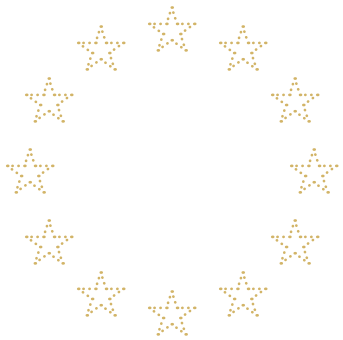
Agora FIC

MAKING CYBERSECURITY THE CORNERSTONE OF EUROPEAN DIGITAL SOVEREIGNTY



28 Recommendations for the
French Presidency of the Council of the European Union
on Digital Security and Regulation

SEPTEMBER 2021

ABOUT

The FIC Agora is the strategic think tank of the International Cybersecurity Forum (FIC). It brings together major economic, academic and political decision-makers and aims to foster public debate on major challenges in digital technology.

This report was prepared by a working group led by **Army General (Rtd) Marc Watin-Augouard**, founder of the FIC, and **Mr Guillaume Klossa**, founder of EuropaNova and former special advisor to the Vice President of the European Commission. The teams of Avisa Partners in Paris and Brussels –including **Guillaume Tissier, Pauline Massart, Paul Azibert, Suzanne McNamara, Clément Rossi** and **Julien Tran Van Nhieu**– also made contributions to the preparation of this report.

It is based on discussions with personalities from national and European institutions, as well as from the industrial and academic spheres, and more broadly from civil society.

Agora FIC

The FIC has been co-organised by Avisa Partners and the French Gendarmerie since 2013

www.forum-fic.com

OVERVIEW

AREA	NO.	TITLE	RECOMMENDATION
TALENTS & SKILLS 	1	PROMOTE DIGITAL ACCULTURATION AMONG EUROPEAN DECISION-MAKERS	Develop a core training scheme for senior officials and political and economic decision-makers.
	2	INCORPORATE DIGITAL TECHNOLOGIES AND CYBERSECURITY INTO UNIVERSITY COURSES	Develop an e-Erasmus programme and standardised certification based on the Test of English for International Communication (TOEIC) model.
	3	BRING SUPPLY AND DEMAND INTO ALIGNMENT FOR DIGITAL JOBS	Further promote *"careers in digital technologies"* and *"digital technologies in careers"* with suitable communication and attractive HR policies.
DIGITAL DIPLOMACY & STABILITY 	4	PROMOTE A EUROPEAN VISION OF INTERNATIONAL CYBERSPACE LAW	Have European institutions endorse the recommendations of the Paris Call for Trust and Security in Cyberspace.
	5	ENHANCE THE EU'S CYBER DIPLOMACY TOOLBOX	Enhance the tools in the Cyber Toolbox: requests for information and corrective actions, intelligence sharing, forensic capabilities, blacklist, etc.
	6	BRING ABOUT REGULATION OF THE ZERO-DAY VULNERABILITY MARKET	Draw up a blacklist of companies that have sold entities to certain regimes and encourage cooperation between vulnerability owners and researchers.
	7	DEVELOP A COMMON UNDERSTANDING OF CYBER THREATS	Strengthen the collective system of cyber situational awareness and operationalise the mutual defence clause of the Member States.
MILITARY CYBER DEFENCE 	8	STRENGTHEN THE EU'S MILITARY CYBER DEFENCE	Establish a forum of Cyber Commanders and support the creation of a European network of military computer emergency response teams (CERTs).
	9	STREAMLINE EUROPEAN CYBER DEFENCE THROUGH EU–NATO COMPLEMENTARITY	Enhance the sharing of best practices between the EU and the North Atlantic Treaty Organization (NATO) and ensure that the two institutions complement each other effectively.
FIGHT AGAINST CYBERCRIME 	10	BUILD CAPACITY IN THE FIGHT AGAINST CYBERCRIME	Create a European public prosecutor's office specialising in cybercrime and promote the creation of a European skills network.
	11	ARRIVE AT A BALANCED SOLUTION ON PRESERVATION OF EVIDENCE	Finalise draft legislation relating to the "e-evidence" regulation according to the prerogatives of the judicial authority and fundamental personal data principles.
	12	GIVE NEW IMPETUS TO THE BUDAPEST CONVENTION	Promote the ratification of the Budapest Convention by non-Member States of the Council of Europe and pursue adaptation efforts.
	13	STRENGTHEN THE FIGHT AGAINST ILLEGAL CONTENT	Establish a signature database of illegal content and strengthen the place of trusted players.

AREA	NO.	TITLE	RECOMMENDATION
CYBERSECURITY & RESILIENCE 	14	IMPOSE SECURITY *"BY DESIGN"*	Accelerate the implementation of European certification schemes and bring about international adoption of the principle of responsibility of systemic manufacturers and publishers.
	15	DEVELOP A EUROPEAN CAPABILITY FOR RESPONSE TO MAJOR INCIDENTS	Finalise the establishment of the new EU Joint Cyber Unit, drawing inspiration from the existing EU Civil Protection Pool.
	16	STRENGTHEN THE PROTECTION OF EU INFORMATION SYSTEMS	Strengthen the capabilities of the Computer Emergency Response Team for the EU institutions, agencies and bodies (CERT-EU) and create a mandatory *"cybersecurity"* qualification for all EU officials.
	17	STRENGTHEN CRITICAL INFRASTRUCTURE PROTECTION	Finalise the draft NIS2 Directive with the inclusion of the entire digital product supply chain and the incorporation of a mechanism for regulating digital service providers.
	18	ENCOURAGE COORDINATED DISCLOSURE POLICIES	Impose policies of coordinated disclosure of vulnerabilities on *"essential entities"* and *"important entities"* as defined in the draft NIS2 Directive.
	19	IMPROVE CROSS-BORDER CYBERSECURITY	Create experimental cross-border CERTs, whether generalist or sector-specific (e.g. in the energy sector).
INDUSTRIAL POLICY 	20	CREATE A DIGITAL TRACEABILITY INDICATOR	Establish an indicator of traceability of digital products and services based on the transparency of the value chain used, compliance with the General Data Protection Regulation (GDPR) and the location of the storage and main processing of data.
	21	REVITALISE THE EUROPEAN STANDARDISATION SYSTEM	Apply the European certification framework established by the Cybersecurity Act and create a security equipment certification with EU-wide validity.
	22	MOBILISE PUBLIC AND PRIVATE PURCHASING	Institute a *"Buy Digital European Act"* for all public purchases and establish tax credits and overamortisation mechanisms for private purchases.
	23	STRENGTHEN PUBLIC AND PRIVATE INVESTMENT	Adapt the conditions proposed by the European Investment Bank (EIB) and the European Investment Fund (EIF) to small and medium-sized enterprises (SMEs) and intermediate-sized enterprises and mobilise European Innovation Council (EIC) funds.
	24	FACILITATE TECHNOLOGY TRANSFER	Relax intellectual property conditions and financial terms governing technology transfer from academia to companies.
	25	IMPROVE SUPPORT FOR INNOVATION	Ensure better coordination and evaluation of existing programmes and afford a special place to *"deep tech"*.
	26	BRING ABOUT THE EMERGENCE OF EUROPEAN LEADERS IN CLOUD COMPUTING	Forge industrial alliances within the new industrial policy of the European Commission using the *"Important Project of Common European Interest"* (IPCEI) statute.
	27	PROMOTE THE DEVELOPMENT OF A EUROPEAN DIGITAL IDENTITY	Promote the adoption of the new version of the electronic identification, authentication and trust services regulation (eIDAS Regulation) and improve the adoption of digital identities in the regulated private sector.
	28	ACCELERATE IMPLEMENTATION OF REGULATION OF SYSTEMIC PLAYERS	Strictly apply competition law to digital markets through a robust Digital Markets Act (DMA) and endow the European Commission with an economic intelligence service.

SUMMARY

[...] Because Europe is demonstrating a newfound vitality, because envious eyes are being cast on a market of 320 million people with a high standard of living, there are those who have no compunction about accusing us of digging moats and building drawbridges. Let us not be taken in by this. Our accusers are those who would like to see an open Europe with no common policy, no reactions, no political will. Our accusers are those who, within their own walls, enact protectionist trade, laws or devise ways of slowing down the first tentative moves towards market liberalisation. We would say this to them: the single market will be open, but it will not be given away.

JACQUES DELORS
TO THE EUROPEAN PARLIAMENT
17 JANUARY 1989

INTRODUCTION

The construction of a digital Europe is under way. Even a few decades ago, such a thing was not possible, because digital transformation was not happening on nearly the scale that it is today. Now, it is gathering momentum as a more proactive European Union (EU) is taking more and more steps towards a digital industrial strategy for its 27 Member States.

The dream of a Europe able to offer its own array of digital products is, however, nothing new. The Unidata consortium, which brought together the International Computing Company (CII, France), Philips (the Netherlands) and Siemens (Germany), was formed in 1970 with the aim of creating a European heavyweight to compete on an industrial dimension with the United States. However, France's unilateral withdrawal a few years later killed the initiative's momentum. While this effort generated a number of frustrations, it now sheds light on the future and gives indications of what needs to be accomplished: **the forthcoming French Presidency of the Council of the European Union must be characterised by wilfulness tinged with humility.**

Half a century later, European ambitions fit into a new strategic context influenced by two digital superpowers, the United States and China. This dynamic risks eventually marginalising the European continent, and yet the latter challenges this duopoly as the world's second largest economic power. The EU has distinguished itself on the international scene through its regulation of digital technologies (Directive on privacy and electronic communications, eIDAS Regulation, General Data Protection Regulation [GDPR], etc.). Yet, it remains a *"colony of the digital world"* when it comes to industry, given its destitution in certain technologies that are shaping the digital age, including major platforms, cloud computing and semiconductors, and its inability to develop a European public procurement system capable of competing with the corresponding national systems of the United States and China.

The COVID-19 pandemic has heightened awareness of Europe's need to evolve from a *"regulatory"* power to a *"creative"* one. This pursuit must not lead Europe to pull back on the regulatory front, as evidenced by the forthcoming Digital Markets Act (DMA), Digital Services Act (DSA) and Data Governance Act (DGA). **The pandemic has highlighted not only the need for control of geopolitical and economic dependencies, but also the requirement of *"digital sovereignty"* from the perspective of strategic autonomy.** Thus the Commission has named digital among 14 priority *"industrial ecosystems"* for recreating value chains and supply chains on the single market.

In April 2021, to provide itself with the means to realise its ambitions, the EU allocated a budget of €7.6 billion to its Digital Europe Programme (2021-2027)[1]. This is intended to achieve not only competitiveness and technological sovereignty, but also widespread **deployment of digital technologies for the benefit of EU citizens, companies and government entities.** This effort is rooted in investments in four priorities, which constitute as many strategic areas: high-performance computing, artificial intelligence, *"advanced digital skills"* and cybersecurity.

In matters of cybersecurity, the key to Europe's digital sovereignty, the continent quickly grasped the extent and ever-evolving nature of the risks involved. In 2007, the cyberattack targeting Estonia was a major shock that spurred several Member States to design a dedicated strategy. While the EU looked first at critical infrastructure, then at information networks and systems, the proliferation and sophistication of attacks incited it to go further so as not to become the *"weak link in the fight against this global threat.*[2]*"*

1. Regulation (EU) 2021/694 of the European Parliament and of the Council of 29 April 2021.
2. Speech by Jean-Claude Juncker at the Tallinn Digital Summit in September 2017.

With this, it passed the Cybersecurity Act (2019), which laid the foundation for a common approach to cybercrime, *"the crime of the 21st century."* This designation is all the more accurate in view of cyber conflict, often of State origin or inspiration, that takes advantage of the absence of universally recognised governance.

In December 2020, against this backdrop of uncertainty, the European Commission presented its new Cybersecurity Strategy. This roadmap is meant not only to develop collective resilience against cyber risk, but also to render the digital tools and services available to citizens and businesses in Europe secure and reliable. It will enable the EU to assert itself as a key player in cybersecurity standards and norms as well as afford it a better framework for its international cooperation to promote an *"open, stable and secure"* cyberspace. This must be based on European values: democracy, rule of law, human rights and fundamental freedoms. Several concrete measures in terms of regulation, investments and actions are planned in this regard.

The European concept of digital transformation must put people back at the heart of debate and action, building on the values shared by European citizens. These citizens must be players in a profound, *"historic"* transformation of a society influenced by a digital sphere that is now enmeshed in all environments: land, sea, air and space.

Hyperconnection, coupled with artificial intelligence and big data, is growing exponentially, conferring a power unmatched in history on data processing and data use. The expected growth of cloud computing is such that the cloud alone will be the *"digital sphere"* of the future.

Citizens have high hopes for the progress anticipated. At the same time, they fear becoming slaves of a system that works against their digital self-determination by conditioning them through algorithms, invading their privacy and severely undermining their freedoms of opinion and decision-making with manipulation of information. The semantic layer of the digital sphere will undoubtedly be the centre of gravity, in every sense of the term, of the cybersecurity of tomorrow.

