues, Dangers and Implications of Smart Information Systems: D1.3 Cyberthreats and Countermeasures' that explores how AI and cybersecurity interact through three different approaches (Patel et al, 2020):

1. the poor use of AI leads to weaknesses in a system that an attacker can exploit
2. the use of AI by an attacker to offer a sophisticated attack (such as poisoning)
3. the use of AI in cybersecurity to identify singularities and abnormalities in established patterns of behaviour

The report, which was completed under the European Union's Horizon 2020 Research and Innovation Programme, notes that 'machine learning models are hard to defend against because there are very many ways for attackers to force models into producing incorrect outputs', but also spells out clearly that 'AI researchers and engineers will need to be aware of the sorts of ethical issues they may encounter in their work and understand how to respond to them' (SHERPA, n.d.Patel et al, 2020).

THE HUMAN ELEMENT OF AI SYSTEM PROTECTIONS

We cannot overlook the human aspect in all of this: 'The main challenge to AI originates from the considerable percentage of the data on which AI systems rely coming from humans. Such data carries with it the irrationalities and subjectivity of humans, who are mostly driven by self-interest' (Winter, 2018).

Matthew Rosenquist adds to this perspective:

Cybersecurity professionals are included beginning in the architecture and design phases for

solutions to help designers and engineers understand the most likely ways attackers may attempt to misuse or manipulate the tools and specific implementations of AI systems. Ongoing risk assessments and mitigation decisions must remain in place for the entire lifecycle, as threats will evolve and vulnerabilities will inevitably be discovered.[14]

Unless we want the machines to have free, unfettered reign over the decisions we empower them to make, we need some human oversight. We need a set of checks and balances to detect problems as early as possible in the lifecycle of the systems we are designing and building. This oversight must be formal and it must be dedicated.

This raises questions about who will determine what is acceptable or too risky. Perhaps we want specific non-legislative people or groups to take control of the societal-specific elements of how AI systems work. But, on the other hand, we'll also need to figure out how guidelines, standards, and laws fit into this picture. We need to figure out:

- Who ensures that the guidelines are followed?
- Who checks to verify that standards are being applied?
- Who enforces the law?

Michael C. Harasimowicz raises a critical point that must not be overlooked: 'If oversight becomes so costly, the incentive to innovate may be lost, and advantage will be given back to the cybercriminals'.[15]

Regardless of the checks and balances (or a lack thereof), a society that successfully embraces AI is likely one that has trust and oversight. But even that can be a delicate balance.

RESULTS

Recommendation: Lean on Multiple Decades of Cybersecurity Maturity

Each of the scenarios described in the 'Architecture and design of AI systems protection' section points to three challenges faced with any technology-driven system:

- Keeping secrets a secret
- Maintaining trust throughout the system
- Ensuring that the system can be accessed when needed

These challenges point directly to the need to look closely at the three critical aspects of cybersecurity – the CIA triad:

- Confidentiality
- Integrity
- Availability (Kim & Solomon, 2013)

Looking at AI systems through the frame of the CIA triad helps define the systems, the data model, and the processes in a way that should highlight situations where something could go wrong and a serious incident could occur (Axelrod, 2021). This should force designers, developers, and deployers to ask the most essential questions imaginable, such as what would happen if:

- a person's information is exposed and they come under risk of a personal attack at work or at home ('What happens if we fail to keep private information private?')
- a small town near the border of an adjacent country has its critical infrastructure (electrical grid, water systems, and highways, for example) manipulated with faulty data, turning the grid off and preventing water from being treated ('What happens if we fail to maintain integrity in the system?')
- a healthcare system is compromised with ransomware and goes offline, so the data is not available, and doctors – and their robotic surgical devices – are unable to treat their patients ('What happens if we fail to keep all systems going, especially when it matters the most?')

Any of these scenarios are worrisome or downright problematic, especially when lives are at risk. Mitigating these risks when a single AI system is involved means that only one system can fail. Presumably, if that system is important enough, it can be controlled and monitored to prevent something terrible from happening if it were to be compromised. However, connect multiple systems together and we begin to create an even more complex environment to manage, monitor, and control.

Using the last example above, take this multi-AI system into a healthcare setting where people, machines, and algorithms are making life-and-death decisions. There need to be some clear controls in place and a formal set of checks and balances applied to ensure that things don't go off the rails (Jercich, 2021).

Securing AI requires more than claiming a balance of protecting confidentiality, integrity, and availability. It requires that:

- Security-oriented operating policies be defined to identify and mitigate the risk of attack and misuse

- Security measures be implemented to protect against compromise and abuse
- Detection capabilities be applied to block attacks and the spread of compromised systems
- Monitoring be put in place to ensure that operating guidelines are being adhered to, spotting and sending alerts of anomalies when they arise
- Response mechanisms be organised and practised to stop, slow, and minimise the impact, providing for a clean path to recovery while limiting damage

This is where something like a security management framework can come into play. More specifically, this is where a common security framework such as the National Institute of Standards and Technology (NIST) Cybersecurity Framework, for example, can be applied to:

- identify
- protect
- detect
- respond
- recover (NIST, n.d.)

We must avoid starting from scratch. Instead, we should leverage what's already available to us to help us mitigate as much risk as possible, even if what we plan to utilise isn't perfect.

> It is noteworthy that while there are standards already available or being developed for concepts and terminology, data and knowledge, human interaction, metrics, networking, performance, safety, risk management, and trustworthiness, there is no formal recognition of the importance of cybersecurity for AI (except perhaps as a side effect of safety and risk management), at least according to the NIST document.[16]

Still, we can't wait for things to be perfect before we proceed. Sometimes good enough is just that: good enough. We can take that as a suitable place to start and progress from there. This isn't a new concept, as in the EU white paper 'On Artificial Intelligence: A European Approach to Excellence and Trust', which suggests that 'The EU should make full use of the tools at its disposal to enhance its evidence base on potential risks linked to AI applications, including using the experience of the EU Cybersecurity Agency (ENISA) for assessing the AI threat landscape' (European Commission, 2020).

Recommendation: beyond standards and frameworks comes regulatory oversight

If standards aren't quite there yet, can we begin to prescribe and rely on regulatory policies to help us mitigate the cyber risks coming in AI? Or will we see a lag in regulatory controls because they may be seen as limiting progress in commercial innovation? Vasiliu-Feltes, Rosenquist, Joyce Drohan, and Macnish all provided some insight into these questions.

> Regulations and societal or ethical positions do not necessarily stifle commercial innovation efforts; however, they interfere and often delay large scale AI deployments.[17]

> Regulations are simply obstacles to criminals. Something to be ignored, avoided, or manoeuvred around. The adversaries are intelligent, and only when regulations are coupled with equally intelligent security does meaningful risk prevention and minimisation capability manifest.[18]

> Although regulations and societal/ethical positions are potentially limiting and have impact, we need to think about what drives these positions.[19]

> I do not see policy, ethics, and innovation as conflicting with one another. They can be, but they do not have to be. To be successful and meaningful, innovation must take place under some guidelines and limits. The question is not whether there should be limits, but where those limits are placed.[20]

In the end, society will determine what is essential and will bring together the people, processes, technology, and policies necessary to ensure that we get to the ideal place we want to be. The journey, however, may not be as smooth and pleasant for everyone across the board. Still, with a bit of effort, hopefully, we can make sure that people remain safe along the way and that the destination is closer to utopia than dystopia.

Michael C. Harasimowicz shares a positive outlook on this front: 'From experience in military operations, financial services, and defence contracting, I have witnessed a general sense of encouragement by existing governmental guidance to pursue ethical approaches to using AI'.[21]

Here are a few examples that demonstrate the ability to integrate cybersecurity directly into the overall narrative:

AI can provide many positive outcomes for society and bring many benefits that were unattainable just a generation ago

- The US Department of Defense's Ethical Principles, published in February 2020, propose deep introspection into how responsible, equitable, traceable, reliable, and governable the use of AI is (Lopez, 2020).
- The European Union's Ethics Guidelines for Trustworthy Artificial Intelligence were finalised in April 2019 (European Commission, 2019).
- The Montreal Declaration is a document covering ethical and responsible AI (Université de Montréal, n.d.).

In addition to guidance, countries must be prepared to take action, as noted by Keenan Skelly:

> As the EU and the US, and the countries that follow begin to roll out legislation for 'ethical' AI and 'secure' AI, we must remember that there are already many nefarious uses of the technology. As such, it would be wise to call those out specifically and early on. Continuous monitoring of AI misuse must also be incorporated, not as a warning, but as illegal activity with consequences.[22]

Surely, the true test will be how well we translate and enforce ethical and cybersecurity policies in the form of code, algorithms, systems, and risk management controls. If we're not talking about it adequately now, the chances of seeing it flow through to implementation will certainly be slim.

CONCLUSION

Artificial intelligence can provide many positive outcomes for society and bring many benefits that were unattainable just a generation ago. In between the promises and the risks of artificial intelligence innovation lies a sea of uncertainty. Our best hope to create the technological future we want is to think ahead and build ethics and cybersecurity into it from the earliest point possible.

Because AI enhances human thought and behaviour, and extends control to machines and applications, we must, as a society, consider carefully how cybersecurity risks could jeopardise the control, outcomes, biases, and execution of AI in achieving our societal goals.[23]

Just as we make decisions based on low, medium, and high returns on our investments, we also need to make decisions based on well-defined low, medium, and high levels of cyber risk.

Therefore, taking this analysis and slapping security onto AI as an afterthought will only increase the chance of AI being compromised and misused, and create a situation where society is negatively impacted. To avoid this, we suggest that EU policymakers include specific language in the AI regulation that leverages existing standards, frameworks, and models to address cybersecurity in the design phase that will enable the checks and balances to follow as the policies, controls, monitoring, and enforcement come together down the line.

Potential implications of cybersecurity (or a lack thereof) to the work being done by EU policymakers have been explained in relation to the EU AI Act.[24]

Our final recommendation is that the EU move above and beyond the existing separate understandings and documents of cybersecurity, AI, and ethics to bring them all together with dedicated analysis and guidance that crosses over into each other's policy. A section dedicated to cybersecurity within the EU AI Act could help tackle cybersecurity as a core element in the age of AI where it is not only developed and used ethically but is also secure by design. Now is the time; we are not too late.

NOTES

1. https://www.lexico.com/en/definition/utopian.
2. https://www.lexico.com/en/definition/dystopian.
3. M.C. Harasimowicz, personal communication, 4 February 2022.
4. https://artificialintelligenceact.eu/analyses.
5. https://artificialintelligenceact.eu/analyses.
6. H. Miller, personal communication, 2 April 2022.
7. I. Vasiliu-Feltes, personal communication, 8 February 2022.
8. H. Miller, personal communication, 2 April 2022.
9. S. Jou, personal communication, 9 February 2022.
10. K. Skelly, personal communication, 10 February 2022.
11. M. Rosenquist, personal communication, 31 January 2022.
12. I. Vasiliu-Feltes, personal communication, 8 February 2022.
13. M. Rosenquist, personal communication, 31 January 2022.
14. M.C. Harasimowicz, personal communication, 4 February 2022.
15. Jou, personal communication, 9 February 2022.

16. I. Vasiliu-Feltes, personal communication, 8 February 2022.
17. M. Rosenquist, personal communication, 31 January 2022.
18. J. Drohan, personal communication, 9 February 2022.
19. K. Macnish, personal communication, 1 February, 2022.
20. M.C. Harasimowicz, personal communication, 4 February 2022.
21. K. Skelly, personal communication, 10 February 2022.
22. H. Miller, personal communication, 2 April 2022.
23. H. Miller, personal communication, 2 April 2022.