It is, of course, important for the European discourse to focus on uses, technologies (in particular disruptive ones), regulations, and organisations. Above all, however, what we need are actions that are likely to foster trust but also mobilise better informed, better trained Europeans. If Europe aspires to maintain its place in the world, human resources will have to be its greatest assets. The COVID-19 pandemic has disrupted citizens' daily lives, called once-certain matters into question and spawned doubt, particularly with regard to the capacity of national or European elites to respond to unprecedented seismic shifts in economic and social matters. Digital technologies applied to health have undoubtedly become the most suitable vector for reviving a collective consciousness.

Before thinking about the rest of the world, Europe must act for itself, while refraining from having its 27 Member States work in isolation. The time has come for it to offer a new way forward and use its voice to address the rest of the world and attract the attention of other States that do not wish to enter a new paradigm dominated by two giants. This effort must be directed at countries in other continents—Africa, Latin America and Asia—which share common values and interests. Brazil, India, South Africa, Japan, South Korea and Taiwan, not to mention the Francophonie, are partners with which this strategy can be developed. This should not thwart the transatlantic dialogue but balance it.

From 1 January to 1 July 2022, France will hold the rotating Presidency of the Council of the EU, succeeding Portugal and Slovenia and preceding the Czech Republic. This presidency is part of a collective movement that the 27 Member States have engaged in for several years. It would be pretentious to break with this movement. However, France, a founder of the EU, continues to exert powerful influence both within the Union and elsewhere in the world. Some criticise France, but many want to hear what the country has to say.

France will undoubtedly have to make progress in the collective response to the question of *"how"*, through ways and means enabling the implementation of decisions that have already been made and the speeding up of the rollout timetable with a stimulating dialogue. However, it must above all contribute to a new impetus, the beginnings of which are emerging, by answering the question of *"why"*. A strategic vision must be built on the basis of meaning. During the French Presidency of the Council of the EU, France must humbly leverage its capacity for influence to build strong momentum that the Czech Presidency will have to perpetuate. The development of the discourse is a political responsibility, but the content of this discourse will be all the richer if proposals from civil society are taken into consideration.

The **International Cybersecurity Forum (FIC)** is a forum that, since its origins, has aspired to bring together the digital ecosystem by transcending divisions tied to borders and developing public–private partnerships, with a resolute focus on service to humanity. These things are embedded in the FIC's DNA.

In this ambitious spirit, the FIC lays out the following proposals. These proposals are not limited to the field of cybersecurity, which cannot be dissociated from a more overarching concept of digital transformation. Cybersecurity allows digital technologies to flourish, and digital technologies contribute to cybersecurity.

Although this is not directly addressed in this reflection, cybersecurity and sustainability are two components of resilience, and a digital Europe cannot be designed without a requirement of sustainability.

The political discourse on digital technology can no longer be reduced to the objective of developing *"new uses"* and the internal market.

FOUNDATIONAL TEXTS

DIGITAL EUROPE

- Directive on privacy and electronic communications
  12 July 2002
- Regulation on electronic identification and trust services for electronic transactions in the internal market—eIDAS Regulation
  23 July 2014
- Regulation on the protection of natural persons with regard to the processing of personal data and on the free movement of such data—General Data Protection Regulation (GDPR) *27 April 2016*
- Shaping Europe's digital future *19 February 2020*
- A European strategy for data *19 February 2020*
- Report on the safety and liability implications of Artificial Intelligence, the Internet of Things and robotics *19 February 2020*
- White Paper On Artificial Intelligence - A European approach to excellence and trust *19 February 2020*
- Updating the 2020 New Industrial Strategy: Building a stronger Single Market for Europe's recovery
  5 May 2021

EUROPE OF CYBERSECURITY

- Directive on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection
  8 December 2008
- Directive concerning measures for a high common level of security of network and information systems across the Union *6 July 2016*
- Regulation on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification, also called the Cybersecurity Act
  17 April 2019
- Regulation concerning restrictive measures against cyberattacks threatening the Union or its Member States *17 May 2019*
- The EU's Cybersecurity Strategy for the Digital Decade
  16 December 2020

RECOMMENDATIONS

TALENTS & SKILLS

For Europe, the development of digital talents and skills determines the digital transformation of its economy and the development of European citizenship—and therefore European identity. In the future, nearly 9 out of 10 jobs will require mastery of certain digital skills, while citizens will go about much of their participation in democracy in the digital sphere.

The talents and skills required are of two orders:

- Cognitive, emotional and social, representing a necessary foundation for the use of digital technology. This means that acculturation is essential in the fight against the phenomenon of fake news.

- Technical, enabling the safe use of digital technologies, whether these are skills related to the use of technologies or the production of equipment and services incorporating digital technology. The EU Digital Competence Framework (DigComp) identifies 21 skills and talents distributed across five domains (information literacy, communication, content creation, safety, and problem-solving).

1 PROMOTE **DIGITAL ACCULTURATION** AMONG **EUROPEAN DECISION-MAKERS**

BACKGROUND Digital transformation is disrupting our society. Because it is characterised by the infinitely large, the infinitely small and the infinitely fast, it takes place outside the traditional space/time framework and is developing at a speed independent of the classic pace of political, administrative and financial decision-making. The world is accelerating, and it waits for no one. Traditional organisations are being put to the test with the emergence of systemic, global and reticular organisations. Elites that have been more used to following than promoting digital transformation are now facing a disruption of their professional practices. On a short-term basis, the *"disconnection of elites"*[3] could thwart the development of the digital society and bring about a generational rift and, with it, a source of tension. European decision-makers —public or private, civilian or military— must *"embrace their century"* and share a collective vision based on a common frame of reference.

OBJECTIVE Establish, in each Member State that wants it, training for decision-makers based on the model of the Institute of Advanced Studies in National Defence (IHEDN) in France. Similar training could be organised for all senior civilian and military officials working in European Union institutions.

RECOMMENDATIONS

› Develop a core training scheme for senior officials and political and economic decision-makers. This will guide national training courses, which will take into account the particularities of each Member State. The core scheme could be developed jointly with the College of Europe with the support of researchers from the European Union Institute for Security Studies (EUISS) and from the European Security and Defence College (ESDC), building on the ESDC's experience in creating a European cyber defence training course for the militaries of the 27 Member States.

› Promote exchanges among auditors in Member States with a view to eventually establishing a European *"cyber community"* with a shared vision. A common massive open online course (MOOC) could be the first stage of development of a more sophisticated system.

3. Laure Belot, *La déconnexion des élites* [The Disconnection of Elites], Les Arènes, 2015.

INCORPORATE **DIGITAL TECHNOLOGIES & CYBERSECURITY** INTO **UNIVERSITY COURSES**

2

BACKGROUND The lack of digital skills in Europe will increase in the coming years. The European Commission has mentioned that, by 2025, there will be 500,000 unfilled jobs in this field in general and in cybersecurity, data science and artificial intelligence in particular. This shortage could represent for Europe a looming bottleneck in growth and jobs, a barrier to innovation and a serious risk of loss of control of technology.

Digital transformation has an impact on all careers. Its impact is not limited to technology-oriented lines of work; it affects all sectors of the humanities and social sciences (*"digital humanities"*), services and industry. Today, it is possible to graduate without ever having received training in digital technology, digital transformation or the risks that they entail. However, cyberattacks affect societies on every level, from ordinary citizens to States.

OBJECTIVE Strengthen initial and continuing training to come to a common understanding of the challenges of digital transformation and the associated risks. There is an urgent need to include acculturation to digital affairs and security, in particular in high-level training, in all training courses at EU schools and universities. Specialised courses will aim to increase exchanges among universities within Europe to arrive at a common European awareness of cyber threats.

RECOMMENDATIONS

- Provide awareness sessions regarding online security as well as coding instruction to young people starting in primary school. This foundation will then be strengthened in secondary school.
- Develop a standardised European certification ensuring a minimum level of digital knowledge among all students, regardless of the courses they pursue. This certification would be based on the Test of English for International Communication (TOEIC) and Test of English as a Foreign Language (TOEFL) models, among others. It would consist of multiple levels, corresponding to secondary education (Level 1) as well as higher education consisting of undergraduate studies (Level 2) and graduate studies (Level 3). It would recognise basic mastery of essential tools, but above all it would validate knowledge of their uses, operation and associated risks. The certification is intended to establish a *"general digital culture"* —one that is not solely focused on technical knowledge— and to ensure a minimum level of digital skills across all sectors of the economy. It would equip workers with initial awareness of cybersecurity issues and could attract girls and women to technological careers.

- Promote all non-technical skills (in the human and social sciences) related to cybersecurity through the organisation of competitions and challenges, in particular the European Cyber Security Challenge (ECSC) of the European Union Agency for Cybersecurity (ENISA).
- Develop a mapping of cybersecurity training available in each Member State in Europe, based on the SecNumEdu model of the French National Agency for the Security of Information Systems (ANSSI). This initiative would precipitate exchanges among universities within Europe, with dedicated scholarships that will eventually facilitate the interoperability of operational technical procedures and methodologies (incident detection and response) among European countries starting with initial training courses.

BRING **SUPPLY & DEMAND** INTO ALIGNMENT FOR **DIGITAL JOBS**

3

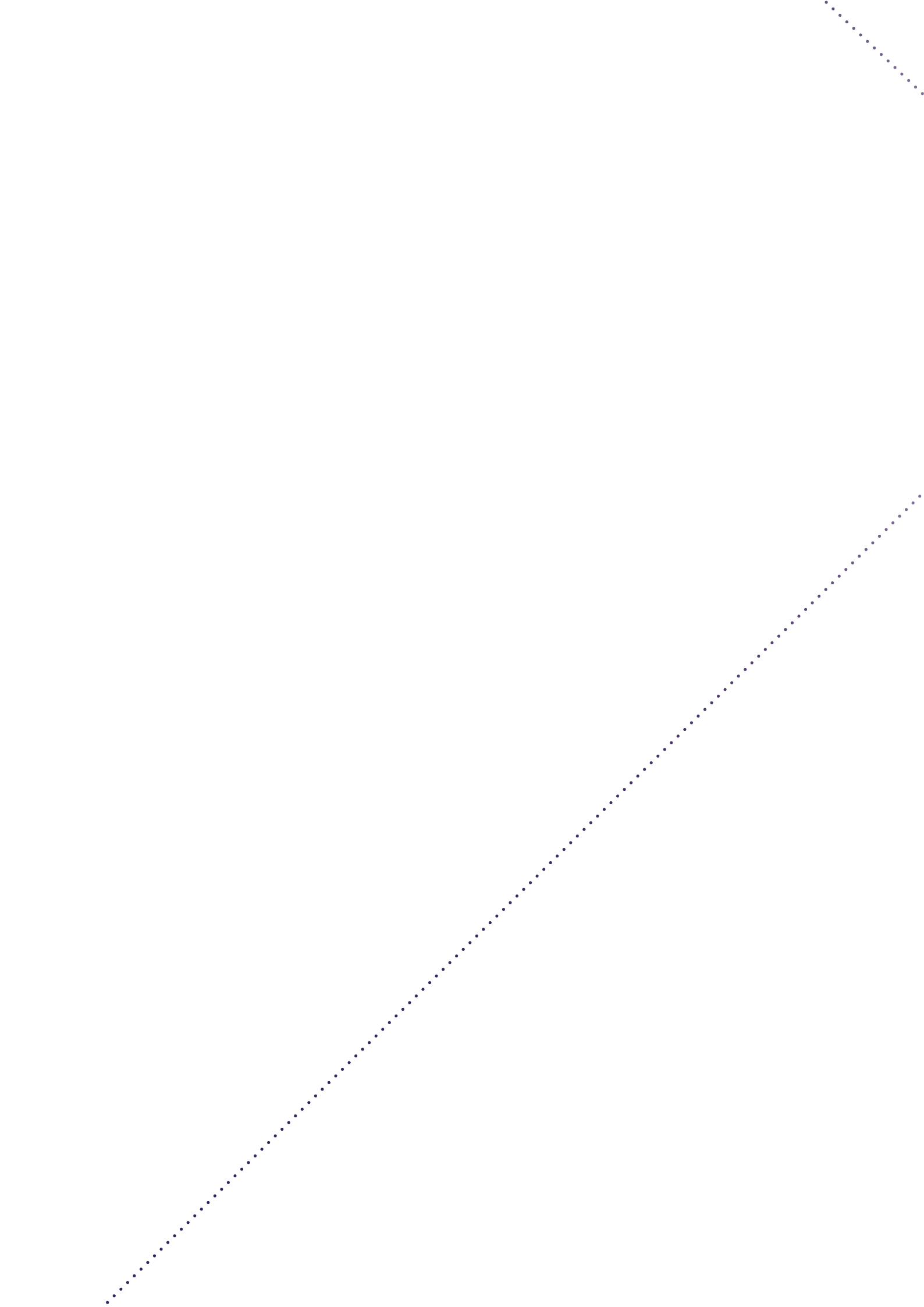
BACKGROUND While figures may vary, all observers agree in estimating that in 2025, unfilled jobs related to digital technologies, particularly cybersecurity, data science and artificial intelligence, will number in the several hundreds of thousands. This shortage relates more broadly to all jobs in science, technology, engineering and mathematics (STEM) and has been exacerbated by the pandemic. By 2030, 9 out of 10 jobs will require digital skills. However, while 79% of Europeans (ages 16-74) connect to the Internet on a regular basis, 44% do not master basic digital skills[4]. Acquisition of these skills therefore represents not only a response to unemployment, in particular among young people, but also a *sine qua non* for Europe as a digital power. All public policies are futile if human resources are lacking.

OBJECTIVE In line with DigComp, the EU's reference framework for digital skills, develop and support training in digital professions and encourage access to this training by women, who are unreasoningly under-represented in these professions.

RECOMMENDATIONS

- Promote digital professions through communication efforts aimed in particular at women, including on the occasion of European Cyber Security Month, which had its eighth edition in 2020.
- Develop an attractive human resources policy that attracts and earns the loyalty of trained young Europeans who often move abroad to accept offers from the highest bidders, especially across the Atlantic.
- Cooperate with foreign countries that send young people to be trained at European universities and *grandes écoles* so that these States do not offset the EU's inadequacies at the expense of brain drain, a problem the Union also faces and seeks to counter.

4. Monika Kiss, *Digital skills in the EU labour market,* Research Services (European Parliament), January 2017.



DIGITAL DIPLOMACY AND STABILITY

In the absence of universally recognised governance, crime and State conflict continue to play out in the digital sphere. Some cyberattacks are now sophisticated enough to affect the functioning of States or businesses on the other side of the world, exploiting our societies' increased digitisation. While several examples have illustrated the potentially systemic and geopolitical repercussions of the malicious use of digital technologies (WannaCry, NotPetya, SolarWinds, etc.), other less severe examples threaten the security and privacy of Internet users on a daily basis. Moreover, the COVID-19 pandemic has served as a reminder that lives can also be at risk, as evidenced by the rise in cyberattacks on hospitals. Thus far, this irresponsible behaviour has been the subject of several relatively unsuccessful diplomatic attempts to mitigate the risk to international security that it entails. Europe must leverage its power in terms of diplomacy and standards to offer an alternative based on its values to arrive at an international consensus.

4 PROMOTE A **EUROPEAN VISION** OF **INTERNATIONAL CYBERSPACE LAW**

BACKGROUND The interest of the United Nations in threats related to information and communication technology (ICT) with repercussions for international security dates back some 20 years. To promote stability in the world, the diplomatic institution has encouraged the emergence of several initiatives —with encouraging if modest successes— aimed at ensuring responsible behaviour among States in cyberspace.

Between 2019 and 2021, two projects received a UN mandate to make recommendations to promote such behaviour. The first, led by Russia, created an Open-Ended Working Group (OEWG) bringing together 140 States. The second, established in response by the United States, was the more exclusive sixth Group of Governmental Experts (GGE), comprised of 25 States.

The fourth GGE, in 2015, distinguished itself by laying the foundation of the current standards framework[5], which has been the basis for all discussions on this topic, including those of the OEWG. This framework rests on four universally recognised *"pillars"*: the applicability of international law to cyberspace, 11 norms of behaviour, confidence-building measures, and the strengthening of the cyber capabilities of States.

UNITED NATIONS NORMS OF RESPONSIBLE STATE BEHAVIOUR IN CYBERSPACE:

- Engage in inter-State cooperation in the domain of cybersecurity
- Consider all relevant information
- Prevent wrongful use of ICT in national territories
- Collaborate to put a stop to crime and terrorism
- Respect human rights and the right to privacy
- Not damage critical infrastructure
- Protect critical infrastructure
- Respond to requests for assistance
- Take steps to ensure the integrity of the supply chain
- Report ICT vulnerabilities
- Not harm emergency response teams

5. United Nations, General Assembly, Developments in the Field of Information and Telecommunications in the Context of International Security, A/70/174, 22 July 2015.

In March 2021, the OEWG achieved a diplomatic feat[6] with the adoption of its final report by consensus of all its participants. The group did not, however, include in that report any substantive proposal with regard to the applicability of international law to cyberspace. Indeed, neither the principle of due diligence nor international humanitarian law (IHL) is mentioned therein. The matter of application of IHL solidifies tensions: its supporters believe that cyberattacks against critical infrastructure can have a human cost, whereas its opponents maintain that it would amount to militarising cyberspace[7].

With a similar mandate, the sixth GGE came to a consensus in May 2021[8], with some progress made. Its report recognises that IHL applies to cyber operations in times of armed conflict, though the implementation of such applicability has yet to be determined. Debate surrounding recognition of the principles of due diligence and sovereignty in law, however, remains in abeyance[9].

The competition between these two initiatives nevertheless reflects different concepts of cyberspace. While some countries seek to control it within their territories, in the name of the principle of sovereignty, others wish it to be free, open and secure. This distinction accounts for two trends: on the one hand, States wishing to create new binding rules through a new treaty (China, Russia, etc.) and, on the other hand, States in favour of the *status quo*, maintaining that existing international law, supplemented with voluntary, non-binding standards, is enough[10] (the United States, Western countries, etc.).

However, the West is not a uniform bloc. Differences exist, in particular with regard to recognition of the principle of due diligence as a rule of law[11]. Proponents of such recognition include several European countries such as Germany[12], Finland[13] and France[14]; opponents thereof include the United States.

6. Aude Géry, "ThucyBlog n° 118 – Ils l'ont fait ! Adoption d'un rapport par l'OEWG sur les progrès des TIC dans le contexte de la sécurité internationale : un succès diplomatique certain" [They Did It! Adoption of a Report by the OEWG on Advances in ICT in a Context of International Security], *Centre Thucydide,* 5 April 2021.
7. Arindrajit Basu, Irene Poetranto, Justin Lau, "The UN Struggles to Make Progress on Securing Cyberspace", *Carnegie*, 19 May 2021.
8. United Nations, *Report of the Group of Governmental Experts on Advancing responsible State behaviour in cyberspace in the context of international security,* 28 May 2021.
9. Michael Schmitt, "The Sixth United Nations GGE and International Law in Cyberspace", *Just Security,* 10 June 2021.
10. *Op. cit.* Arindrajit Basu, Irene Poetranto, Justin Lau, 19 May 2021.
11. According to this principle, recalled by the fourth GGE (2015), States must not knowingly allow their territories to be used to commit ICT-assisted acts in violation of international law.
12. "On the Application of International Law in Cyberspace", The Federal Government, Germany, March 2021.
13. "Finland published its positions on public international law in cyberspace", Finnish Government, October 2020.
14. French Ministry of Armed Forces, *Droit international appliqué aux opérations dans le cyberespace* [International Law Applied to Operations in Cyberspace], September 2019.

OBJECTIVE Promote a European vision of the applicability of international law to cyberspace, centred on the values on which the Union is founded, to foster a consensus within the United Nations.

RECOMMENDATIONS

Bring about the emergence of this European *"third way"* with regard to the applicability of international law to cyberspace, distinct from that of the United States and from that of China and Russia, as follows:

- Establish common European training in international law to promote common assessments among Member States.
- Consider the principle of due diligence to be the foremost condition for the peaceful use of cyberspace. States' accountability and international responsibility must cut off any inclination to use cyberspace for indirect strategies.
- Identify and collectively adopt within the EU the most consensual rules, starting with the prohibition of hack-back and the enforcement of peaceful use of cyberspace and protection of critical infrastructure, with health establishments taking top priority.
- Bring together all countries with a similar vision, as well as *"swing States"* with little involvement in debates on standards, such as South Africa, South Korea and India.
- Refrain from adding an additional component to all existing diplomatic initiatives; rather, have the EU endorse the recommendations of the Paris Call in order to guide the development of its future public policies on the digital sphere and the protection thereof[15].

15. French Higher Commission for Digital and Postal Services, *Recommandations dans le domaine de la sécurité numérique* [Recommendations in the Domain of Digital Security], Opinion no. 2021-03, Recommendation no. 20, 29 April 2021.

ENHANCE THE **EU'S CYBER DIPLOMACY TOOLBOX**

5

BACKGROUND The EU Cyber Diplomacy Toolbox constitutes the framework for a joint diplomatic response by the EU in the event of a cyberattack targeting the Union. Instituted in 2017, this instrument specifies all measures —some restrictive— under the Common Foreign and Security Policy (CFSP) to be put in place to protect the EU and its Member States from cyberattacks.

This initiative was strengthened two years later with the introduction of a sanctions regime. These sanctions include bans on travel to and within the EU as well as asset-freezing measures that prohibit, among other things, making funds or economic resources available[16].

In July 2020, the EU imposed its first sanctions within this regime against six individuals and three entities (from China, North Korea and Russia), to whom were attributed[17] the cyberattacks WannaCry and NotPetya, Operation Cloud Hopper, and the attempt to hack the Organisation for the Prohibition of Chemical Weapons (OPCW)[18].

However, while restrictive measures are applied to individuals and entities involved in cyberattacks, the fact remains that collective attribution by the EU is a challenge, as some Member States wish to retain their decision-making autonomy.

The toolbox acts upstream of attributions and sanctions by providing for several diplomatic measures such as requests for information or corrective actions made to countries from which a cyberattack originates. This component involves concentrating both information sharing and analytical capabilities within the European Union Intelligence and Situation Centre (INTCEN). On this last point, capability development should be based on joint exercises and more synergistic undertakings with the private sector, as well as continued cooperation with NATO and the United Kingdom after Brexit[19, 20].

OBJECTIVE Give the Cyber Diplomacy Toolbox an operational basis and make it an international instrument of influence, deterrence and sanction modelled on executive orders in the United States.

16. "Adoption des toutes premières sanctions économiques européennes en matière de cybermalveillance", [Adoption of the Very First European Economic Sanctions on Cyberattacks] *Hughes Hubbard & Reed*, 8 September 2020.
17. European Union, *Implementing Regulation concerning restrictive measures against cyber-attacks threatening the Union or its Member States*, 30 July 2020.
18. "EU imposes the first ever sanctions against cyber-attacks", *European Union,* 30 July 2020.
19. Stefan Soesanto, "Europe has no strategy on cyber sanctions", *Lawfare*, 20 November 2020.
20. Paul Ivan, *Responding to cyberattacks : prospects for the EU Cyber Diplomacy Toolbox,* European Policy Centre (EPC), 18 March 2019.

RECOMMENDATIONS

- Strengthen information sharing within the INTCEN to consolidate the non-coercive action and influence of the Cyber Diplomacy Toolkit.
- Develop forensic capabilities on a European level by means of increased cooperation with the private sector.
- Establish a European blacklist of individuals and entities having sold offensive capabilities to States or to other entities under sanction, or having the potential to use them for purposes contrary to the fundamental rights or interests of the EU and its Member States.
- Develop a coherent communication strategy around the Cyber Diplomacy Toolbox concerning actions allowed and decisions made, in particular via the Member States, to strengthen their political weight and their deterrent nature.

BRING ABOUT **REGULATION** OF THE **ZERO-DAY VULNERABILITY MARKET**

6

BACKGROUND An *"offensive"* cyber industry allowing States, and even criminal and non-state terrorist organisations, to buy *"off-the-shelf"* zero-day vulnerabilities (i.e. vulnerabilities that have been neither disclosed nor patched) has grown over the course of a few years. The market for zero-day vulnerabilities is a true grey market: it is legal, but not controlled by vulnerability owners or software publishers. It is even structured around an ecosystem comprising cybersecurity researchers, brokers and private companies selling monitoring solutions (so called *"access as a service"* solutions). The researchers identify zero-day vulnerabilities and proceed not to share them with the software publisher or the hardware manufacturer with a view to patching them, but to sell them, along with exploits that enable them to be used in a more or less industrialised way, to brokers or private companies for maximum profit. This market is making major contributions to the proliferation of a cyber arsenal.

OBJECTIVE Capitalise on the EU's power in terms of diplomacy and standards to help establish a framework for acquisitions of zero-day vulnerabilities by supporting international discussions, in particular as part of the Paris Call and with the United Nations.

RECOMMENDATIONS

- Develop a vulnerability management programme within a European framework and promote it to the transatlantic ally.
- Encourage cooperation among vulnerability owners and researchers to reduce risks tied to public disclosure by promoting coordinated disclosure policies[21].
- Identify on blacklists companies having sold capabilities to entities under sanction or having the potential to use them for purposes contrary to fundamental rights or considered illegitimate by the Member States.
- Organise bug bounties to encourage and set guidelines for research on vulnerabilities by proposing a financially attractive alternative for cybersecurity researchers.

21. "Encouraging vulnerability treatment: Overview for policy makers", *Digital Economy Papers*, no. 307, Organisation for Economic Co-operation and Development (OECD), Paris, 2021, pp. 24-25.

7 DEVELOP A **COMMON UNDERSTANDING** OF **CYBER THREATS**

BACKGROUND Given the deteriorating security situation in neighbouring countries, the EU is firming up expectations as to its role in regional crisis prevention, stabilisation and peace. The reality, however, is different[22]. Although the EU has reinforced its security architecture and capabilities under the Common Security and Defence Policy (CSDP), Member States ultimately make little use of this multilateral framework, as evidenced by the modest number of missions and associated operations that are under way[23].