REFERENCES

Alicke, K., Dilda, V., Görner, S., Mori, L., Rebuffel, P., Reiter, S., & Samek, R. (2021), 'Succeeding in the AI Supply-Chain Revolution', McKinsey, 30 April, https://www.mckinsey.com/industries/metals-and-mining/our-insights/succeeding-in-the-ai-supply-chain-revolution.

Axelrod, C. W. (2021), 'Ransomware and the C-I-A Triad', *Security Boulevard*, 19 July, https://securityboulevard.com/2021/07/ransomware-and-the-c-i-a-triad.

Bonderud, D. (2021), 'Supply Chain Attack: What It Is (and What to Do About It)', *Security Intelligence*, 28 September, https://securityintelligence.com/articles/supply-chain-attack-what-it-is-what-to-do.

Bughin, J., Seong, J., Manyika, J. Chui, M., & Joshi, R. (2018), 'Notes from the AI Frontier Modeling the Impact of AI on the World Economy', McKinsey Global Institute, https://www.mckinsey.com/~/media/McKinsey/Featured%20Insights/Artificial%20Intelligence/Notes%20from%20the%20frontier%20Modeling%20the%20impact%20of%20AI%20on%20the%20world%20economy/MGI-Notes-from-the-AI-frontier-Modeling-the-impact-of-AI-on-the-world-economy-September-2018.ashx

California Casualty (2020), 'Top 6 Risk Factors for Boating Accidents', https://mycalcas.com/2020/06/top-6-risk-factors-for-boating-accidents.

Comiter, M. (2019), 'Attacking Artificial Intelligence: AI's Security Vulnerability and What Policymakers Can Do About It', Belfer Center for Science and International Affairs, Harvard Kennedy School, August, https://www.belfercenter.org/publication/AttackingAI

ETSI (European Telecommunications Standards Institute) (2021), 'Securing Artificial Intelligence (SAI); Data Supply Chain Security', https://www.etsi.org/deliver/etsi_gr/SAI/001_099/002/01.01.01_60/gr_SAI002v010101p.pdf.

EUR-Lex (2021), 'Proposal for a Regulation of the European Parliament and of the Council: Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts. (Article 3, Item 44)', https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206.

European Commission (2019), 'Ethics Guidelines for Trustworthy AI', 16 November, https://op.europa.eu/en/publication-detail/-/publication/d3988569-0434-11ea-8c1f-01aa75ed71a1/language-en.

European Commission (2020), 'On Artificial Intelligence – A European Approach to Excellence and Trust', white paper, 2 February, https://ec.europa.eu/info/sites/default/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf.

Gans, J. (2018), 'AI and the Paperclip Problem', *Vox*, 10 June, https://voxeu.org/article/ai-and-paperclip-problem.

Gartner (2021), 'Gartner Predicts By 2025 Cyber Attackers Will Have Weaponized Operational Technology Environments to Successfully Harm or Kill Humans', press release, 21 July, https://www.gartner.com/en/newsroom/press-releases/2021-07-21-gartner-predicts-by-2025-cyber-attackers-will-have-we.

Hambleton, M. (2017), 'The 5 Most Common Dangers to Cyclists on the Road', Royds Withy King, 17 August, https://www.roydswithyking.com/info-hub/5-common-dangers-cyclists.

Jacovi, A., Marasović, A., Miller, T., & Goldberg, Y. (2021), 'Formalizing Trust in Artificial Intelligence: Prerequisites, Causes and Goals of Human Trust in AI', FAccT '21, https://arxiv.org/pdf/2010.07487.pdf.

Jercich, K. (2021), 'Diagnostic AI May Be Vulnerable to Cyberattacks, UPMC Study Shows', *Healthcare IT News*, 14 December, https://www.healthcareitnews.com/news/diagnostic-ai-may-be-vulnerable-cyberattacks-upmc-study-shows.

Jobin, A., Ienca, M., & Vayena, E. (2019), 'Artificial Intelligence: The Global Landscape of Ethics Guidelines', Health Ethics & Policy Lab, https://arxiv.org/pdf/1906.11668.pdf.

Kanowitz, S. (2020), 'How AI Can Reduce Traffic Congestion and Fuel Consumption', GCN, 25 March, https://gcn.com/emerging-tech/2020/03/how-ai-can-reduce-traffic-congestion-and-fuel-consumption/303335.

Kim, D., & Solomon, M.G. (2013). *Fundamentals of Information Systems Security*. 2nd ed. Burlington, MA: Jones & Bartlett Publishers.

Lange, J. (2020), 'The Dangers of Private Helicopters and Planes', *The Week*, 29 January, https://theweek.com/articles/892128/dangers-private-helicopters-planes.

Lopez, C. T. (2020), 'DOD Adopts 5 Principles of Artificial Intelligence Ethics', US Department of Defense, 25 February, https://www.defense.gov/News/News-Stories/Article/Article/2094085/dod-adopts-5-principles-of-artificial-intelligence-ethics.

Micro.ai (2022), 'Ransomware in the Industrial Automation Sector', https://www.micro.ai/blog/ransomware-in-the-industrial-automation-sector.

Newton, E. (2022), 'How Are AI and Robotics Increasing Manufacturing Quality and Efficiency?', *IoT Times*, 12 January, https://iot.eetimes.com/how-are-ai-and-robotics-increasing-manufacturing-quality-and-efficiency.

NIST (National Institute of Standards and Technology) (n.d.), 'Request for Information | Evaluating and Improving NIST Cybersecurity Resources: The NIST Cybersecurity Framework and Cybersecurity Supply Chain Risk Management', https://www.nist.gov/cyberframework.

Patel, A., Hatzakis, T., Macnish, K., Ryan, M., & Kirichenko, A. (2020), 'Security Issues, Dangers and Implications of Smart Information Systems: D1.3 Cyberthreats and countermeasures', SHERPA, 29 April, https://figshare.dmu.ac.uk/articles/online_resource/D1_3_Cyberthreats_and_countermeasures/7951292.

SHERPA (n.d.). 'Security Issues, Dangers and Implications of Smart Information Systems (SIS)', https://www.project-sherpa.eu/security-issues-dangers-and-implications-of-smart-information-systems-sis.

Trend Micro Research (2020), 'Malicious Uses and Abuses of Artificial Intelligence', https://static1.squarespace.com/static/5b504068365f025b0e4f790a/t/5fbbdee340350635ed33c68f/1606147831970/AI+MLC.pdf.

Université de Montréal (n.d.), 'The Montreal Declaration for the Responsible Development of Artificial Intelligence', https://www.montrealdeclaration-responsibleai.com/the-declaration.

Weissinger, L. (2021), 'AI, Complexity, and Regulation: OUP Handbook on AI Governance', SSRN, 14 October, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3943968.

White House (2021), 'Executive Order on Improving the Nation's Cybersecurity', 12 May, https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity.

Winter, D. (2018), 'AI Errors vs. Human Errors. International Director', 19 June, https://internationaldirector.com/technology/ai-errors-vs-human-errors.

WEF (World Economic Forum) (2022), 'Global Cybersecurity Outlook 2022: Insight Report', https://www3.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2022.pdf.

Cybercrime-as-a-Service: EU Perspectives

Pierluigi Paganini

https://doi.org/10.53121/ELFTPS3 • ISSN (print) 2791-3880 • ISSN (online) 2791-3899

ABSTRACT

This chapter analyses the impact of cybercrime on society, with a focus on EU organisations and businesses. It explores the key contributory factors in the growth of the cybercrime ecosystem and the development of the most active cybercrime rings. The chapter also provides evidence of the impact of the ongoing conflict between Russia and Ukraine on the operations of cybercriminal gangs on a global scale, as well as detailing the medium term (three to five years) initiatives needed to strengthen cybersecurity and dismantle cybercrime organisations.

ABOUT THE AUTHOR

Pierluigi Paganini is CEO of the cybersecurity firm Cybhorus, and a member of the European Union Agency for Network and Information Security ad hoc Working Group on Cyber Threat Landscapes. Paganini is also Adjunct Professor in Cyber Security at University Luiss Guido Carli and a strategy consultant for government and private businesses. His passion for writing and a strong belief that security is founded on knowledge-sharing and awareness led Paganini to create the security blog 'Security Affairs', which has been named several times as the Best Personal European Cyber Security blog. He has authored several books, the most recent being *Digging The Deep Web: Exploring the Dark Side of the Web*.

INTRODUCTION

The impact of cybercrime on our society continues to increase while we move more of our lives and business activities into cyberspace. We are observing a dangerous trend on a global scale – most of the reported crimes are related to fraudulent activities online. This is the tip of the iceberg because cybercrimes are often not reported by the victims.

It is not simple to evaluate the economic impact of cybercrime. Many cybersecurity firms have attempted to estimate it by analysing multiple factors, such as the loss of intellectual property and sensitive data, costs of service disruptions, damage to brand image and victims' reputation, penalties and compensatory payments to customers or contractual compensation (for delays, etc.), costs of countermeasures and insurance, costs of mitigation strategies and recovery from cyberattacks, loss of trade and competitiveness, distortion of trade, and job losses.

Cybercrime has been estimated to cost the world $10.5 trillion annually by 2025 (Morgan, 2020), according to the Internet Crime Report (IC3) 2020 released in 2021. In 2020, the reported losses exceeded $4.2 billion, and authorities observed an increase of more than 300,000 complaints from 2019 (+69 per cent) (FBI, 2021).

One of the biggest contributors to the significant increase is the rapid evolution of the cybercrime-as-a-service (CaaS) model in the threat landscape.

ASSESSING THE PROBLEM: CAAS, THE WINNING MODEL

In the CaaS model, skilled cybercriminals offer their products and services to other criminals. CaaS has lowered the barrier to entry into the cybercrime arena and offers rapid means for crooks to maximise their profits.

FIGURE 1: **The rising cost of cybercrime**

Source: CyberSecurity Ventures

Threat actors who pay for products and services are not necessarily lower-level criminals; in some cases, they opt to rent services and infrastructure to speed up their operations or to make it harder to attribute the attacks to them. In some cases, attackers simply rent out their services/products, while in other cases they request the payment of a share (10–20 per cent) of any profits made in an attack conducted with their support.

The most profitable services and products for cybercriminals using a CaaS model are those that can be automated and that can leverage the anonymity offered by the dark web and cryptocurrencies.

CaaS is a win-win model as threat actors offering their products and services only need to invest once in the development and maintenance of a solution that can be used for multiple attacks.

To analyse the diffusion of CaaS, it is important to study the channels used to match the supply of CaaS with demand, such as underground marketplaces, cybercrime forums, and custom Tor websites. A study titled 'Measuring Cybercrime as a Service (CaaS) Offerings in a Cybercrime Forum' published in 2021 presented a comprehensive longitudinal analysis of the types of CaaS supply and demand on a cybercrime forum (Akyazi et al., 2021). A team of researchers developed a classifier to identify the supply and demand for each type of service and measure their relative prevalence. The study was based on a dataset spanning 11 years of posts on the popular cybercrime forum Hack Forums. Table 1 reports the different types of CaaS along with the price model and estimated price for each service.

The study revealed that 15.6 per cent of the first posts in the 'Market' section offered CaaS, demonstrating the high demand for such services. The offers and demands for services under the 'bot/botnet as a service', 'reputation escalation as a service', and 'traffic as a service' categories represented over 60 per cent of CaaS activities.

The researchers also analysed the evolution of the numerous services. For example, the demand for 'bot/botnet as a service' decreased after 2013, and also relative to 'hacker as a service' after 2015.