Member States have different priorities and perspectives due to their differences in strategic culture. While this pluralism is a strong point of the EU —which also has a *"360-degree"* view of international issues— it does not contribute to cohesion within Europe. This is especially true since Member States regularly vote in favour of European operations, then fail to mobilise the required forces[24]. Faced with these operational dead ends, several countries are dropping the multilateralism of the CSDP in favour of *"coalitions of the willing"*. Under this approach, countries are able to work pragmatically with the most *"willing and able"* countries rather than wait for everybody to reach a consensus.

This trend reflects, in addition to a lack of support for European crisis management, an inability on the part of the EU to offer a credible collective response. However, in cyberspace, a common positioning requires a joint vision of threats and vulnerabilities: Europeans must together be able to anticipate, detect, understand and characterise attacks, as well as, where appropriate, attribute them to one or more agents. This method will at least make it possible to limit their effects and take initiative with the intention of discouraging attacks.

Joint identification of cyber threats is therefore essential. It requires a framework in which Member States can name their adversaries in complete confidentiality, in order to better understand how they reveal themselves, because all cyberattacks are a matter of strategy and intentionality.

To this end, Germany launched the Strategic Compass project in 2020. These reflections aim to clarify relationships among Member States and bolster the EU's credibility as an international partner. They must bring Europeans together around a shared analysis of (cyber) threats, the starting point for a European dialogue and identification of priorities. However, this common understanding can only be strengthened by promoting information

22. Jana Puglierin, "Direction of force: The EU's Strategic Compass", European Council on Foreign Relations (ECFR), 1 April 2021.

23. Twelve civilian missions and six military operations.

24. "Strategic Compass: Developing strategic principles", eu2020.de, 25 August 2020.

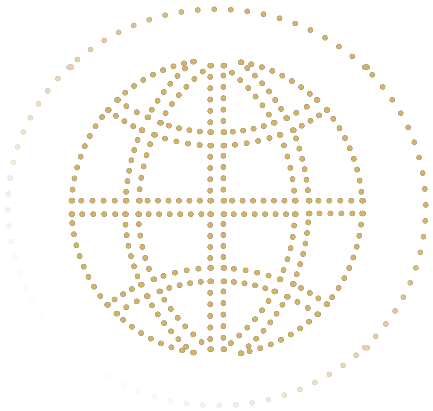
sharing, building trust and ensuring a common level of cybersecurity among Member States. With regard to this last point, while the legislative framework guarantees a threshold, disparities in operational capabilities must be reduced through cooperation.

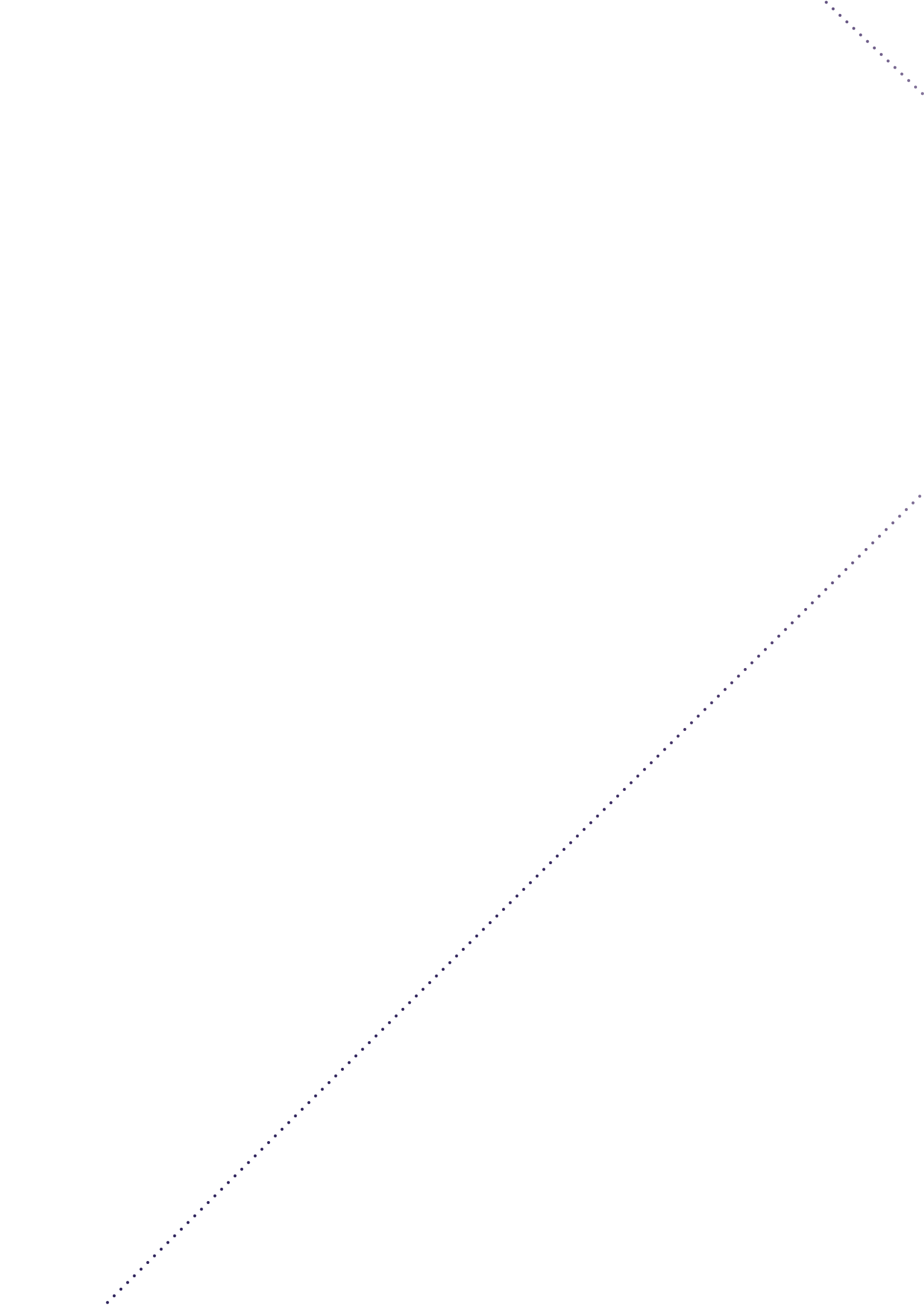
OBJECTIVE Accelerate the adoption of the Strategic Compass, which constitutes an essential step towards strengthening European solidarity against cyber incidents.

RECOMMENDATIONS

The adoption and implementation of the Strategic Compass involves the following upstream efforts:

- Strengthen the collective system of cyber situational awareness based on the development of *ad hoc* tools through the EU's Defence Technological and Industrial Base (EDTIB).
- Explore the possibility of enlisting the support of the private sector to detect cyber threats, within the well-established limits of their responsibilities and the level of confidentiality.





MILITARY
CYBER DEFENCE

Conflicts play out in cyberspace just as they do on land, in the air, by sea and in space. In order to better understand the military dimension of cyberspace, the EU has initiated the development of a strategy that will formalise its ability to conduct operations in that environment as in others. This roadmap will affirm several European wishes in terms of autonomy, deterrence, civil–military continuum, cooperation (primarily with NATO) and capability development. The EU's development of military cyber defence in these respects can include a large number of players, including its Member States, the European Union Military Staff (EUMS) and the European Defence Agency (EDA). However, this proliferation of stakeholders, as well as projects and initiatives, carries a need for overall coordination and coherence, as resources are currently scarce and insufficient.

8 STRENGTHEN THE **EU'S MILITARY CYBER DEFENCE**

BACKGROUND Europeans aspire to act autonomously and collectively in the field of military cyber defence[25]. Provided for by Article 42.7 (the mutual defence clause) of the Treaty on European Union (TEU), European *"solidarity"* means that Member States can call upon other Member States in the event of a major cyberattack against one of them. While the implementation modalities (type of assistance, time frame, etc.) have yet to be determined, the fact remains that the EU already has an architecture covering the entire spectrum of cyber operations, as it already has a multitude of entities enabling it to organise, equip and train its Member States: the Common Security and Defence Policy (CSDP), the European Union Military Staff (EUMS), the European Defence Agency (EDA), the Permanent Structured Cooperation (PESCO), CERT networks, etc.

The PESCO, part of the CSDP, enables a group of Member States to make mutual commitments to military spending, armament programmes and operational capabilities. This framework has enabled the emergence of four collective cyber defence structures, including:

- The Cyber and Information Domain Coordination Centre (PESCO/CIDCC), which constitutes, operationally speaking, a prototypical command and control (C2) centre for military cyber operations. However, as it stands, it only brings together four Member States (Germany, France, Hungary and the Netherlands).

- The Cyber Rapid Reaction Team (PESCO/CRRT), which is in charge of incident reporting and response, although it lacks the necessary legal basis to intervene beyond its mere six participating nations (Croatia, Estonia, Lithuania, the Netherlands, Poland and Romania).

While PESCO projects develop European interoperability, they are constrained by weak participation on the part of Member States. The EDA does address these shortcomings through its central role in education and training. Indeed, through EDA exercises such as Cyber Phalanx, the EU MilCERT Interoperability Conference (MIC) and CYBRID, European nations are able to concentrate operational cyber capabilities and gain experience in them under real-world conditions.

25. European Union, *Shared vision, common action: A stronger Europe,* June 2016, p. 16.

OBJECTIVE Have strong long-term leadership to strengthen and ensure the consistency of existing military cyber defence, rather than add new structures and functions, against a backdrop of constraints on Member States' human resources.

RECOMMENDATIONS

Military cyber defence requires comprehensive, enduring coordination that cannot be limited to a single Presidency of the Council of the EU. The French Presidency must initiate —if not perpetuate— a dynamic that promotes the collective development thereof, starting with the following:

- Strengthen strategic cooperation among the competent authorities of the Member States through the establishment of a forum of Cyber Commanders to complement the traditional Communication and Information Systems & Cyber Defense (CIS&CD) conference.
- Initiate and support the creation of a European network of military computer emergency response teams (CERTs) to foster interoperability between Member States. This project, identified in 2014 but neglected since, represents an opportunity to bring together national resources for the benefit of fruitful cooperation on both a State and an EU level.

9 STREAMLINE **EUROPEAN CYBER DEFENCE** THROUGH **EU-NATO COMPLEMENTARITY**

BACKGROUND Cyber defence cooperation between the EU and NATO is limited and has not realised its full potential. Yet, these organisations, which have 21 members in common, face the same challenges and cover a similar area of action, but their operational exchanges are not up to the same level as their strategic relationship.

In 2016, the EU and NATO signed a joint declaration identifying matters of common interest, which have since been addressed in a high-level dialogue. This dialogue is characterised by a high level of convergence on cyber risk, hybrid threats, China, Russia and other matters[26]. Today, the EU and NATO are confronted with players who increasingly resort to hybrid strategies combining diplomatic, informational, military, economic and legal means to make gains. This overall ambiguous dynamic is difficult both to detect and to report[27].

Amid these global power strategies, in which cyber affairs occupy a growing place, ensuring European freedom of action means investing in cyberspace. While the EU has fallen behind in understanding this competitive space, NATO —an alliance whose very essence lies in defence and *de facto* cyber defence of its members— quickly recognised cyberspace as an area of operations and became involved further upstream in the resilience of the majority of Member States, thus contributing to Europe's security.

NATO, with its more substantial military budget, has more mature entities (Cyber Operations Centre, Cooperative Cyber Defence Centre of Excellence, etc.) than the Union does and therefore more influence over the development of the military cyber capabilities of European countries. For the EU, which takes a broader approach to cyber defence, military affairs are just one of many dimensions.

OBJECTIVE Streamline Europe's military cyber defence by bringing together the EU's civil advances and NATO's operational expertise. Indeed, the duality of cyberspace is such that civil regulations are sometimes prescriptive for military applications[28].

26. NATO, *NATO – EU Relations,* Fact Sheet, Public Diplomacy Division, March 2021, p. 2.
27. French Ministry of Armed Forces, *Actualisation stratégique* [Strategic Update], 2021, p. 39.
28. Morgan Jouy, "Une cyberdéfense collective en Europe ?" [Collective Cyber Defence in Europe?], Research Note, no. 83, Institute for Strategic Research of the École Militaire (IRSEM), 2017.