TABLE 1: **CaaS categories and their properties**

	CaaS name	Status	Pricing model	Estimated price
EaaS	Exploit as a Service	Existing	Licence Subscription	up to more than $250,000 $150,000 per month
PLaaS	Payload as a Service	Existing	Pay-per-install Commission	$0.02-$0.1 per install 40%
DaaS	Deception as a Service	Existing	Subscription Commission	$85-$115 per month 40%
OBaaS	Obfuscation as a Service	Existing	Subscription	$50-$150 per month 40%
SCaaS	Security Checker as a Service	Existing	Subscription	$25 per month
TRaaS	Traffic Redirection as a Service	Existing	Pay-per-click	$7-$15 per 1000 visitors
BNaaS	Botnet as a Service	Existing	Subscription	$40 per month
BHaaS	Bulletproof Hosting as a Service	Existing	Subscription	$300 per month
TAaaS	Traffic (including DDoS) as a Service	Existing	Subscription	$999 per month
REaaS	Reputation Escalation as a Service	Existing	Pay-Per-record	$0.42-$0.7 per record
MPaaS	Marketplace as a Service	Existing	Licence Commission	$4500 per licence 2%-10%
MRaaS	Money Mule Recruiting as a Service	Existing	Licence	$1700 per licence
MLaaS	Money Laundering as a Service	Existing	Commission	2%-30%
HTaaS	Hacker Training as a Service	Existing	Licence	$200-$800 per person
PPaaS	Personal Profile as a Service	Evolving	Licence	$4-$20 per record
TPaaS	Tool Pool as a Service	Evolving	Subscription	$4000 per month
RaaS	Reputation as a Service	Evolving	Subscription	–
HRaaS	Hacker Recruiting as a Service	Evolving	Subscription	–
VDaaS	Vulnerability Discovery as a Service	Emerging	Subscription	$542.04-$1810.31per vulnerability
TSaaS	Target Selection as a Service	Emerging	Subscription	–
EPaaS	Exploit Package as a Service	Emerging	Subscription	$4000 per month
RPaaS	Repackage as a Service	Emerging	Subscription	–
DMaaS	Domain Knoweledge as a Service	Emerging	Subscription	–
VEaaS	Value Evaluation as a Service	Emerging	Subscription	
CPaaS	CAPTCHA solving as a Service	Existing	Pay-per-solution	$0.5-$20 per 1000 CAPTCHAs solved
PSVaaS	Phone/SMS Verification as a Service	Existing	Pay-per-challenge Licence	$0.20 per challenge $8-$15 per server
RPSaaS	RDP/Proxy/Seedbox as a Service	Existing	Subscription	$25-$250 per month
EWaaS	E-Whoring as a Service	Emerging	Subscription	–

However, 'account' and 'other' categories are dominant accounting for around 70% of the total number of posts (39.7% and 29% respectively). Posts related to 'cash-out' (12.6%) and 'product-type [*sic*] – composed of *crypter, e-whoring pack, exploit, malware/hacker tool* (3.1%) were lower in number than CaaS offerings.

The diffusion of multipurpose botnets is one of the factors that most influence the threat landscape. Multiple threat actors leverage botnet to conduct a broad range of malicious activities, such as ransomware distribution, DDoS attacks, fraudulent crypto mining, disinformation, and boosting social media accounts or web-shopping page rankings.

Today, it is easy to find a broad range of cybercriminal services in underground marketplaces. The most popular ones are ransomware-as-a-service (RaaS), access-as-a-service, DDoS for hire, and Bitcoin Tumblers.

THE EXPLOSION OF THE RAAS MODEL AND ITS IMPLICATIONS

The number of ransomware attacks spiked in the last couple of years due to the adoption of the RaaS model provided by the most prominent cybercrime gangs.

Dozens of ransomware gangs have created a network of affiliates and provide them their malware with various levels of customisation, depending on the specific operations. Almost any criminal group, even technically inexperienced ones, could become an affiliate of one of the ransomware gangs and spread their malware by paying a fee that is a percentage of the ransom (10–25 per cent). The model has lowered the entry barrier to the cybercrime arena and allows minor gangs to make millions in profits, with the result that damage caused by ransomware attacks is increasing. Critical infrastructure is more exposed to a new generation of threats that are more aggressive and sophisticated. Unfortunately, the situation is becoming worse despite the numerous operations conducted by law enforcement on a global scale.

Another element of the success of ransomware attacks is the implementation of a 'double extortion' model to force victims to pay the ransom. The gang threatens to publish the data stolen by the victims if they do not pay up. In some cases, ransomware gangs also implemented a triple extortion by launching DDoS attacks against the victim to further pressure them into paying the ransom.

To get an idea of the profits behind the double-extortion model, let's analyse the findings of a study conducted by Swiss security firm Prodaft with the support of blockchain analysis firm Elliptic on the operation of a notorious ransomware gang known as Conti.

Conti ransomware operators offer a private RaaS. The malware appeared in the threat landscape at the end of December 2019 and was distributed through TrickBot infections. Experts speculate the operators are members of a Russia-based cybercrime group known as Wizard Spider. In August 2020, the group launched a leak website to threaten its victims with releasing stolen data.

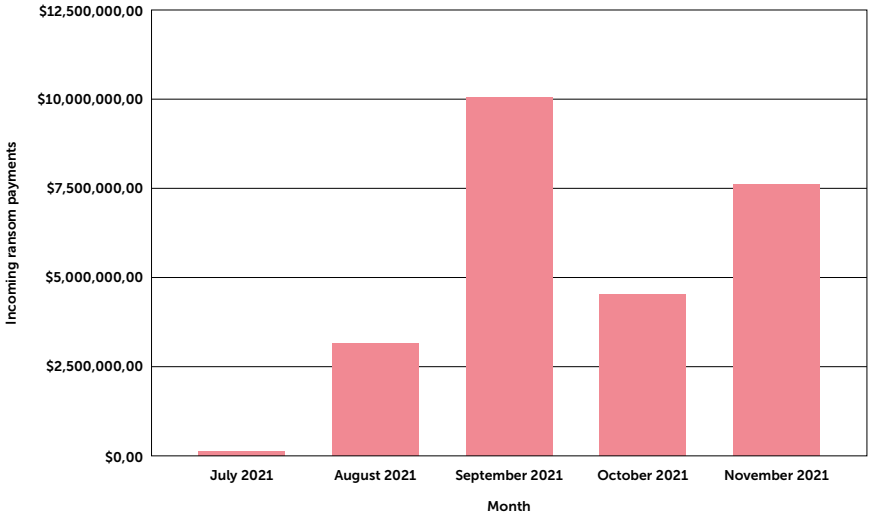
The study revealed that the operators of the Conti ransomware have earned at least $25.5 million from attacks and subsequent ransoms carried out since July 2021 (Prodaft, 2021). The experts analysed 113 wallets associated with Conti ransomware operations that were involved in transactions for more than 500 bitcoins.

The numbers in Figure 2 are only the tip of the iceberg. Experts believe that the Conti ransomware operation has earned much more over this period.

Elliptic experts also analysed the transactions associated with Conti affiliates. One cluster identified by the researchers received payments from both Conti and DarkSide, a circumstance that suggests that a threat actor was affiliated with both groups.

The study also highlights the sophisticated money-laundering operation implemented by Conti

FIGURE 2: **Monthly ransom payments to Conti gang**



Source: Security Affairs

affiliates. Some affiliate funds have not yet been moved from the wallets due to the pressure of law enforcement, in other cases the threat actors used multiple services, including exchanges, coin swaps, privacy-enhancing wallets including Wasabi, and the Russian language darknet marketplace Hydra.

In March 2021, Elliptic researchers also analysed the profits of another cybercrime gang, the Darkside ransomware group, and revealed that it had earned over $90 million from ransom payments from its victims since October 2020 (Robinson, 2021).

The cybercrime gangs offering their support to Russia represent a double threat to Western organisations

ASSESSMENT OF THE EU SITUATION

The EU's situation is similar to that of other countries – in recent years, we have observed an exponential increase in cybercriminal activity. In the current scenario, amid the COVID-19 pandemic, cybercriminals have continued exploiting opportunities created by the remote working allowed by many organisations and used the coronavirus as bait for several attacks and frauds. Mobile malware operators and scammers have exploited the increased use of online shopping services, and we have seen an increase in attacks against mobile-banking users.

In this scenario, the growing CaaS market on the dark web has played a crucial role, law enforcement agencies reported a surge in the malware-as-a-service offerings and the auctioning of stolen data that could be used by threat actors to conduct multiple attacks.

One of the best sources of information about criminal activity online is the annual 'Internet Organised Crime Threat Assessment' (IOCTA) published by Europol (2021).

The IOCTA report provides a law enforcement-focused assessment of an evolving threat landscape and analyses key developments in the area of cybercrime with contributions from European law enforcement agencies and private sector partners, including security firms.

> The crime-as-a-service (CaaS) model remains a prominent feature of the cybercriminal underground and is a cross-cutting factor throughout the cybercrime sub-areas. In the past 12 months, European law enforcement agencies have reported an increase in MaaS [malware-as-a-service] offerings on the Dark Web, of which ransomware affiliate programs seem to be the most prominent. These programs are an evolution of the Ransomware-as-a-Service (RaaS) model in which the operators share profits with partners who can breach a target network and either harvest all the information required to launch an attack or deploy the malware themselves. This has expanded the market of selling access to compromised infrastructure and data breaches. (Europol, 2021)

Another trend observed by the experts is the rapid diffusion of the access-as-a-service whereby threat actors sell access into networks. Experts observed the creation of remote access markets, which are automated stores that allow threat actors to exchange access credentials to compromised websites and services. Buying access to an organisation as a service lowers the entry barrier for further exploitation and exposes organisations to a broad range of attacks, drastically increasing their success rate.

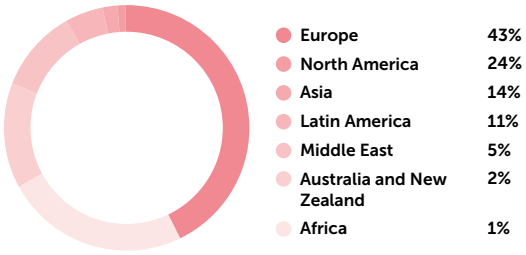
The data offered by access brokers in the hacking forums and marketplaces have different sources. They may come from past data breaches that were made public, exchanges with other threat actors, vulnerability exploitation, or other attacks performed by the brokers themselves. In rare cases, access brokers may have purchased the stolen credentials from malicious third-party actors.

One of the most popular services offered by access brokers is credential validation, wherein they check if usernames and passwords work by either trying them manually or using automation to perform mass validation.

RDP- AND VPN-BASED ACCESS

A study conducted at the end of 2021, based on the analysis of over 900 access broker listings being offered for sale from January to August 2021 on multiple English and Russian language underground cybercriminal forums revealed that the majority (43 per cent) of all the advertisements for access brokers were related to businesses in the European region, followed by North America with 24 per cent and Asia 14 per cent (TrendMicro, 2021).

FIGURE 3: **Access broker in 2021**



Source: Trend Micro

THE IMPACT OF THE RUSSIA-UKRAINE CONFLICT ON THE CYBERCRIME ECOSYSTEM

Many cybercrime gangs are composed of crooks from countries in Eastern Europe, including Russia, Ukraine, and Belarus, and the ongoing conflict has upset the balance on which many of the criminal groups were based. Some gangs operate from Russia, targeting organisations worldwide, and local authorities have never persecuted them. These gangs have obtained a sort of immunity by avoiding targeting Russian organisations. Their malware is often explicitly developed to avoid infecting the systems of Russian users. However, security experts and intelligence agencies claim that the indulgence of Russian law enforcement towards local cybercrime organisations is due to the close link between Russia-linked hacking groups and major cybercrime organisations, such as the Conti ransomware gang.

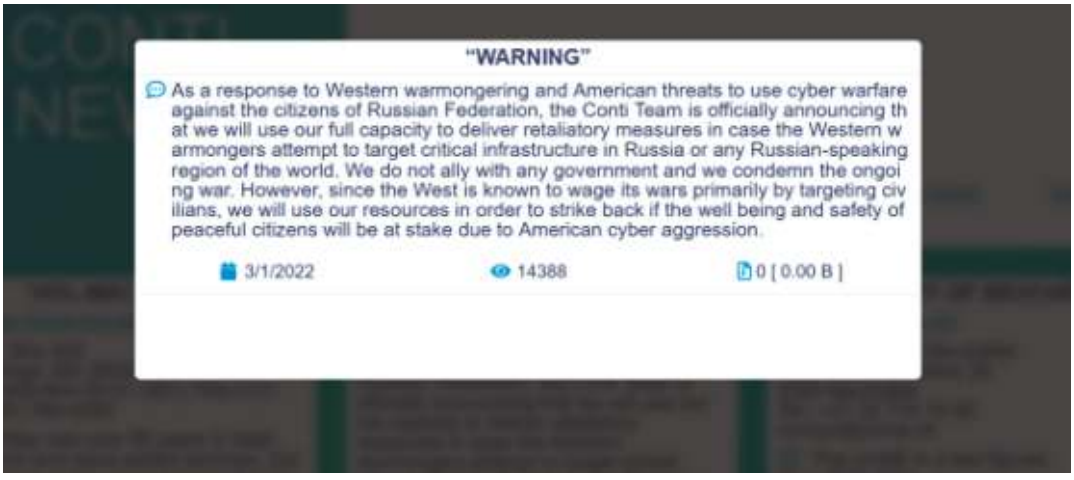
The position of the Conti ransomware gang is a case worth studying. Immediately after the Russian army's invasion of Ukraine, this cybercrime organisation publicly announced its support for the Moscow government.

After the announcement, a Ukrainian researcher leaked 60,694 internal chat messages belonging to the Conti ransomware operation. He was able to access the database XMPP chat server of the Conti group. The data leak was retaliation for Conti's support for the Russian invasion of Ukraine. The attack will have a significant impact on the operation of the gang, considering that many of Conti's affiliates are Ukrainian groups. The researcher who leaked Conti's communications announced more dumps would be forthcoming, and also leaked the source for their ransomware, including the administrative console. The public availability of the source code could temporarily destroy the Conti ransomware operation because security experts can reverse engineer it to determine how it works and develop a working decrypting software.

On the other side, the cybercrime gangs supporting Russia represent a double threat to Western organisations. Besides the damage caused by the attacks, these groups could share stolen data and access to the networks of the target organisations with the Russian government, which could use them to conduct further attacks. Most exposed are critical infrastructure targets that could be hit with cyberespionage and sabotage attacks with unpredictable consequences.

The conflict has shattered the balance in the criminal ecosystem by bringing the operations of many criminal gangs closer to Russian and Ukrainian state actors. Some gangs have separated because of their

FIGURE 4: **Conti ransomware announcement of support for Russia**



members' political differences, and new crews have appeared on the threat landscape. The overall result is the pressure on EU organisations has increased. We cannot rule out the possibility that some criminal operations will be backed by nation-states that will use cyber mercenaries to attack Western businesses bypassing sanctions.

HOW EUROPEAN INSTITUTIONS ARE FIGHTING CYBERCRIME

In response to the escalation in the number of cyberattacks, the EU is addressing cybersecurity challenges from different perspectives.

According to the European Council, the EU authorities are conducting multiple activities to tackle cyber threats, including (European Council, 2021):

- enhancing cyber resilience
- fighting cybercrime
- boosting cyber diplomacy
- reinforcing cyber defence
- boosting research and innovation
- protecting critical infrastructure

The European Council recognises the need to enhance the cybersecurity of critical sectors such as transport, energy, health, and finance, where the level of technological penetration is extremely high.

In December 2021, the Council agreed on the new cybersecurity directive. During the December Telecommunications Council, EU ministers adopted the NIS2 directive as a 'general approach' on measures to create a high level of cybersecurity across the EU members. The NIS2 has been designed to further improve the resilience and incident response capacities of both the public and private sectors, aligning the capabilities of the individual states.

The first directive on the security of network and information systems (NIS) was introduced in 2016 to increase cooperation among Member States on cybersecurity. It provides security obligations for operators of critical services. In December 2020, the European Commission revised the NIS directive (NIS2) to respond to the evolving threat landscape.

The pillars of the new directive are the further increase in information-sharing and cooperation, and the enhancement of the security of supply chains. The establishment of the EU Agency for Cybersecurity is another important move to increase cybersecurity at the EU level. The new agency that is based on the European Union Agency for Network and Information Security (ENISA), under a permanent mandate, covers a crucial role in the process of improving cybersecurity among Member States. It is tasked with supporting EU institutions and other stakeholders in dealing with cyberattacks.

Fighting cybercrime in all its forms is a priority of EU authorities. For this reason, a specialised European cybercrime centre has been created within Europol to help EU countries investigate cybercrimes and dismantle criminal rings.

The EU also launched the European Multidisciplinary Platform Against Criminal Threats, a security initiative aimed at prioritising and addressing threats posed by international organised crime, including cyberattacks.

Other measured adopted by the EU include a sanctions framework, first proposed in 2019, for cyberattacks launched by entities outside the EU. The framework allows the EU to place sanctions on perpetrators of cybercrime. In July 2021, for the first-ever time, the EU imposed economic sanctions on Russia, China, and North Korea following cyberattacks aimed at the EU and its Member States (European Council, 2020). The EU Council announced sanctions on a Russia-linked military espionage unit, as well as companies operating for Chinese and North Korean threat actors who launched cyberattacks against the EU and its Member States.

CONCLUSION AND FUTURE CHALLENGES

The deep penetration of technology in our lives, most of which continues to be unsecured by design, is sustaining the growth of online crime and is putting national critical infrastructure and private businesses at risk and threatening economic growth and development. Our vulnerability to attacks has increased like never before, and threat actors are aware of this and are attempting to devise new sophisticated attack techniques. The CaaS model is attracting new players to the cyber arenas – criminals with huge capital who are investing in cybercrime due to the high profits and low risks compared with other criminal activities. Cybercrime will soon be the principal criminal activity and authorities worldwide are approaching the problem by creating new processes and developing new capabilities to counteract these practices.

The thin line between cybercrime and state-sponsored hacking represents a threat to modern society. We are likely to see an increasing number of financially motivated cyberattacks conducted by state-sponsored hackers for fundraising purposes and to bypass sanctions. The attacks will be more

The CaaS model is attracting new players to the cyber arenas – criminals with huge capital who are investing in cybercrime due to the high profits and low risks

sophisticated, will involve new technologies and will be quite impossible to attribute to a specific actor – the perfect crime.

In this scenario, governments are approving new directives that would oblige organisations and businesses to act against cyber threats and proactively implement countermeasures. Organisations in critical and important sectors would be supported in adopting the proper cyber posture to protect their assets and the supply chains to which they belong.

Legislation should cover security requirements and processes including supply-chain security, patch management, vulnerability disclosure, information-sharing, and incident response.

A crucial aspect of mitigating the threat of cybercrime is the establishment of a framework for better cooperation and information-sharing between private and public authorities in Europe, and enhanced collaboration with international bodies from other continents (i.e., US, African, and Asian authorities).

FURTHER CHALLENGES

In the medium term (three to five years), the EU will carry out the initiatives it has already announced, aimed at strengthening cybersecurity and dismantling cybercrime organisations. One of the most interesting initiatives proposed by the European Commission is the creation of a new Joint Cyber Unit (JCU) to provide a coordinated response to cyberattacks and crises.

The creation of the JCU was first proposed in 2019 by European Commission President Ursula von der Leyen. It is considered a milestone in reinforcing the European cybersecurity crisis management framework. The European Commission highlighted the importance of a joint and orchestrated response to a growing number of increasingly sophisticated attacks (ENISA, 2021). The JCU is the result of the EU Cybersecurity Strategy and the EU Security Union Strategy meant to secure the digital economy and society. The unit will represent a point of connection for the European cybersecurity bodies and communities.

The JCU aims to roll out plans for joint preparedness activities by the end of June 2022 and should be fully running by 2023. it will be funded through the Commission's programme for digital technology, likely using the European Defence Development Fund.

The JCU will be composed of experts from ENISA, EU countries, Europol's European Cybercrime Centre, the European External Action Service, and the European Defence Agency. To improve cybersecurity in the EU in the coming years, Member States will dedicate significant efforts and huge investments to research into innovative solutions through dedicated financial programmes. Cybersecurity is an important part of the EU research and innovation funding framework programme Horizon 2020 and its successor Horizon Europe.

In May 2020, the EU committed €49 million to boost innovation in cybersecurity and privacy systems; this figure will increase in coming years.

The EU Digital Europe Programme for 2021–27 established an investment of €1.6 billion in cybersecurity to design a broad range of cybersecurity infrastructure and tools that will be used to protect public administrations, businesses, and individuals in Europe (European Commission, 2021).

In the next couple of years, we will see an increasing number of successful operations coordinated by Europol to curb cybercriminal activities in the EU. These operations will be possible thanks to a major level of information-sharing between European law enforcement bodies and the US FBI. Cybercrime is a prolific industry, and a growing number of criminal organisations will attempt to expand their operations to cyberspace, and the CaaS model will help this process.

POLICY RECOMMENDATIONS

An efficient strategy to mitigate the growing threat posed by cybercriminal organisations must:

- **Foster partnerships specifically defined to combat cybercrime that see the contribution of national agencies and private security firms.** These partnerships must enhance their knowledge-sharing and operational capabilities

to counter illegal activities online. Government agencies and private companies must develop a process for sustainable cooperation. The adoption of a common framework for collective action against cybercrime should be one of the principles of long-term strategic alignment. Another important principle to promote is to ensure that participation in the cooperation adds value for every actor involved in the process.

- **Foster intragovernmental and intergovernmental collaborations.** To achieve this goal, it is necessary for an entity to be tasked with coordinating multiple efforts from the actors involved. Investigating cybercriminal operations requires international information-sharing and efficient cross-border cooperation. The main obstacle to cooperation is the misalignment with existing legislative and operational frameworks adopted by the different states involved in an investigation. Another problem is the speed required in the investigation of online crimes – often the sharing of information across different entities is slow due to the involvement of legal entities from states using different frameworks. Unfortunately, despite the numerous successes against criminal organisations worldwide in Western countries, the likelihood of arrest is extremely low. The cooperation mechanisms at the disposal of law enforcement agencies must be improved to speed up information-sharing and coordinate on-field operations against criminal rings.
- **Improve public–private partnerships**. Private operators could provide essential technical capabilities to prevent and investigate sophisticated cyber incidents. An efficient model of collaboration between the public and private sectors could enhance the response to cybercrime. To improve the partnership against cybercrime, it is important to involve international stakeholders to achieve a global overview of cross-border cybercriminal activities and commitment to cooperate. Government and private initiatives must facilitate strategic dialogue and support cooperation between stakeholders. Multiple organisations and think tanks promote a model based on a collaborative network composed of permanent nodes. Each node gathers information about the threat landscape and shares it in real-time with other nodes through a framework for information-sharing. The nodes should also promote the creation of threat-focused groups, which could be short-term and mission-driven groups of partners that work together to investigate and dismantle a specific criminal operation.
- **Promote the creation of working groups focused on cybersecurity in vertical industries**. The creation of working groups could help to focus on cyber threats that target specific sectors using sophisticated and ad hoc tactics, techniques, and procedures. Working groups can define specific frameworks to mitigate exposure to cyber threats and should focus on the development of innovative technologies to detect and neutralise a new generation of cyber threats. These groups should be tasked with promoting awareness programmes and helping organisations adopt proper cyber hygiene.