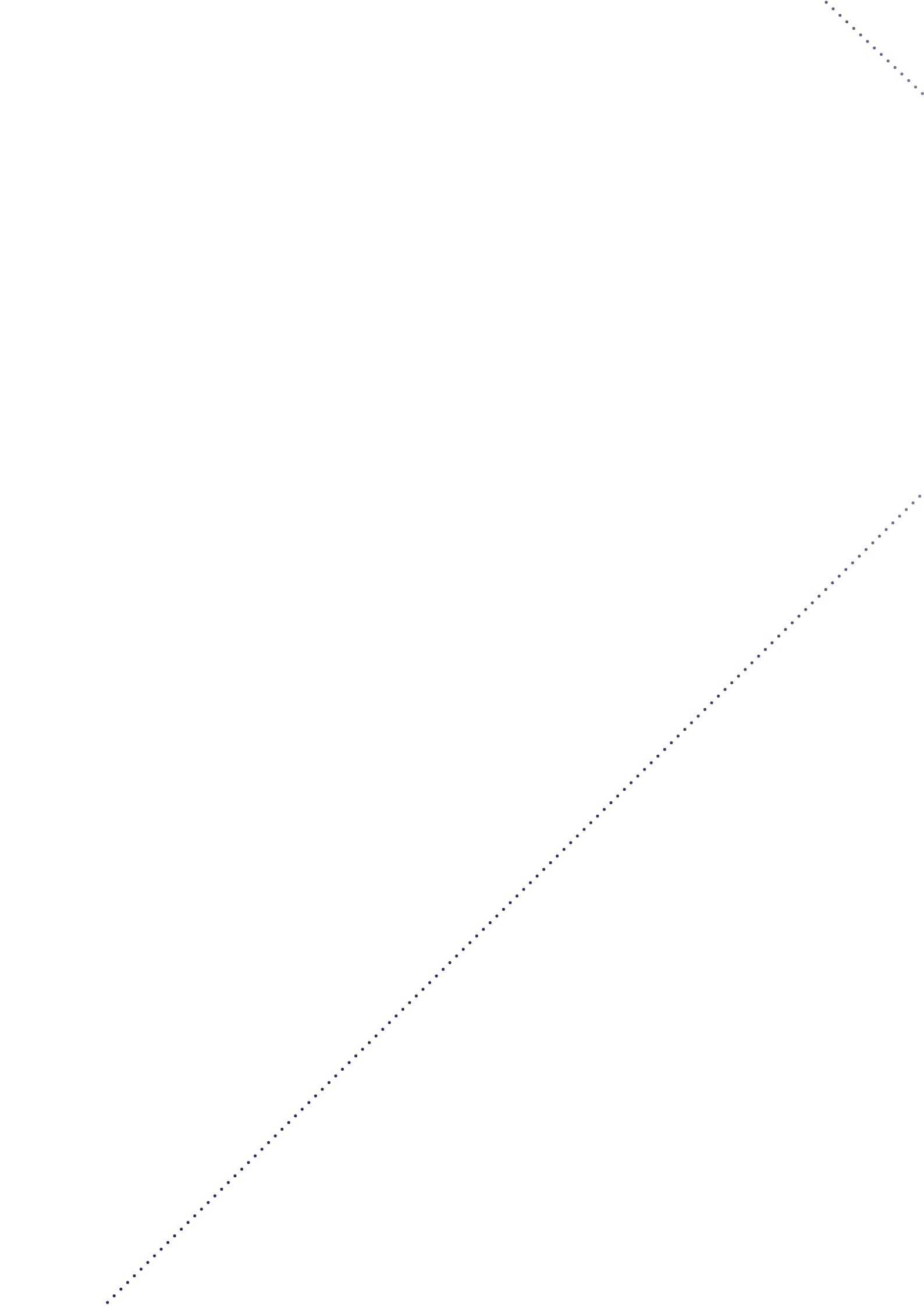
RECOMMENDATIONS

EU military cyber defence, confronted with hybrid strategies, must go beyond responses strictly limited to capabilities and operations. The Union must also contribute more generally to international security by promoting confidence-building measures, taking part in discussions on the applicability of international law to cyberspace, and accelerating synergies with the private sector.

The EU must still strengthen itself in military affairs by cooperating more with NATO, but must not seek to compete, due to the potential for redundant or overlapping activities:

› Enhance the sharing of best practices between the EU and NATO as part of joint operations. The theatre best suited to this is the Mediterranean, where both organisations are active.

› Ensure effective complementarity between the mutual defence clause of the EU Member States (Article 42.7 of the TEU) and that of NATO (Article 5 of the North Atlantic Treaty) in the event of a major cyberattack.



FIGHT AGAINST CYBERCRIME

Cybercrime is *"the crime of the 21st century"*[29]. Since the onset of the COVID-19 pandemic, it has undergone exponential growth that is bound to continue in the years to come. While criminals are flocking to cyberspace, States and para-State agencies are also entering this arena to engage in activities below the threshold of armed conflict. These activities, though they do not qualify as armed conflicts in a legal sense, can be distinguished from classic cybercrime by the breadth and nature of their targets. The United States just elevated ransomware to the level of terrorism, underscoring the seriousness of certain cybercrimes. The fight against these offences calls for increased cooperation among Member States of the European Union, strengthening of national and European capabilities, and common legislation that promotes the detection and collection of digital evidence—without challenging the national sovereignty asserted in matters of defence and security.

29. Theme of the FIC 2007.

10 BUILD CAPACITY IN THE FIGHT AGAINST CYBERCRIME

BACKGROUND The fight against cybercrime has too often been neglected, sometimes under the pretext of difficulties tied to the cross-border nature of offences committed from *"rogue"* States in matters of cyberattacks. Nevertheless, recent examples (Avalanche, the VPN Safe-iNet, EncroChat, etc.) have shown that European cooperation can be effective and is sometimes even necessary (with the help of the FBI and other foreign police forces).

OBJECTIVE Build capacity in the fight against cybercrime in the EU and its Member States by ensuring that everybody agrees upon efforts in terms of organisation, staffing, and resources.

RECOMMENDATIONS

Several concrete steps would bolster the fight against cybercrime:

- Create a European public prosecutor's office specialising in cybercrime, similar to the European Public Prosecutor's Office for financial matters, to combat cyberattacks targeting EU institutions. This office must acquire skills in processing and enforcing cybersecurity penalties without encroaching upon matters under national jurisdiction[30].
- Implement a common cyber threat intelligence platform that the law enforcement agencies of the Member States will be able to directly access in a simple and secure manner. Such a tool, intended to facilitate rapid exchange of information, must be user-friendly and available in multiple languages. Training can be put in place to instruct the various units concerned in its effective use.
- Develop within Europol (European Cybercrime Centre [EC3]) forensic investigation capabilities to achieve better control, in particular of the Darknet and cryptocurrency, and to facilitate the process of filing criminal charges.

30. French Higher Commission for Digital and Postal Services, *Recommandations dans le domaine de la sécurité numérique,* [Recommendations in the Domain of Digital Security], Opinion no. 2021-03, Recommendation no. 4, 29 April 2021.

› Promote the creation of a European skills network to improve collaborative and synergistic efforts by:

- developing, within the European Police College (CEPOL), training in the fight against cybercrime common to law enforcement agencies, computer security incident response teams (CSIRTs), and magistrates.
- establishing an e-Erasmus programme among schools that train cyber investigators.
- instituting a European reserve that can be called upon by one or more Member States to strengthen (joint) investigation teams.
- clearly identifying the fight against cybercrime in the missions of the future Bucharest-based Cybersecurity Competence Centre and the EU Joint Cyber Unit.
- institutionalising operational cooperation between border States by organising Police and Customs Cooperation Centres (PCCCs) designed for the fight against cybercrime.

› Bring together players in cyber defence and the fight against cybercrime, according to each individual player's goals, in order to facilitate exchange of intelligence of cyber origin and cyber interest while respecting the sovereignty of the Member States.

› Develop a public–private partnership, in particular to enhance knowledge of cybercrime phenomena, so that security providers and insurers have an instantaneous awareness of cyberattacks useful in bringing down crime numbers that influence the orientation of public policies. This partnership must also be designed within a more operational framework (reporting of cybercrimes, preservation of evidence, and assistance with forensic analysis).

› Further extend secondment opportunities within Member States among law enforcement agencies as well as national and governmental CSIRTs.

ARRIVE AT A **BALANCED SOLUTION** ON **PRESERVATION OF EVIDENCE**

BACKGROUND According to the EU, 85% of criminal evidence is digital, and more than half of it is hosted in a territory other than the site of the corresponding offence. It is important to be able to access evidence under stable legal conditions that reconcile investigation needs and respect for privacy. It must be possible to store this evidence for an adequate period of time and access it quickly without undermining the sovereignty of States, including when requests come from non-European countries.

The French Conseil d'État has interpreted the case law of the Court of Justice of the European Union (CJEU) in a manner diametrically opposed to that of the Constitutional Court of Belgium. It is important for Member States to have shared legislation. The CJEU's ruling on 6 October 2020 was based on texts designed within the framework of the Single Market for the Single Market. Interference in the field of defence and national security that falls under the sovereignty of the Member States is the result of a federalist approach, on which there is no consensus. On the pretext of avoiding general surveillance of content, case law abandons victims, who now have limited hope of their predators being caught.

OBJECTIVE Develop mechanisms for collecting digital evidence, as crimes and delinquent acts have become inseparable from the digital sphere, whether they target it or leverage it in some way.

RECOMMENDATIONS

- Finalise draft legislation relating to the *"e-evidence"* regulation, promoting the rapid transfer of the data necessary for the establishment of digital evidence, according to the prerogatives of the judicial authority and fundamental personal data principles.
- Take advantage of the more favourable conditions for transatlantic dialogue to advance the negotiations initiated in September 2019 between the EU and the United States in order to resolve difficulties related to data transfer in criminal matters (discrepancies between, on the one hand, the Clarifying Lawful Overseas Use of Data [CLOUD] Act and, on the other hand, the GDPR and the Data Protection Law Enforcement Directive).
- Prepare European legislation that ensures a clear separation between the data host, who must store evidence under conditions of *"cybersecurity"*, and the requesting service, whose requisitions must be validated by a judge or an independent authority, as desired by the CJEU.

GIVE **NEW IMPETUS** TO THE **BUDAPEST CONVENTION**

12

BACKGROUND The Budapest Convention is the only binding international text in the fight against cybercrime. The convention, which has now been ratified by 67 States —some of which are not members of the Council of Europe but are signatories to the Malobo Convention of the African Union (2014)— has inspired a total of nearly 150 foreign laws. The convention is based on values that cannot be called into question by a more expedient treaty, which some States wish to bring to the United Nations. As it approaches its 20th anniversary, a new additional protocol is in the process of being finalised.

OBJECTIVE Support the implementation of the Budapest Convention's second additional protocol to render it the predominant instrument in cross-border cooperation.

RECOMMENDATIONS

- Promote its ratification by non-Member States of the Council of Europe through cyber diplomacy[31].
- Implement its recommendations in a pragmatic manner, without systematically seeking unanimity, through bilateral agreements (especially cross-border ones), with a view to setting an example to be widely followed.
- Continue the work of adapting the Budapest Convention after the new additional protocol is finalised in pursuit of *"interoperability"* of digital investigations.

31. cf. Recommendation no. 4 "Promote a European Vision of International Cyberspace Law".

13 STRENGTHEN THE **FIGHT AGAINST ILLEGAL CONTENT**

BACKGROUND Content is considered *"illegal"* when it does not comply with the laws of the EU or its Member States. According to European directives, this designation covers aiding and abetting terrorism, child sexual abuse material, hate speech, scams and infringements of intellectual property rights such as audiovisual piracy. In the digital age, this content is essentially produced and distributed through intermediary platforms (social media, blogs, marketplaces, etc.) created and operated by private players such as Google, Facebook and Baidu.

In Europe, the Directive on electronic commerce (2000) laid out the responsibilities of online service providers, according to a distinction made between *"publishers"* and *"hosts"*. While publishers are responsible for everything published on their sites, hosts become responsible as soon as they are notified of the presence on their servers of illegal content, which they must then remove *"expeditiously"*. Intermediary services, which back then had mere thousands of users, not millions as they do now, were classified as hosts. In the early days of the Internet, legislators were unable to anticipate either its misappropriation for illegal purposes or the *"systemic"* dimension that certain platforms have taken on today.

Such a regulation promotes circulation of illegal content, and platforms —especially major ones— do not play enough of a role in curbing this phenomenon. This is all the more worrying when the manipulation of information that is occurring is taken into account. Indeed, fake news has been found to spread six times faster than *"real"* information on social media[32].

To counter this dynamic, which threatens both user security and the sustainability of democracies, the European Commission presented the Digital Services Act (DSA) in December 2020. Thierry Breton summed it up thus[33]: *"what is forbidden offline must be forbidden online"* and *"all illegal content must be removed"*. The DSA is aimed at imposing new obligations on platforms with, among other things, a mechanism for reporting illegal content (already in force in some Member States) and an internal system for handling user complaints.

Major platforms, for their part, will fall into an *ad hoc* category of *"gatekeepers"*, understood to refer to platforms that are developed enough to control access to a given market.

32. Peter Dizikes, "Study: On Twitter, false news travels faster than true stories", *MIT News*, 8 March 2018.

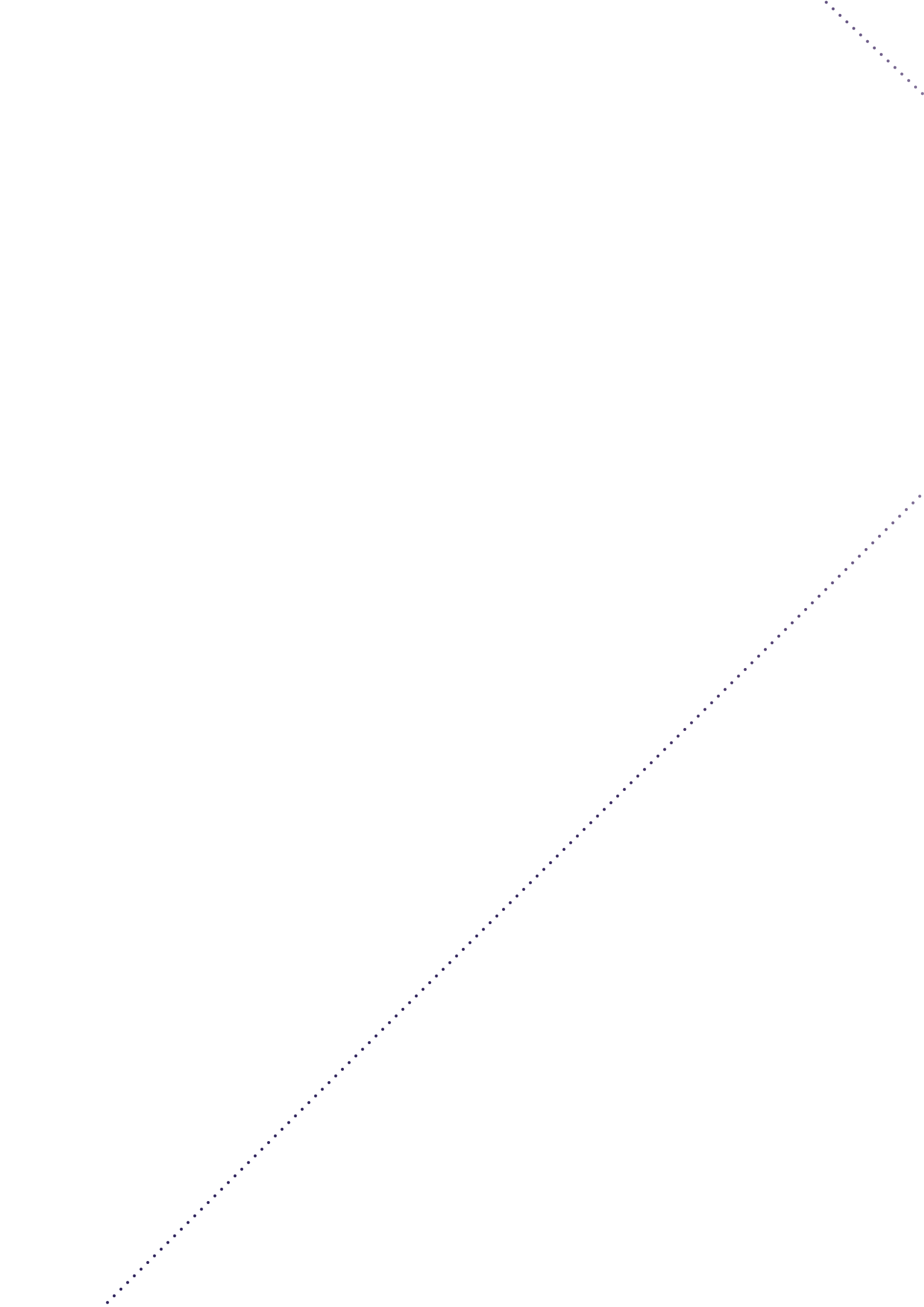
33. Virginie Malingre, "Thierry Breton : « Dans bien des cas, l'espace numérique est une zone de non-droit »", [In Many Cases, the Digital Sphere is a Lawless Realm], *Le Monde,* 22 October 2020.

These operators must, among other things, assess and mitigate the systemic risks associated with the operation and use of their services, undergo external audits of their level of compliance, and report the parameters used in their content recommendation systems.

OBJECTIVE Unite all Member States in finalising the text of the Digital Services Act (DSA) for its accelerated adoption.

RECOMMENDATIONS

- Establish a *"signature database"* of illegal content in each Member State.
- Aggregate these databases on a European level.
- Bolster innovation in artificial intelligence, which must always be used in service to humanity, to facilitate detection and removal of illegal content.



CYBERSECURITY & RESILIENCE

The strengthening of the collective level of cybersecurity and resilience of European digital infrastructure constitutes an operational imperative. This requirement, which lies at the heart of the new EU cybersecurity strategy, will have to translate to:

- Adoption of an even more proactive framework for laws and standards to improve the security of critical infrastructure (NIS2 Directive) and to require software publishers and hardware manufacturers to incorporate security *"by design"* and *"by default"* into their products.

- Strengthening of capabilities of European institutions, both to meet their own needs and to develop a capability for response to major incidents, which will complement rather than replace the capabilities of each Member State.

14 IMPOSE SECURITY "*BY DESIGN*"

BACKGROUND More than three-fourths of software applications have security vulnerabilities. One-fourth of these vulnerabilities are believed to have a high level of severity[34]. With the explosion of connected objects, the number of vulnerabilities will grow exponentially. Connected objects often have a very weak level of security for various reasons, such as time-to-market requirements, the global market, a lack of security expertise, the complexity of the value chain, the absence of standards, and poorly defined responsibilities. If regular reports of vulnerabilities identified on major platforms are to be believed, cloud computing infrastructure is not to be left out of this grouping.

OBJECTIVE This is no longer just a matter of certifying the reliability of security equipment. Now, it is also a matter of guaranteeing the security of products and services that either are digital in nature or incorporate digital elements—whether they belong to the world of generic information technologies, operational technologies (OTs), or cyber-physical systems, where security and safety are intimately linked.

RECOMMENDATIONS

- Accelerate the implementation of European certification schemes according to the legal framework adopted in the Cybersecurity Act.
- Propose legislative measures to improve cybersecurity in all digital products, including software programs placed on the internal market. In June 2021, the European Parliament decided to pursue a sufficiently demanding cross-sectoral regulation for *"applications, software, embedded software, and operating systems by 2023"*[35].
- Bring about international adoption of the principle that publishers and manufacturers —in particular, systems manufacturers and publishers— must take responsibility for the design

34. Veracode, "State of Software Security v11", June 2021.

35. European Parliament, *The EU's Cybersecurity Strategy for the Digital Decade*, 10 June 2021, p. 5

and maintenance of their products. Voluntary commitments, such as the 2018 Charter of Trust, are good initiatives, but they are not enough. The Organisation for Economic Co-operation and Development (OECD)[36] and Cigref[37] have both observed a trend among many suppliers towards placing responsibilities in this regard on end users, even though end users are not in the best position to manage security and risks associated with products.

› Establish *"security by default"* as a principle. Applications must incorporate the highest levels of personal data protection and security from the outset, without the user having to choose among different options.

› Require publishers and manufacturers to maintain secure conditions, through regular updates, to address the matter of obsolescence of installed products. To fulfil this objective, the provisions of the 2019 European consumer protection directives that require sellers to make patches available to end users of digital services[38] would have to be extended to companies. This commitment would have to be upheld even after the end of the marketing period, as equipment often remains in use after it ceases to be sold[39]. The European Parliament has also recommended that manufacturers give advance notice of the minimum period during which they will provide patches and updates so that consumers may make informed choices[40].

36. OECD, "Enhancing the digital security of products: A policy discussion", *Digital Economy Papers*, no. 306, 2021.

37. Letter of 13 November addressed to the Prime Minister of the French Republic.

38. Directives 2019/770/EU and 2018/771/EU of 20 May 2019.

39. Sébastien Meurant, Rémi Cardon, "La cybersécurité des entreprises - Prévenir et guérir : quels remèdes contre les cyber virus ?" [The Cybersecurity of Companies—Prevent and Cure: Remedies for Cyber Viruses], *Information Report*, no. 678, French Senate, 10 June 2021.

40. *Op. cit. The EU's Cybersecurity Strategy for the Digital Decade,* 10 June 2021, p. 5.

15 DEVELOP A **EUROPEAN CAPABILITY** FOR RESPONSE TO **MAJOR INCIDENTS**

BACKGROUND Most European countries lack the technical capabilities to detect and respond to major incidents in a timely manner. Nevertheless, as of now, there is no procedure for assistance and no common structure capable of an operational as well as political and diplomatic response in the event of an attack on one or more Member States. As Guillaume Poupard, Director General of the French National Agency for the Security of Information Systems (ANSSI), put it, the EU must be able to, on a Union-wide scale, *"pursue collective attribution"* to rule on *"inadmissible"*[41] attacks.

The European Cybersecurity Strategy proposes building a network of Security Operations Centres (SOCs) within the EU. The challenge is to build the densest possible network in order to generate collective knowledge as well as share tools and best practices.

In June 2021, an important step was taken with the European Commission's proposal to establish a new Joint Cyber Unit[42, 43] in Brussels, not far from the CERT-EU. This unit's mission is to ensure a coordinated response to the most serious cybersecurity incidents.

OBJECTIVE Ensure the proper articulation of the European response system around the following three levels:

- Internal capabilities of Member States. These are indispensable as cybersecurity affairs must above all be conducted as close to the ground as possible. Any attempt to develop a cyber *"umbrella"* through which a few large States would ensure the protection of smaller States would also come up against sovereignty concerns—and not without reason.
- The networking of these capabilities available in all cybersecurity communities, including law enforcement agencies, armed forces and diplomatic services. To this end, an exchange network christened the Cyber Crisis Liaison Organisation Network (CyCLONe) was established by the European Commission and the European Union

41. "Audition, à huis clos, de M. Guillaume Poupard, directeur général de l'Agence nationale de sécurité des systèmes d'information sur l'actualisation de la LPM 2019-2025", [Hearing, behind closed doors, of Mr Guillaume Poupard, Director General of the French National Agency for the Security of Information Systems (ANSSI) on the updating of the French Military Planning Law (LPM) 2019-2025], *French National Assembly,* 8 June 2021.

42. "Commission proposes a Joint Cyber Unit to step up response to large-scale security incidents", *European Commission,* 23 June 2021.

43. "Joint Cyber Unit", *European Commission,* 23 June 2021.

Agency for Cybersecurity (ENISA) in 2020. This network must interact appropriately with the pre-existing network of computer security incident response teams (CSIRTs).

- Common capabilities. The EU Joint Cyber Unit will pool public and private resources at the request of a European nation in the name of the solidarity of the Member States. The exchange of information between SOCs will significantly improve Member States' detection capabilities.

RECOMMENDATIONS

› Finalise the implementation of the system by 30 June 2023 and put it in operation by 30 June 2022:

› Draw inspiration from the European Civil Protection Pool, the existing EU civil protection system[44]. This platform owes its functioning to the standardised capabilities proposed by the Member States and validated by the European Commission. To date, 25 participating nations have proposed close to 110 capabilities and 77 of them have been certified. These certified capabilities can be deployed at any time, inside or outside of the EU, when a Member State submits a request to the Emergency Response Coordination Centre (ERCC)[45]. The mechanism was used 102 times in 2020.

44. "European Civil Protection Pool", *European Commission,* 28 May 2021.

45. "Emergency Response Coordination Centre", *European Commission,* 28 May 2021.

16 STRENGTHEN THE **PROTECTION** OF **EU INFORMATION SYSTEMS**

BACKGROUND The European Union must help the 27 Member States raise their cybersecurity levels. It must also ensure the security of its own information systems, which will be all the more targeted as Europe seeks to play a leading role in the digital sphere.

According to the Director General of the French National Agency for the Security of Information Systems (ANSSI), European institutions are themselves a weak point in terms of cybersecurity, as they are obvious targets, especially for espionage, by virtue of the EU's economic and diplomatic power. Protection of the EU's information and communication systems is therefore not optional: any weakness would undermine the credibility of European efforts for the 27 Member States.

OBJECTIVE Strengthen the operational capabilities of European institutions and raise awareness of cybersecurity amongst all European officials.

RECOMMENDATIONS

- Strengthen the capabilities of the Computer Emergency Response Team for the EU institutions, agencies and bodies (CERT-EU), in conjunction with the European Union Agency for Cybersecurity (ENISA), and of the entire network of computer emergency response teams (CERTs) of the Member States.
- Establish a course dedicated to cybersecurity in the core curriculum for the training of future European managers, especially at the College of Europe.
- Create an ENISA-issued *"Digital Security and Cybersecurity"* qualification that EU officials must earn when they take office. Initial levels can be done through massive open online courses (MOOCs), but subsequent levels intended for senior officials will require in-person training.

STRENGTHEN **CRITICAL INFRASTRUCTURE PROTECTION**

17

BACKGROUND The Directive on Security of Network and Information Systems (NIS Directive), adopted in 2016, was intended to guarantee a high level of security of operators of critical infrastructure within the EU. However, its implementation by the Member States has been uneven, with inconsistencies and disparities in levels of cyber risk management. In addition, digital transformation, accelerated by the COVID-19 pandemic, has intensified the landscape of threats to States and companies. Appropriate and innovative responses are needed[46].

Thus the European Commission has noted several limitations of the NIS Directive, in addition to the insufficient level of resilience of companies active within the EU[47]. Indeed, this directive no longer offers protection against cyberattacks commensurate with increases in attack surface. In December 2020, to address these findings, the European Commission proposed the revised Directive on Security of Network and Information Systems (NIS2 Directive). Currently, it is in the initial stages of the legislative process, as it has yet to be approved by the European Parliament and the Council.