REFERENCES

Akyazi, U., van Eeten, M., & Gañán, C.H. (2021), 'Measuring Cybercrime as a Service (CaaS) Offerings in a Cybercrime Forum', WEIS online conference, 28–29 June, https://weis2021.econinfosec.org/wp-content/uploads/sites/9/2021/06/weis21-akyazi.pdf.

ENISA (European Union Agency for Cybersecurity) (2021), 'EU Boost Against Cyberattacks: EU Agency for Cybersecurity Welcomes Proposal for the Joint Cyber Unit', https://www.enisa.europa.eu/news/enisa-news/eu-boost-against-cyberattacks-eu-agency-for-cybersecurity-welcomes-proposal-for-the-joint-cyber-unit.

European Commission (2021), 'EU Digital Europe Programme', https://digital-strategy.ec.europa.eu/en/activities/digital-programme.

European Council (2020), 'EU Imposes the First Ever Sanctions Against Cyber-Attacks', https://www.consilium.europa.eu/en/press/press-releases/2020/07/30/eu-imposes-the-first-ever-sanctions-against-cyber-attacks.

European Council (2021), 'Cybersecurity: How the EU Tackles Cyber Threats', https://www.consilium.europa.eu/en/policies/cybersecurity.

Europol (2021), 'Internet Organised Crime Threat Assessment (IOCTA) 2021', https://www.europol.europa.eu/publications-events/main-reports/internet-organised-crime-threat-assessment-iocta-2021.

FBI (2021), 'Internet Crime Report 2020', Internet Crime Complaint Center, https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf.

Morgan, S. (2020), 'Cybercrime to Cost the World $10.5 Trillion Annually by 2025', Cybersecurity Ventures, 13 November, https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016.

Prodaft (2021), '[Conti] Ransomware Group In-Depth Analysis', 18 November, https://www.prodaft.com/resource/detail/conti-ransomware-group-depth-analysis.

Robinson, T. (2021), 'DarkSide Ransomware Has Netted over $90 Million in Bitcoin', 18 May, https://www.elliptic.co/blog/darkside-ransomware-has-netted-over-90-million-in-bitcoin.

TrendMicro (2021), 'Investigating the Emerging Access-as-a-Service Market', 30 November, https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/investigating-the-emerging-access-as-a-service-market.

The Need to Introduce a New Individual Right to Cybersecurity

Vagelis Papakonstantinou

https://doi.org/10.53121/ELFTPS3 • ISSN (print) 2791-3880 • ISSN (online) 2791-3899

ABSTRACT

Currently cybersecurity concerns are often perceived as exclusively pertaining to states and organisations. All current regulatory instruments either in effect or in the legislative process are addressed to Member States and (large or important) organisations in the EU. For individuals, on the other hand, cybersecurity is seen as a service to be indirectly provided by third parties. This is a fundamentally flawed understanding. Individuals should not be seen as passive recipients of cybersecurity, dependent on the goodwill and effectiveness of third parties. On the contrary, they need legal tools to protect themselves in the digital environment. The introduction of a new right to cybersecurity will enable individuals to protect their digital selves, while legally requiring third parties to respect their rights.

ABOUT THE AUTHOR

Vagelis Papakonstantinou is a professor of law at the Faculty of Law and Criminology of the Vrije Universiteit Brussel (VUB). Coordinator of VUB's Cyber and Data Security Lab, a core member of VUB's Research Group on Law, Science, Technology & Society, and a research member of the Brussels Privacy Hub, his focus is on privacy and data protection, cybersecurity, digital personhood, and computer programmes.

INTRODUCTION

Although cybersecurity concerns are usually high on the list of issues that worry Europeans, under the current policy-making understanding (if not conventional wisdom) cybersecurity is a matter that exclusively pertains to states and organisations. In essence, all current regulatory instruments either in effect or in the legislative process are addressed to Member States and (large or important) organisations in the EU. As far as individuals are concerned, cybersecurity is effectively a service to be indirectly provided to them by the above direct recipients of legislation, once they have complied with their regulatory obligations.

This is a fundamentally flawed understanding. Individuals ought not to be treated as passive recipients of cybersecurity, dependent on the goodwill and effectiveness of third parties – even if these refer to their respective Member States. On the contrary, they need to be provided with the legal tools to protect themselves in the digital environment. The exponential growth of cyber threats, which now target individuals in the same manner as they do organisations or entire states, means that the protection of their rights cannot justifiably continue to remain outside their grasp. The introduction of a new right to cybersecurity would enable individuals to protect their digital selves, while legally requiring third parties to respect their rights.

This policy recommendation builds on an academic paper by the author that has recently been published in the *Computer Law and Security Review* (Papakonstantinou, 2022). While the theoretical groundwork for the introduction of a new individual right can be found in its text, here this idea will be placed within the boundaries of a policy brief, to conceptualise and formulate it in a clearer, and hopefully more practical manner.

ASSESSING THE PROBLEM

Individuals are threatened daily by cyber threats. Information technology developments have enabled attackers to target daily millions of internet users in a multitude of manners and with a wide range of aims and purposes. This comes in stark contrast to the situation ten or more years ago, when the first systematic cybersecurity efforts were noted at the EU level. The then limited technical capacities meant that only states and large organisations could be targeted by expensive and time-consuming cyberattacks. Nowadays, however, each one of us is faced daily with cyber threats ranging from identity theft to credit card fraud and from internet scams to ransomware (ENISA, 2021).

The lack of a specific right to cybersecurity means that individuals are at a disadvantage in their efforts to defend themselves against cyber threats. Whatever EU cybersecurity legislation already exists is not addressed to them and does not afford them any meaningful tools to protect themselves (see Chapter 3). While it is true that several related fields of law may step in to assist individuals who have to deal with a cyberattack (for example, personal data protection law in the event of unlawful processing of their personal data or criminal law in the event of fraud), the fact remains that all these solutions are piecemeal and incremental and do not provide a complete protective framework.

In essence, individuals are deprived of a right to security in the digital realm although they enjoy a right to security in the physical world. The right to security is a fundamental human right,[1] which (according to certain human rights theories) even takes precedence over any other right, in the sense that unless it is enjoyed in full, all other rights become impossible (Shue, 1996: 20). Such reasoning aside, the fact remains that individuals enjoy in the physical world a right to security, which affords them the right to be and feel secure within their natural environment.

Although the right to security is not spelt out in much detail in legal texts, due to its inherently elusive exact content (Lazarus, 2007: 330), in practice, formal acknowledgement of its existence means that secondary legislation can be constructed around it. In essence, criminal law protects the integrity of the person,[2] a right to defence allows a person to react in case of violence against them, tort law grants them a right to monetary indemnity in the event they are harmed in any way, etc. (Fredman, 2007: 308). Nevertheless, such secondary legislation builds upon notions (for example, what constitutes an 'act' or an 'omission' or 'psychological and physical violence') that have been formulated over thousands of years of written human history and have by now become intuitive, security being a fundamental preoccupation of humans.

A similar approach in the digital realm is missing. Although digital life has become increasingly important to individuals, there is no formal acknowledgement that they have a right to cybersecurity in the same manner as they have a right to security in the physical world. The right to (physical) security could not possibly fill that gap. Cybersecurity is not a subset of security.[3] Essentially, it differs from security in exactly the same way that our digital life differs from our natural-world one.

In addition to differences in nature (digital life versus the physical world), the lack of an explicit right to cybersecurity means that secondary legislation around it cannot be built. While, as will be seen in the next chapter, the EU has put substantial effort into introducing cybersecurity-relevant laws, none takes the individual into account. Being addressed only to states and (large or important) organisations, they fail individuals in a twofold manner: they fail to create the necessary understanding around basic notions such as 'threat', 'attack', 'violence', and 'security' in the digital realm, and they also fail to provide individuals with the means to defend themselves.

ASSESSMENT OF THE EU SITUATION

The EU has been at the forefront of global cybersecurity regulation. Its first attempts were in 2008,[4] and the law-making pace has not eased up since. In practice today, the NIS Directive of 2016 and the Cybersecurity Act of 2019 set the EU regulatory scene.[5] At the same time, an influx of important new instruments is imminent, in the form of the NIS 2 Directive,[6] and a directive on the resilience of critical entities.[7]

However, what all current EU initiatives have in common is that they single-mindedly address only state and (large or important) organisations. Within their provisions, cybersecurity emerges as a concern only of those actors, an administrative and bureaucratic task to carry out through the introduction of mechanisms and procedures, instead of a living and ongoing concern of everybody. They do not create any rights. Essentially, infringement of their provisions only leads to administrative fines at best. Individuals and courts (and also organisations that are not their addressees, which is the vast majority of organisations in Europe) are kept out of

the cybersecurity discussion. All EU initiatives and existing laws point in the same direction and adopt the same approach, without exception.

Nevertheless, the tools to begin the acknowledgement of a new right to cybersecurity are already at hand. The EU Cybersecurity Act, in particular, has made important contributions in this regard. First and foremost, it defines cybersecurity in its text as 'the activities necessary to protect network and information systems, the users of such systems, and other persons affected by cyber threats' (Article 2, point 1). This definition acknowledges 'users' as well as 'other persons' as recipients of cybersecurity, thus creating the necessary broad and inclusive circle of addressees for any new individual right. Second, in its Article 1, it places 'a high level of cybersecurity, cyber resilience and trust within the Union' on the same level as 'ensuring the proper functioning of the internal market', therefore paving the way for the introduction of a new right to warrant such trust and resilience. Third, it provides a suitable name ('Cybersecurity Act') to create public expectations of the creation of new cybersecurity conditions, exiting decidedly from the inward-looking and technical 'network and information systems directive' or 'critical infrastructures directive'.

In addition, from a human rights perspective, the EU Charter of Fundamental Rights has brought forward two law-making options: under the first – the traditional route – it is enough to spell out a human right in constitutional texts, and then laws and courts are expected to apply it without any need for further definitions. Under this category falls, for example, the traditional right of security in Article 6. Under the second option, primary texts mandate the release of a secondary law, that will more closely define the right's particulars. The right to data protection in Article 8 (and the subsequent GDPR system)[8] is a prime example of this.[9]

CURRENT EU INITIATIVES

No initiatives are underway, or even under discussion, at the EU level for the introduction of a new individual right to cybersecurity. Neither the draft NIS 2 Directive nor the directive on the resilience of critical entities (see Chapter 3) takes this issue into account. To the author's knowledge at least, this is an entirely new proposal. No similar proposals have been discussed in any Member States or third countries, in spite of the fact that cybersecurity legislation, in one way or another, has been enacted in most regions of the planet.[10]

> What all current EU initiatives have in common is that they single-mindedly address only state and large or important organisations

FURTHER CHALLENGES AND OPTIONS

A number of challenges lie ahead for the adoption of a new EU individual right to cybersecurity. First and foremost, the content of such a right needs to be agreed upon. Immediately, two issues stand out: Is this to be a social human right or a traditional, positive one? And is this to be a simple declaration of principle or does its exact content need to be detailed in secondary legislation? As regards the former, an individual right to cybersecurity could not possibly be a social right.[11] An obligation by the government to create a safe online environment, perhaps going hand-in-hand with the protection of the environment or providing education, misses the basic point that individuals need to be provided with legal means to protect themselves, not broad political declarations. After all, current EU initiatives already take exactly that into account, creating 'a high level of cybersecurity, cyber resilience and trust within the Union' (see Chapter 3).