The draft NIS2 Directive is designed to cover more sectors (health, transport, banking, energy, space, pharmaceuticals, agri-food, and others), in particular with regard to digital technology (infrastructure, social media, data centres, etc.). It proposes redefining operators of essential services (OESs) as *"essential entities"*[48] and digital service providers (DSPs) as *"important entities"*[49].

In other words, operators of critical infrastructure will be subject to new obligations intended to guarantee the resilience of their networks and information systems. They will therefore have to adopt all appropriate technical and organisational measures to manage cyber risk, including those risks related to supply chains, by securing their relationships with suppliers and service providers. In addition, they will report to national authorities not only cyber incidents, but also IT vulnerabilities that they themselves have identified as part of a coordinated vulnerability disclosure (CVD) programme.

46. "Proposal for directive on measures for high common level of cybersecurity across the Union", *Commission européenne,* 16 December 2020.

47. "Joint communication to the European Parliament and the Council – The EU's Cybersecurity Strategy for the Digital Decade", *European commission,* 16 December 2020.

48. Current OESs and companies from new sectors such as agri-food, pharmaceutical research and development, manufacturing of medical devices, and digital infrastructure services (cloud computing, DNS services, etc.).

49. Postal services, waste management companies, and DSPs (online market services, search engines, and social media).

Member States will also gain powers of regulatory control and sanctions. Indeed, they will be able to suspend an entity's licence or authorisation for activities in the event of repeated breaches.

OBJECTIVE Finalise the draft NIS2 Directive with the inclusion of the entire digital product supply chain and accelerate the adoption of this directive by the European institutions.

RECOMMENDATIONS

The following measures would heighten the robustness of the NIS2 Directive:

- Grant the competent national cybersecurity authorities the power of injunction. Like in the United States model, European countries must be able to impose corrective measures on entities within their territories once a flaw has been detected in their information systems. Victims will have 48 hours to take corrective measures under penalty of sanctions. Indeed, most do not gauge the seriousness of the warning messages issued by these national authorities[50].
- Impose a yearly frequency, at least, for security audits of networks and information systems of critical infrastructure operators, conducted by the competent national authorities.
- Include software publishers and hardware manufacturers in the coordinated vulnerability disclosure (CVD) programme.
- Strengthen the obligations of DSPs. An attack on these companies has systemic repercussions because it may grant attackers direct access to all these companies' customers. Hence, a cybersecurity component could be made compulsory in responses to calls for bids from DSPs. As long as this component is optional, the companies with the cheapest bids —which will not cover costs associated with cybersecurity— will win contracts and act as vectors of risk[51].

50. "Audition, à huis clos, de M. Guillaume Poupard, directeur général de l'Agence nationale de sécurité des systèmes d'information sur l'actualisation de la LPM 2019-2025", [Hearing, behind closed doors, of Mr Guillaume Poupard, Director General of the French National Agency for the Security of Information Systems (ANSSI) on the updating of the French Military Planning Law (LPM) 2019-2025], *French National Assembly*, 8 June 2021.

51. *Ibid.*

ENCOURAGE **COORDINATED DISCLOSURE POLICIES**

18

BACKGROUND Policies of coordinated disclosure of vulnerabilities set guidelines for the discovery of vulnerabilities by people outside the organisations concerned. They provide a clear operational framework that protects both people acting in good faith who are anxious to see vulnerabilities patched quickly and organisations that sometimes need time to design and rollout patches.

However, despite their usefulness, these policies are few in number in France and in the EU at large. The situation is all the more worrying as fewer and fewer vulnerabilities are present within code. Most are found in configurations and implementations related to the use of development frameworks and multiple layers of software (cloud computing).

Following the recent attacks on SolarWinds and Colonial Pipeline, the President of the United States signed an executive order imposing new cybersecurity obligations on federal suppliers, in particular the implementation of Coordinated Vulnerability Disclosure programmes. Digital transformation of all activities increases potential exposure to all sorts of vulnerabilities. Some of these vulnerabilities become systemic given the limited array of solutions.

OBJECTIVE Make coordinated disclosure policies mandatory, in particular for the digital supply chain, where vulnerabilities most often have systemic effects. Operators of vital importance, including operators of critical infrastructure, must promptly seize the opportunity to control cyber risk associated with this type of policy. Finally, public procurement must set an example by introducing these policies as requirements for current and future suppliers.

RECOMMENDATIONS

The NIS2 Directive, which is under development, cannot be content to recommend the implementation of coordinated disclosure programmes[52]. Indeed, it should:

- Impose these programmes to the extent possible on *"essential entities"* and *"important entities"*, which will include digital service providers and some government entities. These measures must be seen as a *"business opportunity"* to restore confidence damaged by the numerous rebound attacks in recent months.
- Add an *"active"* component encouraging research on vulnerabilities within a structured, ethical framework by implementing *"bug bounties"* in organisations, thus complementing coordinated disclosure policies, which represent a passive approach.
- Create a European vulnerability registry, entrusted to the European Union Agency for Cybersecurity (ENISA), that lists the vulnerabilities reported within the scope of the NIS2 Directive. Such an instrument will be useful both in improving the transparency of the process and in awarding European contracts for contracting entities.

52. cf. Recommendation no. 17: "Strengthen Critical Infrastructure Protection".

IMPROVE
CROSS-BORDER CYBERSECURITY

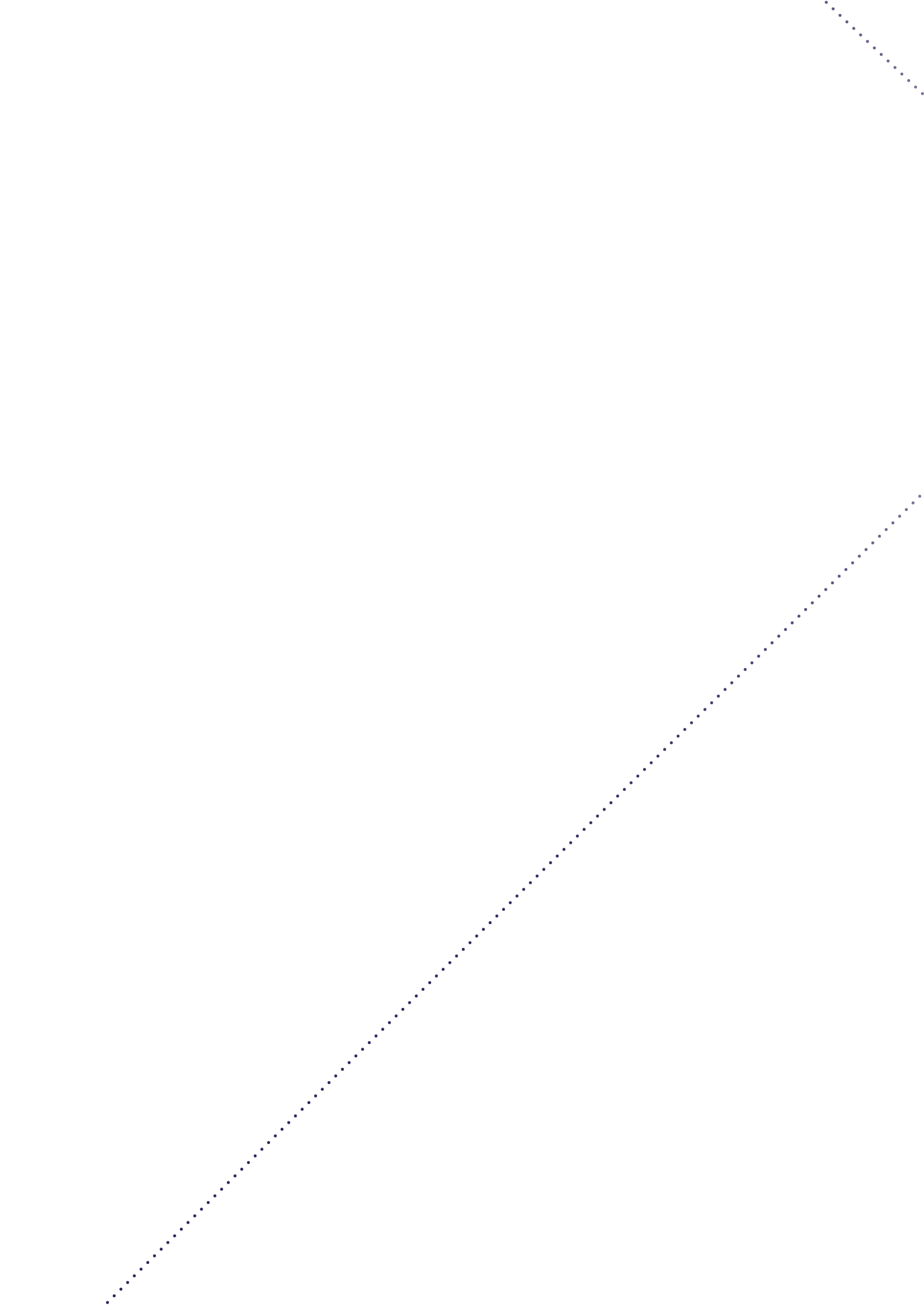
19

BACKGROUND The internal borders of the Union are growing more and more porous, as economic activities are being conducted based on geographic clusters, largely determined by proximity and infrastructure. As a result, the cybersecurity of one State does not end where others begin, especially for bordering States. It is therefore necessary to strengthen cross-border operational cooperation while respecting the sovereignty of each Member State. Common centres for sharing information, similar to Police and Customs Cooperation Centres (PCCCs), which could play a more significant role in the fight against cross-border cybercrime, must be imagined.

OBJECTIVE Create experimental cross-border CERTs, whether generalist or sector-specific (e.g. in the energy sector). This measure, based on the voluntary efforts of the Member States, could be generalised if successful.

RECOMMENDATIONS

› Initially experiment with a cross-border entity that would work in conjunction with national or regional CERTs (under development in France), with the Computer Emergency Response Team for the EU institutions, agencies and bodies (CERT-EU) and with the forces contributing to the fight against cybercrime.



INDUSTRIAL POLICY

Europe has long declined to develop any true industrial policy to promote integration of its internal market by working on supply (competition policy) and demand (trade policy)[53]. Thus, the new industrial policy being developed under the leadership of Thierry Breton, the European Commissioner for Internal Market, marks a turning point. It benefits from initially favourable circumstances: on a societal level, the COVID-19 pandemic has revealed Europe's industrial dependencies and raised its awareness; on an economic level, the United States and China have adopted proactive, if not aggressive, industrial policies making Europe their *"playground"* and, on a political level, the concepts of strategic autonomy and technological sovereignty are finally emerging from the fog to which they had been confined for years. Even better, traditional divisions between Europeans are fading. For example, Germany, which long adhered to strict application of competition law, now shares the need to establish a European industrial policy.

53. Patrice Anato, Michel Herbillon, "L'avenir de la politique industrielle européenne", [The Future of European Industrial Policy], Information Report, *French National Assembly,* 25 March 2021.

20 CREATE A **DIGITAL TRACEABILITY INDICATOR**

BACKGROUND User trust, which is key for digital transformation and adoption of new uses, is increasingly being undermined by the proliferation of attacks and data leaks. It is all the more key given user fears of the emergence of a society of widespread surveillance, raising some concerns and even resulting in the beginnings of rejection. The first symptoms are already showing with biometric technologies and artificial intelligence. Finally, the COVID-19 pandemic brought to light many European dependencies on equipment and digital traffic from non-European countries.

In short, while *"use"* remains the main driver of digital transformation, end consumers are gradually becoming aware of the impact of digital technology on their personal and professional lives and on society as a whole. The recent exodus from WhatsApp[54] following changes to its terms of service shows that end consumers are becoming more and more sensitive to these matters.

Consumer information is now a priority for maintaining and developing trust. Consumers must be able to make informed choices of digital products and services with embedded digital technologies. Users need transparency, among other things, with regard to the location of storage and processing of their data, the chain of subcontractors involved and general terms of service.

On a strategic front, these dependencies must be identified to ensure business resilience through continuity plans, and their reduction or at least their equilibrium must be based on industrial policies. In a digitised and globalised economy, these dependencies are not problematic in themselves. They become problematic when they are ignored, imposed, irreversible or overly exclusive.

OBJECTIVE Make digital products and services transparent to the user.

54. "WhatsApp : pourquoi un tel exode des utilisateurs" [WhatsApp: Why Such an Exodus of Users?], *Le Monde*, 18 January 2021.

RECOMMENDATIONS

- Create a digital traceability indicator, modelled on food products, in the form of labelling established by a third party based on suppliers of each organisation.
- Break down this indicator into three parts: the transparency of the digital value chain, the compliance with the General Data Protection Regulation (GDPR), and the location of the storage and main processing of data in Europe.
- Promote the integration of this indicator into business communication for both B2B and B2C activities. More generally, this system aims to promote companies *"playing the European card"* wherever possible as part of a *"name and fame"* approach.
- Make the indicator compulsory for public calls for bids incorporating a digital dimension as part of a *"Buy European Digital Act"*[55].
- Make the methodology fully auditable to avoid *"black box syndrome"* — precisely what this traceability indicator is intended to combat.
- Strike a compromise between the complexity of certain types of processing and the readability required of any indicator, and quickly reach a critical mass for the indicator to become established on the market.