The latter, whether a simple, traditional human rights declaration or detailed legislation like the GDPR, would best suit a new right to cybersecurity, but it poses more significant difficulties. A simple declaration (for example, an extension of Article 6 of the EU Charter of Fundamental Rights to read 'everyone has the right to liberty and security of person, *including in the digital environment*')[12] may perhaps appear more appealing at first, particularly because it seems easier to agree upon and thus adopt. Nevertheless, such a solution would miss the basic point of the introduction of such a new right, namely the provision of legal tools for individuals to protect themselves. Any general declaration to cover cybersecurity in the same manner as physical security risks running the same theoretical and practical dead-ends met by the latter (see Chapter 2). Nevertheless, in the case of cybersecurity,

individuals do not benefit from thousands of years' knowledge of what a 'threat' or 'violence' really is. Cybersecurity only has a recent history of a few decades. Although it exponentially increases in importance for individuals with each passing day, its exact content still needs to be defined. This task cannot be left to common knowledge, that will take a disproportionately long time to formulate. Therefore, it is in specificity that the merits of any new right to cybersecurity lie. Just as with personal data protection and the GDPR system, any new right to cybersecurity would require secondary legislation to spell out its exact contents.

Other difficulties pertain to the EU's power to legislate in the field. Cybersecurity, falling under the broader topic of security, in principle falls outside the EU's legislative scope. In essence, all EU initiatives listed in Chapter 2 are based on Article 114 of the Treaty on the Functioning of the European Union (TFEU), on the functioning of the internal market. While this may be true, there is certainly no restriction in including such a right in the next amendment of the EU's Charter of Fundamental Rights. If this, as history has taught us, may take time to achieve, secondary EU legislation could move ahead anyway.

This is not unprecedented law-making in the EU. Most prominently, data protection could serve as a model *par excellence* for cybersecurity. The 1995 EU Data Protection Directive,[13] which anticipated both Article 16 TFEU (which was introduced in 2008) and the GDPR system (which was introduced in 2016), was released on the basis of Article 100a of the then TFEU, which was the equivalent of today's Article 114. Consequently, the EU legislative process is not necessarily linear. In other words, it is not necessary for a new right to first be spelt out in the treaties in order for secondary legislation to further detail its particulars. As personal data protection has demonstrated, a directive or regulation could well grant Europeans rights and obligations akin to a right, before the right itself finds its way into the treaties.

POLICY RECOMMENDATIONS

The introduction of a new human right in the EU is by no means an easy or straightforward matter. While the end of the (long) trail could include a combination of a traditional individual right in the EU treaties accompanied by secondary legislation, this is an accomplishment that may lie well ahead of us – while cyber threats and the need for the EU to act are present and imminent. Therefore, the EU could introduce a right to cybersecurity in already existing or soon-to-be-released regulatory instruments. The Cybersecurity Act, with its ambitious title and its Title I offering 'general provisions' on cybersecurity, would be an obvious candidate in this regard. Provisions detailing the contents of a new right to cybersecurity could be inserted there once its text is next amended.

The introduction of a new human right in the EU is by no means an easy or straightforward matter

Alternatively, an entirely new EU instrument could be released, preferably a regulation, but possibly a directive,[14] specifically for the purpose of protecting individuals from digital threats and risks. Such an instrument would need to coordinate with what is already available, meaning the definitions and other *acquis* of the EU cybersecurity instruments already in effect, while introducing the exact content of a right to cybersecurity.

While the exact legislative option (amendment of the EU Cybersecurity Act or introduction of entirely new legislation) may not matter, or at least be of merely practical significance because the actual content of the relevant provisions would be identical, what a new right to cybersecurity would offer is a new perspective in EU cybersecurity law. Until today all, significant EU efforts over the past decade have focused entirely on governments and important organisations protecting themselves in the digital environment. While this is a commendable cause, in line with what other regions are striving for globally, it misses the individual point of view. Individual lives are spent increasingly in the digital environment. Threats, technology permitting, are increasingly becoming individualised instead of institutional, as in the past. It is therefore important for the EU to shift perspectives to place individuals under its protective scope as well. This can be performed through the introduction of a new right to cybersecurity, broadly following the steps of the individual right to data protection. The right to data protection is a useful case study for the introduction of a digital-born right in the EU treaties. Its contribution ought not to be wasted or overlooked; in fact, a

new right to cybersecurity would enhance the protection afforded to Europeans in the digital realm, creating an environment of online safety and trust while at the same time furthering the EU's goals.

NOTES

1. See Article 3 of the Universal Declaration of Human Rights. In Europe, see Article 5 of the European Convention on Human Rights and Article 6 of the EU Charter of Fundamental Rights.
2. Nevertheless, Piet Hein van Kempen discusses extensively the insufficiency, or even unsuitability, of criminal law to effectuate human rights, affecting, in practice, the relationship between cybercrime legislation and a right to cybersecurity (van Kempen, 2013: 16ff).
3. See also the European Commission's distinction between 'physical security' and 'cybersecurity' in the Explanatory Memorandum of its its NIS 2 draft (Proposal for a Directive of the European Parliament and of the Council on Measures for a High Common Level of Cybersecurity Across the Union, repealing Directive (EU) 2016/1148, COM/2020/823 final).
4. Council Directive 2008/114/EC of 8 December 2008 on the Identification and Designation of European Critical Infrastructures and the Assessment of the Need to Improve Their Protection.
5. 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. Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on Information and Communications Technology Cybersecurity Certification and Repealing Regulation (EU) No 526/2013 (Cybersecurity Act).
6. Proposal for a Directive of the European Parliament and of the Council on Measures for a High Common Level of Cybersecurity Across the Union, Repealing Directive (EU) 2016/1148, COM/2020/823 final.
7. Proposal for a Directive of the European Parliament and of the Council on the Resilience of Critical Entities, COM/2020/829 final.
8. 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).
9. See also Article 3, para. 2, point a, and Article 52, para. 5.
10. See, for example, ITU's Global Cybersecurity Index 2020, listing 167 countries 'with some form of' cybersecurity legislation (ITU, 2021: vii).
11. In this context, see Bart Custers, who discusses a 'right to a safe online environment' (Custers, 2022: 12).
12. Incidentally, it should be noted that there is absolutely no mention of the digital or on-line world in the Charter.
13. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data.
14. A regulation that benefits from direct applicability in Member State law is better suited for intra-EU harmonisation purposes, however a directive, in spite of the need to be incorporated into national laws through new domestic legislation, would also suffice.

REFERENCES

Custers, B. (2022), 'New Digital Rights: Imagining Additional Fundamental Rights for the Digital Era'. *Computer Law & Security Review*, 44, 105636, https://doi.org/10.1016/j.clsr.2021.105636.

ENISA (European Union Agency for Cybersecurity) (2021), 'ENISA Threat Landscape 2021: April 2020 to Mid July 2021', 27 October, https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021.

Fredman, S. (2007), 'The Positive Right to Security'. In B. J. Goold & L. Lazarus (eds.), *Security and Human Rights*. Oxford: Hart.

ITU (International Telecommunications Union) (2021), '2020 Global Cybersecurity Index', https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTM-E.

Lazarus, L. (2007), 'Mapping the Right to Security'. In B. J. Goold & L. Lazarus (eds.), *Security and Human Rights*. Oxford: Hart.

Papakonstantinou, V. (2022), 'Cybersecurity as Praxis and as a State: The EU Law Path Towards Acknowledgement of a New Right to Cybersecurity?', *Computer Law & Security Review*, 44, 105653, https://doi.org/10.1016/j.clsr.2022.105653.

Shue, H. (1996). *Basic Rights: Subsistence, Affluence, and U.S. Foreign Policy*, 2nd ed. Princeton, NJ: Princeton University Press.

van Kempen, P.H. (2013), 'Four Concepts of Security: A Human Rights Perspective'. *Human Rights Law Review*, 13(1), 1–23.

The Manipulation of Perceptions: Why Fake News and Disinformation Are a Cybersecurity Issue

Arturo Di Corinto

https://doi.org/10.53121/ELFTPS3 • ISSN (print) 2791-3880 • ISSN (online) 2791-3899

ABSTRACT

Disinformation has now become a cyber problem, given that its actors use digital tools to communicate false knowledge. Cyber disinformation tools range from an army of trolls, bots, and fake accounts, to the extensive use of memes, clickbait, and online news artfully created by digital guerrilla groups that also use software hacking techniques to manipulate information and its protagonists, not least the deep-fake videos and computational propaganda that travel on forums such as Reddit, Discord, and 4chan. Information manipulation campaigns that make widespread use of fake news to sow doubt and discontent in the population are spread on the main social networks; and the more time you spend online, the more likely you are to be exposed to commercial information and products.

ABOUT THE AUTHOR

Arturo Di Corinto is Professor of Digital Identity, Privacy, and Cybersecurity in the Faculty of Political Science, Sociology and Communication at Sapienza, University of Rome.

He is a former Director of Communication of the National Cybersecurity Lab, a visiting scholar at Stanford University, and has served as an information officer at the Presidency of the Council of Ministers. A broadcaster, writer and journalist, he has written some 2,300 articles and over 40 books.

INTRODUCTION

Fake news is a serious problem for democracies, whose lifeblood is public opinion. The danger is known: through fake news it is possible to manipulate public opinion and guide the decisions of governments, delegitimise people and institutions, and pollute the scientific debate. Fake news may have contributed to the defeat of Hillary Clinton in the race for the White House in 2016 (Gunther et al., 2018), as the result of a poisonous strategy that favoured, among others, the spread of the false news that the former US First Lady ran a paedophilia ring from the basement of a pizzeria. The false news was far more popular than its debunking by major established news sites. Former US President Donald Trump has repeatedly called several news outlets fake news sources: the *New York Times*, *Washington Post*, and CNN, to name a few. However, while the media outlets attacked by Trump were resilient in responding to the disinformation campaign, by recognising the publication of inaccurate news, we discovered that the fake news of the anti-Clinton campaign was produced by disinformation outlets headed by men close to Russian President Vladimir Putin and used thousands of fake accounts later removed from Facebook and Twitter.

We have witnessed much disinformation in recent years, and, among the most serious, we can cite those that polluted the Brexit campaign (Wylie, 2019). More recently we have read that '5G causes Coronavirus', that 'Drinking hot water can prevent COVID-19 infection' and that 'Throughout the emergency the government will record all Facebook and WhatsApp messages' (Poynter Institute, n.d.).

Created and disseminated on social networks, these hoaxes have gone viral through e-mail, chain letters, and chat groups

Created and disseminated on social networks, these hoaxes have gone viral through e-mail, chain letters, and chat groups and, to dismantle them one by one, the Poynter Institute has brought together about 100 fact-checkers from 45 different countries.

It is thanks to their work that we discovered that the 20-second clip on Facebook with a Pakistani woman in a burqa suffering from breathing difficulties came from India, not Pakistan, and that she had not contracted COVID-19. We also discovered that it was untrue that 'the wife and daughter of the Spanish president fled to Cuenca for quarantine' and that the WhatsApp message that went viral in Spain according to which 'Pope Francis asked believers to put a white handkerchief on the door to prevent the plague' was false.

More recently we have witnessed the spread of false news by Russian and Ukrainian media outlets after Russia's invasion of Ukraine for ideologically or politically motivated goals. Armies of trolls, website defacements, botnets, and false flags, are examples of what we call the 'weaponisation of disinformation' from both sides. However, addressing this politically motivated information war is not the goal of the chapter.

'CAN WE DEFINE FAKE NEWS?'

Given the diffusion of fake news articles – there are hundreds of them every day – it is good to remember that fake news is not the result of a journalistic error, but is designed to manipulate people, delegitimise institutions, and pollute public debate. Unlike satire, criticism, or personal opinion, fake news is built to deceive us by putting forth plausible facts that are built on the basis of partial truths and unverifiable events.

Despite its success, however, fake news can be recognised almost immediately. Fake news often appears on clickbait sites that typically have 'screamed' headlines, built to cause anger and indignation. Whoever writes them tries to trigger the emotional reactions of readers and spectators. But when we see a story that seems incredible or shocking, we can check if other accredited sources are reporting it with a quick online search. This is the first step to understanding whether, despite the juicy sensationalistic title that the hoaxes present, we should refrain from immediately sharing the item. Such articles generally have nothing to do with the title and we discover that the story is completely false and that evidence to support it is unavailable. Similarly, we are also learning to use common sense in the face of memes that have the advantage of spreading through a vehicle that synthesises a universe of meanings and beliefs into a single image and an overlaid slogan.

Fact-checking, common sense, and removal of hoaxes from social platforms are all means by which it is possible to combat fake news. And this is *the first piece of good news*. The bad news is the difficulty of identifying fake news posts. Fake news, put plainly, is also 'written and published' by someone, somewhere. Even if published in newspapers or websites, opinions are not fake news, satire is not fake news, and criticism and the right to exercise it are not fake news, given the condition that anyone who watches, listens to, or reads the news is aware of the form of communication used. And here comes *the first piece of bad news*. Ordinary people are unable to distinguish true news from fake. The reason is obvious: fake news is always a mixture of truth and falsehood; it often comprises plausible news, partial and twisted truths, and controversial and unverifiable facts.

The second piece of bad news is that people want to believe fake news. This happens when the news confirms their own prejudices, making it possible to explain complex facts without effort, legitimises pre-existing political and cultural orientations, or produces a group advantage. This is a well-known effect in literature called 'confirmation bias' (Quattrociocchi, Vicini, 2018). The 'bandwagon effect' is when we adapt to the majority and support the theses of the 'leader', when politicians' discourses favour the 'echo chambers' (Jamieson & Cappella, 2008) produced by the 'filter bubble' (Pariser, 2011). Moreover, the tendency to aggregate and trust the people most similar to us is a frequent behavioural mechanism. These are all effects of an information overload that leads us to simplify and trivialise the world around us.

If we add to these 'cognitive biases' the 'attention war' that the media fights with sensationalist facts

and shouted headlines and the extreme personalisation of the information produced by our daily interactions with the predictive algorithms of search engines and social networks (if you have clicked a certain news item, you will be likely to click a similar one and so they present it to you before others), we understand that fake news is not a phenomenon to be underestimated because it is we, the public, who want to believe it.

It is a basic principle of cognitive economics, but also the result of the wholly human tendency to always want to be right (Ferraris, 2017) that facilitates homophilia (we band together with those who resemble us and agree with us) and the 'backfire effect' (the aggressive reaction against what is far from our own beliefs and knowledge).

THE 'SPAMOUFLAGE DRAGON': A CASE STUDY

According to a report released by research firm Graphika, a network of bogus accounts criticised President Donald Trump across multiple platforms and broadcast positive images of then-Democratic presidential candidate Joe Biden during the presidential campaign in 2021 with the aim of attacking the White House.

The network of accounts, which Graphika called the 'Spamouflage Dragon' (Graphika, 2020) due to its apparent proximity to the Chinese government, released videos critical of the US government relating both to the executive order that forced the Chinese company Bytedance to sell TikTok, and to Trump's mismanagement of the pandemic, and addressing police brutality in the United States. Using YouTube, Facebook, and Twitter, the puppeteer behind the operation used groups of fake accounts to share and comment on the videos, giving the impression of genuine consensus around those posts. And, to make them credible, they also used accounts with profile pictures generated by artificial intelligence tools.

For Graphika, the company that provided the US Congress evidence of the political-electoral manipulation by Cambridge Analytica through Facebook, the 'Spamouflage' group (spam plus camouflage) is also the author of many fake news items that denigrated pro-democracy protesters in Hong Kong.

The behaviour of the Spamouflage Dragon brings us back to the reasons behind the effectiveness of disinformation: people are not keen to compare sources of information; they do not defend themselves from fake news contrarily to what happens with viruses; and the software that produces fake news is less and less distinguishable from humans.

Furthermore, messages deriving from *computational propaganda* that are also repeated with little or no variation are often received 'without filter' due to the credibility drawn from the 'similarity' between the interlocutors. We trust them because they make their way mainly to the people we know – family and friends – because 'they would never tell us a lie', and because they share our political and religious beliefs. Believing in fake news items justifies the choice to vote for political leaders who, using them, strengthen a bond with us based on common beliefs that we do not question out of respect for authority. The same happens with websites and newspapers due to the same principle, and few accept the idea that 'my newspaper' is a machine for consent production.

Thus, despite the usefulness of the efforts of journalists, governments, and organisations such as the Poynter Institute,[1] it is no longer enough to denounce fake news and the manipulation of perceptions conducted through their dissemination to stop them. The *infodemic*, or Coronavirus disinformation, is an example of this.

With the rising importance of social media and AI, fake news has become a cyber problem: once digitised, it can be reproduced at no cost, so it propagates quickly on digital networks; furthermore, it is generated by bots, as Viola Bachini and Maurizio Tesconi noted in their book *Fake People: Stories of Social Bots and Digital Liars*.

THE EUROPEAN UNION FIGHTS BACK

The COVID-19 crisis has clearly highlighted the threats and challenges posed by disinformation to our societies. The 'infodemic' created significant risks to personal and public health systems, the global economy, and all of society, but the European Union fought back.

The approach followed by the EU in the fight against disinformation has its roots in protecting freedom of expression and safeguarding an open democratic debate, with the aim of increasing transparency and accountability in the online environment and empowering its citizens. It goes hand in hand with the other objectives of the action plan for European democracy, namely the promotion of free and fair elections and the protection of media freedom and pluralism.

On 26 May 2021, the European Commission published guidelines on how to strengthen the code of good practices on disinformation, the first of its

kind worldwide, to make it a more effective tool in the fight against disinformation. The guidelines call for the code to be strengthened in the following areas:

- Greater participation and specific commitments: the Commission invites consolidated and emerging platforms active in the EU, stakeholders operating in the online advertising ecosystem, private messaging services, and all those who can bring resources or expertise to join the code to contribute to the effective functioning of the code. The strengthened code should include specific new commitments commensurate with the size of the signatories and the nature of the services they provide.
- Demonetise disinformation: platforms and actors active in the online advertising ecosystem need to take responsibility and collaborate more effectively to cut off funds to disinformation by exchanging information on ads rejected by one of the signatories as a source of disinformation, improving transparency and responsibility in relation to advertisements, and prohibiting the participation of those who systematically publish content that gets denied.
- Ensure integrity of services: the strengthened code should ensure full coverage of current and emerging forms of manipulation used to spread disinformation (such as bots, fake accounts, organised manipulation campaigns, and account misappropriation), and include specific commitments to ensure accountability and transparency in relation to the measures taken to reduce the effects of manipulation.
- Provide users with tools to identify and report disinformation: Users must have access to tools that allow them to better understand the online environment and to browse it safely. Signatories need to make their referral systems, i.e., how content is offered to users, transparent, and to take measures to mitigate the resulting risks, such as the viral spread of disinformation. Signatories should also provide users with accessible and effective tools and procedures to report disinformation and have access to an adequate and transparent redress mechanism to enforce their rights. The strengthened code should also make it possible to improve the visibility of reliable information of public interest and to warn users who have interacted with content qualified as false by fact-checkers.
- Increase coverage of fact-checking and provide researchers with greater access to data: the new code should provide for greater cooperation with fact-checkers and increase coverage of fact-checking in all EU countries and languages, as well as provide a solid framework for researchers to access data.
- A robust monitoring framework: the strengthened code should provide for an improved monitoring framework based on clear performance indicators to measure the results and effects of the measures taken by the platforms and the overall impact of the code on disinformation in the EU. The platforms should report regularly to the Commission on the measures taken and on the corresponding performance indicators. The platforms should provide disaggregated information and data at the level of each individual Member State and in standardised formats.

Finally, signatories should set up a Transparency Center where they can communicate which policies they have adopted and publish all relevant data and metrics for performance indicators. The guidelines also propose the establishment of a permanent task force chaired by the Commission and composed of signatories, representatives of the European External Action Service, the Group of European Regulators for Audiovisual Media Services, and the European Digital Media Observatory, which received over €11 million for the creation of eight regional poles to help run and expand its activities in the Member States. The task force, which will also draw on expert support, will contribute to the review and adaptation of the code based on technological, social, regulatory, and market developments.

FAKE NEWS IS MORE RESISTANT THAN VIRUSES

Some countries such as France have declared war on fake news. Italy has proposed a specific task force, while Germany has intervened several times to regulate social platforms.

However, research by Marco Cremonini, Nahid Maleki-Jirsarae and Samira Maghool of the State University of Milan (2019), confirms that fake news cannot be defeated for the simple reason that people use fake news to obtain personal advantages.

The scientific proof comes from the use of a new software for the simulation of propagation phenomena in social networks, which has shown how fake news and online hatred spread with much more complex mechanisms than those that determine the contagion of real viruses. This is because their propagation also depends on other human factors such

The COVID-19 crisis has clearly highlighted the threats and challenges posed by disinformation to our societies

as the desire to imitate others and the willingness to spread certain ideas.

> When a disease spreads, people become aware and react to protect themselves, limiting the infection. In the case of a fake news [item] online, the likelihood of it being disseminated depends not only on whether I believe it and want to imitate my friends, but also on the desire to spread the idea itself. For this, it is important to refine our models more and more, in order to better understand the dynamics and develop more effective strategies to counteract negative information by favoring positive information.

MANIPULATION OF PERCEPTIONS, A EUROPEAN BATTLE

We assume that the effects of disinformation cannot be countered without addressing four problems: cognitive biases, platform's business models, mal-information, and nation-state political agenda during a crisis. Nevertheless, to counter computational propaganda, disinformation, and fake news, the European Union set up several important initiatives (European Commission, n.d.):

- The Code of Practice on Disinformation, a set of worldwide self-regulatory standards for industry
- The European Digital Media Observatory, a European hub for fact-checkers, academics, and other relevant stakeholders to support policy-makers
- The action plan on disinformation
- The European Democracy Action Plan to develop guidelines for obligations and accountability of online platforms in the fight against disinformation
- The Communication on 'Tackling Online Disinformation: A European Approach', offering a collection of tools to tackle the spread of disinformation and ensure the protection of EU values

Among the array of tools used to cope with disinformation, the regulation of online platforms has been high on the European agenda in recent years. In December 2020, the European Commission presented a digital services package comprising the Digital Services Act (DSA) and the Digital Markets Act, to increase the transparency and accountability of platforms.

Noncompliance with these rules could result in fines for the tech giants. Nevertheless, the ambitious proposals have been criticised for their lack of focus on the rights of individual users and are missing a key point: the blurred line between opinion and what we call information. Balancing citizens' rights to express themselves and the need for a safer and more accountable information ecosystem is the challenge. That's why we've been waiting for the DSA to address important items that have not been agreed on yet, including the ban on targeted ads, dark patterns, access to data, obligations for very large online search engines, and more. This may also have been delayed by the war in Ukraine. Finally, on 23 April 2022, a provisional political agreement was reached on the DSA between the Council and the European Parliament, creating the world's first digital regulation to protect the digital space against the spread of misleading content and, to ensure the protection of users' fundamental rights, and it will apply to all online intermediaries providing services in the EU.

The obligations are intended to be proportionate to the nature of the services concerned and tailored to the number of users, meaning that very large online platforms (VLOPs) and very large online search engines (VLOSEs) will be subject to more stringent requirements. This means that 'Services with more than 45 million monthly active users in the European Union will fall into the category of very large online platforms and very large search engines'. But, 'To safeguard the development of start-ups and smaller enterprises in the internal market, micro and small enterprises with under 45 million monthly active users in the EU will be exempted from certain new obligations'.

Governance

In order to ensure effective and uniform implementation of requirements under the DSA, the Council and Parliament have decided to confer

Among the array of tools used to cope with disinformation, the regulation of online platforms has been high on the European agenda in recent years

on the Commission exclusive power to supervise VLOPs and VLOSEs for the obligations specific to this type of actor.

They will be supervised at European level in cooperation with the Member States. This new supervisory mechanism maintains the country-of-origin principle.

Online marketplaces

Given the important role played by these actors in the daily lives of European consumers, the DSA will impose a duty of care on marketplaces vis-à-vis sellers who sell their products or services on their online platforms. Marketplaces will have to collect and display information on the products and services sold to ensure that consumers are properly informed. (European Commission, Digital Services Act)

Systemic risks of very large platforms and search engines

The DSA introduces an obligation for very large digital platforms and services to analyse systemic risks they create and to carry out risk reduction analysis.

This analysis must be carried out every year and will enable continuous monitoring aimed at reducing risks associated with:

- dissemination of illegal content
- adverse effects on fundamental rights
- manipulation of services having an impact on democratic processes and public security
- adverse effects on gender-based violence, and on minors and serious consequences for the physical or mental health of users

Dark patterns

'For online platforms and interfaces covered by the DSA, the co-legislators have agreed to prohibit misleading interfaces known as "dark patterns" and practices aimed at misleading users'.

Recommender systems

Recommendation systems are found in many uses of online users, allowing them to quickly access relevant content. Transparency requirements for the parameters of recommender systems have been introduced in order to improve information for users and any choices they make. VLOPs and VLOSEs will have to offer users a system for recommending content that is not based on their profiling.

Crisis mechanism

In the context of the Russian aggression in Ukraine and the particular impact on the manipulation of online information, a new article has been added to the text introducing a crisis response mechanism. This mechanism will be activated by the Commission on the recommendation of the board of national Digital Services Coordinators. It will make it possible to analyse the impact of the activities of VLOPs and VLOSEs on the crisis in question and decide on proportionate and effective measures to be put in place for the respect of fundamental rights.

The EU communication regarding the adoption of the DSA says:

> The provisional agreement reached is subject to approval by the Council and the European Parliament. From the Council's side, the provisional political agreement is subject to approval by the Permanent Representatives Committee (Coreper), before going through the formal steps of the adoption procedure. (European Council, 2022)

THE SWEDISH PSYCHOLOGICAL DEFENSE AGENCY

On 1 January 2022, Sweden launched the first Psychological Defense Agency to combat disinformation. It operates in times of peace and war, works long-term and preventively, through training and information, conducting research, and collaborating with state agencies and other actors at the international level.

There was a similar attempt in Italy, but it was not an agency. Then Italian Minister of the Interior

Marco Minniti had decided in 2018 to create a government task force to combat false news. The project didn't start, but Europe started the Action Plan against Disinformation. In Italy, a consortium led by Luiss University was awarded the €1.4 million tender for the Italian Digital Media Observatory of the European Union.

In short, the message is loud and clear: be careful when we find ourselves sharing unverified information. A recent Carnegie Endowment for International Peace report found that disinformation on COVID-19 remains high in Europe, reflecting the dynamics of the infodemic, and of different conspiracy theories that attribute the spread of unexplained diseases and events to the plans of unspecified powers aiming at global domination.

The Swedish Psychological Defense Agency is the first government authority in the world created to protect a country from disinformation. Headquartered in Karlstad and headed by former ambassador Henrik Landerholm, it is a state intelligence agency 'for the proactive defense of information' intended as a resource of national interest and has the aim of 'safeguarding society open and democratic, the free formation of public opinion, the freedom and independence of Sweden'. To achieve this goal, they're using all known tools to identify, analyse, and prevent disinformation aimed at unduly influencing citizens' perceptions, behaviours, and decision-making processes.

But be careful not to confuse bad information with disinformation. Bad information, or misinformation, refers to erroneous information put out by journalists by mistake or to support the political-editorial line of their publishers, while disinformation is always the result of information manipulation campaigns organised centrally by specialised entities that usually weaponise fake news to propagate misleading content. Bad information and disinformation can both create anxiety, hatred, and fear making society more vulnerable. For this reason, according to the agency, a real work of 'psychological prevention' is needed, with the aim to stimulate the democratic antibodies of society, protect the population's health, social functioning, and national values such as democracy, law, freedom, and human rights.

It is no coincidence that the agency makes its appearance at this time – Sweden will hold its general elections in September 2022, and is concerned about the effects that fake news and conspiracy narratives can have on the democratic process, which has already been targeted, according to Landerholm, by disinformation campaigns by Russia and China.

The agency's goal, however, is ambitious for the reasons stated above: 1) most people do not know how to recognise true news from false; 2) individuals are inclined to believe in hoaxes when they confirm their prejudices; 3) disinformation has exponential growth patterns because those affected do not seek to protect themselves but become the bearers of it to obtain advantages and recognition in the group to which they belong.

CONCLUSION: MISINFORMATION, A CYBER PROBLEM

The creators of the agency must have read about the so-called Gerasimov doctrine (Cristadoro, 2022), named after the famous Russian Army general who theorised how to overthrow the soft power that the United States exerts on the global imagination through cinema and social networks, using Netflix, Facebook, Instagram, Twitter, and WhatsApp as weapons of mass persuasion.

The undeclared reason for the agency's mission is the awareness that disinformation has now become a cyber problem given that its actors use digital tools to shake people's confidence in their beliefs. These tools range from armies of trolls, bots, and fake accounts, to the extensive use of memes, clickbait and online news artfully created by digital guerrilla groups that also use software hacking techniques to manipulate information and its protagonists, not least the deep-fake videos and computational propaganda that travel on forums such as Reddit, Discord, and 4chan. Information manipulation campaigns that make broad use of fake news to sow doubt and discontent in the population are spread on the main social networks, social environments engineered to encourage people's engagement and the polarisation of opinions so that they remain as long as possible on the platforms, increasing their value for advertisers: the more time you spend online, the more likely you are to be exposed to commercial information and products.

We must accept the idea that fake news is the poisoned fruit of 'the democracy of opinions', established by blogs and social networks that allow us to say anything and its opposite, to the detriment of every criterion of decency, respect, and objectivity. But fake news is also the result of decades in which institutions have neglected their social, regulatory, and filtering function in the conflicts that animate society. It is the result of media outlets that have abandoned their role in maintaining civil values,

the role of the watchdogs of democracy, watering down their critiques of power and favouring the interests of the few to the detriment of the many. It is also the result of a structural mutation of audiences that are now global, fragmented, and capable of criticising the media establishment thanks to the power of online publishing.

Fake news can be countered, though. But how do you know if a news item is a hoax?

We have said that generally fake news is plausible news, sometimes fictionalised and seasoned with curious or singular details. Here our cultural endowment and knowledge of the facts of the world must come to our aid. But there are also other ways to determine when we are faced with fake news. And they all focus on the media literacy of news consumers.

Therefore, it is important to promote different and credible sources of information across all media, including social networks; to protect intermediaries from any form of responsibility for the content posted by users, to promote literacy in the use of media and digital technology; and to disseminate, even at the government level, reliable information on matters of public interest.

Media pluralism, fact-checking, information literacy, and the fight against functional illiteracy are the resources to call upon to combat disinformation that hinges on fake news. It is up to journalists to verify the facts, schools are responsible for training and education in the critical spirit, institutions have to intervene to reduce social anger, and guarantee authorities have the role of enforcing the right and duty to information, being aware that it will be an uneven and long-lasting battle.

Other attempts, apparently close at hand, such as fact-checker task forces, can be useful in hitting the disinformation centres, but without the collaboration of all the subjects listed, they are doomed to fail. This means that information alone may not be enough to stop fake news. It is a cultural battle to be fought all together, because of the risks of transforming the digital ecosystem into a world in which distinguishing the true from the false will be increasingly difficult. Consider fake videos of politicians and public figures making statements of a certain weight. It happened in April 2022, when a fake speech by Ukraine President Volodymyr Zelensky was spread to weaken people's resistance after the Russian invasion.

But we must be careful, as some analysts have written, not to find another Big Brother around the corner. Fear of a police state is invoked by Singapore's anti-fake news law, for example. In the city-state, fake news is governed by the Law on Protection from Online Falsehoods and Manipulation, and has already been applied to politicians, bloggers, and dissidents who weren't spreading fake news but airing personal opinions.

REFERENCES

Bachini, V. & Tesconi, M. (2020). *Fake People: Storiee di social bot e bugiardi digitali.* Turin: Codice Edizioni.

Cappella, N., & Hall Jamieson, K. (2008). *Echo Chamber: Rush Limbaugh and the Conservative Media Establishment*. Oxford: Oxford University Press.

Cristadoro, N. (2022). *La dottrina Gerasimov. La filosofia della guerra non-convenzionale nella strategia russa contemporanea*. Solarussa : Edizioni il Maglio.

European Commission (n.d.) 'Tackling Online Disinformation', https://digital-strategy.ec.europa.eu/en/policies/online-disinformation.

European Council (2022) 'Digital Services Act: Council and European Parliament Provisional Agreement for Making the Internet a Safer Space for European Citizens', 23 April, https://www.consilium.europa.eu/it/press/press-releases/2022/04/23/digital-services-act-council-and-european-parliament-reach-deal-on-a-safer-online-space.

Ferraris, M. (2017). *Postverità e altri enigmi*. Bologna: Il Mulino.

Graphika (2020) 'Spamouflage Dragon Goes to America', 12 August, https://graphika.com/reports/spamouflage-dragon-goes-to-america.

Gunther, R., Beck, P. A., & Nisbet E. C. (2018) 'Fake News May Have Contributed to Trump's 2016 Victory', 8 March, https://www.documentcloud.org/documents/4429952-Fake-News-May-Have-Contributed-to-Trump-s-2016.html.

Maghool, S., Maleki-Jirsaraei, N., & Cremonini, M, (2019). 'The Coevolution of Contagion and Behavior with Increasing and Decreasing Awareness'. *Plos One*, 3 December, https://doi.org/10.1371/journal.pone.0225447.

Pariser, E. (2011). *The Filter Bubble: What The Internet Is Hiding From You*. London: Penguin UK.

Poynter Institute (n.d.) 'The CoronaVirusFacts/DatosCoronaVirus Alliance Database', https://www.poynter.org/ifcn-covid-19-misinformation/page/2.

Quattrociocchi, W., & Vicini, A. (2018). *Liberi di crederci. Informazione, internet e post-verità*. Turin: Codice Edizioni.

Wylie, C. (2019). *Mindf*ck: Cambridge Analytica and the Plot to Break America*. New York: Random House.

The pervasiveness of digitalisation has made cybersecurity no longer only a matter of concern for computer scientists but a central factor in securitising our future digital society.

Recently, both the Covid-19-related rise in the use of digital tools and the conflict in Ukraine have raised questions about the security of cyberspace and how the European Union should deal with this. To clarify how to better regulate the future, it is necessary to assess what policymakers can do to foster a constructive approach between the Member States so that they can keep up with the challenges of cyberspace.

This study, edited by Professor Luigi Martino and Nada Gamal, approaches the topic from a multidisciplinary point of view, considering critical infrastructures, skills, strategic autonomy, artificial intelligence, cybercrime, privacy, and the use of space. Starting from an EU perspective, the authors examine the regulatory achievements in this field and consider best practice for the implementation of rules and standards. Based on a holistic approach, the explanations and policy recommendations in the various chapters aim to define the role of the European Union in this dynamic and constantly changing world of cyberspace.

Daniel Kaddik, ELF Executive Director

ISBN 978-2-39067-035-3

liberalforum.eu