55. cf. Recommendation no. 22: "Mobilise Public and Private Purchasing".

21 REVITALISE THE **EUROPEAN STANDARDISATION SYSTEM**

BACKGROUND Europe has a long tradition of standardisation; nevertheless, it must be said that it has lost the leadership in this regard that it could claim a few years ago. Standardisation is a major tool of influence and industrial policy. As Ms Claude Revel pointed out, *"international standards/rules represent a major point of application of economic and strategic intelligence. It is becoming increasingly difficult to separate the 'technical' from the political, as technical choices often not only stem from a desire to open up markets or close them to competitors, but also reflect political, ideological, or even societal choices of those who promote them*[56]*"*.

Standardisation is also essential for harmonising and strengthening the internal market. Last but not least, it contributes to the defence of European values. In view of the rise of China —which doubled and in certain cases tripled its participation in international working groups between 2011 and 2018, and today dominates discussions on facial recognition technologies— Europe must urgently make its voice heard. Standardisation is therefore a strategic mechanism that must no longer be seen solely from the perspective of interoperability and integration of the internal market.

OBJECTIVE Support the European Commission's industrial roadmap by revitalising the standardisation system. The European Committee for Standardization (CEN), the European Committee for Electrotechnical Standardization (CENELEC) and the European Telecommunications Standards Institute (ETSI) must have more resources at their disposal for their work on digital challenges[57] and develop their international influence. A heightened presence on international committees (the International Organization for Standardization [ISO] and the International Electrotechnical Commission [IEC]) is thus essential.

Improvements must also be qualitative: to adapt to the speed of technological progress and new uses, standards must be more agile and market responsive. In addition, the standardisation system has become too complex and must be simplified and modernised, as observed in the report *"Calling the Shots"*, prepared by an expert panel chaired by former Prime Minister of Sweden Carl Bildt. These efforts must ultimately be long-term ones, as standardisation yields visible effects only after a number of years.

56. Claude Revel, *Développer une influence normative internationale stratégique pour la France* [Developing France's Strategic International Influence in Matters of Standards], 31 January 2013.

57. Today, just 20% of so-called "harmonised" standards come from standardisation institutions; the rest come from the world of industry.

RECOMMENDATIONS

- Extend the European certification framework established by the Cybersecurity Act to digital services and equipment through multiple certification schemes. The Commission could include, in its next annual rolling plan on standardisation, the development of schemes concerning the Internet of Things (under way), cloud computing (being discussed), industrial systems, artificial intelligence and cybersecurity equipment.
- Develop a security equipment certification with EU-wide validity to decompartmentalise the internal market and allow European manufacturers in the field to distribute their solutions and services across the continent. Moreover, any European regulation that includes matters of digital trust, regardless of the target sector, must be based on the Cybersecurity Act for technical security specifications, in order to avoid each vertical regulation resulting in recreation of new rules and new criteria, thus rendering consistency difficult to ensure.

22 MOBILISE **PUBLIC & PRIVATE PURCHASING**

BACKGROUND Europe invests billions of euros in R&D but is supplied to a very large extent from outside due to a lack of regulation establishing a European preference in certain key areas. This means that one of the essential mechanisms of any industrial policy worthy of the name is not being used to stimulate the development of the European digital industry.

OBJECTIVE Encourage private purchasing with incentives, and public purchasing with a European preference, to foster the development of the European digital industry. Adoption of a *"Buy European Act"* modelled on the *"Buy American Act"* of 1933 is the only measure that can really have an impact on public purchasing. Such a measure is frequently cited, particularly by Emmanuel Macron. Moreover, it is interesting to note that Joe Biden not only is aligned with his predecessor on this subject, but also has even stressed that certain key supplies such as semiconductors, batteries, active ingredients of drugs and rare metals be *"made in America"* (Executive Order 14005). The principle, which has only political value, is not enough. It must be set in stone to have legal force. Of course, this project will arouse strong opposition, especially in Northern Europe. This undoubtedly means that a measure applied by a limited number of countries will have to suffice, at least at first.

RECOMMENDATIONS

- Adopt a *"Buy Digital European Act"* requiring at least 50% of components and services in any public purchase in the digital field to be developed in Europe. Foreign components are not excluded, but their assessment will be weighted with penalties that may be increased if the European competitor is a small and medium-sized enterprise (SME). Such weighting could also be modulated depending on the strategic priorities and the fields in question.
- Establish a tax credit or overamortisation measures for purchasing European digital services and solutions, including cybersecurity, to offer incentives in matters of private purchasing. Although such a measure would have an impact on the budget of the Member States, its cost must be weighed against *"the cost of inaction for the community"*, according to Philippe Vannier, President of the Alliance for Digital Trust (ACN). *"The creation of a cyber tax credit incentive system must be regarded by the State as an investment, not as an expense"*.

› Promote transnational pooled procurement schemes allowing administrations from several Member States to buy together. This condition is key to developing European leaders. The European Innovation Council (EIC) could play a role in this.

23 STRENGTHEN PUBLIC & PRIVATE INVESTMENT

BACKGROUND Investment, both public and private, is an essential element in the development of companies that are leaders in their markets. Europe is still lagging behind the United States, which raise the lion's share of cybersecurity funds: 65% of operations and 77% of the €7.5 billion raised globally (compared to Europe's 24% and 12%, respectively). With the COVID-19 pandemic, funds raised by Europe in this domain (pre-seed, seed, and series A through late-stage operations) even failed to match the €1 billion raised in 2020, thus showing a drop in operations in one year[58].

The average size of funding rounds was also lower: €5.3 million in Europe (€6.5 million in 2019) versus €13.5 million in the United States or Israel. The consequences are clear: in 2020, six of the eight new unicorns in the field of cybersecurity were American and two were Israeli[59]. This weakness does not take anything away from the dynamism of the European industry, which is even becoming more and more attractive, despite a highly partitioned domestic market, as shown by the acquisitions of Alsid and Sqreen by the American companies Datadog and Tenable. However, it does carry an air of missed opportunities.

OBJECTIVE Mobilise all public and private instruments to accelerate the growth of European cybersecurity gems, which need to grow and struggle to find not only seed money but also funds for development, especially where development requires a major infusion of capital.

58. 183 operations in 2018 versus 153 operations in 2019.

59. ACE Management, *Ace Barometer of European Investment in Cybersecurity,* May 2021.

RECOMMENDATIONS

Use existing public funds to finance European companies on a priority basis:

- Agree, though the European Investment Bank (EIB) and the European Investment Fund (EIF), to more favourable conditions to companies, including small and medium-sized enterprises (SMEs) and intermediate-sized enterprises. The latter have difficulty negotiating conditions that do not cut too deeply into their intellectual property rights.
- Fund industrial projects, including startups and SMEs, with the European Defence Fund, which has a budget of €100 million for cybersecurity (2021-2027).
- Invest in technology-intensive sectors like cybersecurity by mobilising the European Innovation Council (EIC)[60]. This fund, launched in March 2021, will dedicate €3-3.5 billion to direct participation[61] and €6-7 billion to loans and subsidies.
- Make use of Digital Europe programme[62], aimed at bringing digital technologies to companies, citizens and government entities, and of the Connecting Europe Facility[63] for infrastructure development. These instruments, with respective budgets of €7.5 billion and €400 million for 2021-2027, constitute an indicator of trust in private investment.

With regard to the private sector, although the proliferation of attacks has already fuelled a renewed interest in cybersecurity companies, it is essential to accelerate investments through fiscal and regulatory incentive measures, as well as *ad hoc* funds able to support entrepreneurs.

60. "Commission launches European Innovation Council to help turn scientific ideas into breakthrough innovations", European Commission, 18 March 2021.
61. Up to €15 million in its own funds for a capital share of 10-25%.
62. "The Digital Europe Programme", *European Commission,* 2021.
63. "Connecting Europe Facility", *European Commission,* 2021.

24. FACILITATE TECHNOLOGY TRANSFER

BACKGROUND The link between academic research and companies is not working well. Very few startups emerge from the world of academia[64]. Just 4 of the 116 European unicorns are university spin-offs[65]. This means that a large part of European research, in particular in the digital domain (artificial intelligence, cybersecurity, etc.), does not lead to industrial projects. The main reason is that academic entrepreneurship is not sufficiently encouraged, and researchers receive little support in making the leap from research to the private sector. Even worse, they are often mired in a cumbersome and inefficient bureaucracy that discourages them. Intellectual property claims made by research centres and academic laboratories represent yet another obstacle. Whereas American universities require only 5-10% of the capital of companies created, European universities usually demand 25-50%. The same applies to royalties, even though it sometimes takes several years for startups to convert technologies into operational solutions.

OBJECTIVE Streamline technology transfer from academia to the private sector. Yeda (Israel) and Stanford Research Park (United States) are dedicated organisations that appear to be models worthy of emulating. Stanford Research Park has 150 companies employing 25,000 people. Yeda, which has the distinction of being a private company, has succeeded in spawning 73 companies with a combined turnover of $28 billion[66].

64. Read in this regard: Nathan Benaich, "Universities in the UK and Europe have a start-up problem", *Financial Times,* 10 May 2021.

65. Of particular note is the success of Darktrace, a pioneer in threat detection that was created based on technologies developed at the University of Cambridge (United Kingdom).

66. "Yeda, Israël et le bureau de transfert de technologies de l'Université de Genève" [Yeda, Israel and the Technology Transfer Office at the University of Geneva.], *IsraelValley,* 7 February 2019.

RECOMMENDATIONS

The understanding of intellectual property in the digital sphere cannot be the same as in other fields such as biotech: the developer of a code must be able to own it in order to update it permanently without having to manage the thorny problem of co-ownership. Projects must thus be accompanied by professionals in entrepreneurship with a real vision of the market and uses. Several options may facilitate transfer:

- Institute a standard technology transfer agreement providing for a limited capital share of 1-5% and realistic amounts for licences, and make sure that such agreement does not take effect in initial years, so as not to stifle startups or discourage creators.
- Ensure that technology transfer organisations are at no risk of conflicts of interest. Such organisations must not license products themselves or place their own employees in the companies that they support. The stakes of the different stakeholders must be aligned and, to the extent possible, commensurate with the risks taken.
- Create dynamic systems of alumni, who should be seen not as *"wallets"* but as *"mentors"*, to encourage dovetailing of academia and entrepreneurship.
- Bring academia and investment funds closer together to fund deep tech, the development of which requires lengthy maturation periods.

25 IMPROVE **SUPPORT** FOR **INNOVATION**

BACKGROUND Since 1984, about €200 billion have been allocated by the European Commission to R&D, including €95.5 billion under Horizon Europe (2021-2027), €6.8 billion under the Digital Europe programme, and €1.8 billion under the interconnection mechanism in Europe. While the interdisciplinary nature of the projects supported is a source of global envy, the return on investment of these projects becomes uncertain when they suffer from scattering, competition amongst themselves, funds that are spread too thinly, bureaucratic dysfunction and dilution of responsibility. Despite starting with a commendable goal—to protect public funds and prevent fraud—the functioning of these projects has ultimately obliterated any appetite for risk, which is simply part and parcel of R&D.

OBJECTIVE Focus European R&D budgets on certain key objectives (quantum computing, AI, cybersecurity, etc.) and avoid current bad distribution practices. This is especially important since the budgets allocated to digital technologies are already not on a par with those of GAFA (Google, Apple, Facebook and Amazon). The budget for the Digital Europe programme, for example, amounts to just 1.8% of Amazon's investments in 2018, and the annual budget for Horizon Europe (€13.6 billion) is equivalent to the R&D budget of the holding company Alphabet alone[67].

RECOMMENDATIONS

Several courses of action would avoid poor R&D budget distribution practices:

- Establish a system of project assessment, void of complacency and considerations of nationality, as early as one year after project launch to identify what should be kept and what should not.
- Ensure better coordination among existing programmes, in particular Horizon Europe, Digital Europe and the EU space programme, following the example of the European Commission's action plan in 2021 to improve synergies among the civilian, space, and defence industries.
- Accelerate the implementation of the Recovery and Resilience Facility (NextGenerationEU). To do this, EU research policy must be subject to better governance. The missions of the recently created European Innovation Council (EIC) must therefore be clarified.
- Grant deep tech a place of its own in research programmes. *"Moonshots"* bringing together industry, academia and government around major thematic challenges must also be developed, following on the proposal of the Joint European Disruptive Initiative (JEDI) modelled on XPRIZE, which has been organising large-scale competitions on themes with a strong impact on society since 1994.

67. Ophélie Coelho, *Quand le décideur européen joue le jeu des big techs* [When European Decision-Makers Play the Big-Tech Game], Institut Rousseau, June 2021, p. 36.

BRING ABOUT THE **EMERGENCE OF EUROPEAN LEADERS** IN **CLOUD COMPUTING**

26

BACKGROUND Digital sovereignty covers two concepts: data sovereignty and technological sovereignty. When it comes to cloud computing, Europe today does not have either[68], and 50-70% of Europe's data are stored in the United States[69].

This dependency has multiple consequences for organisations: irreversibility, vendor lock-in, application of extraterritorial laws, legal risks with regard to the General Data Protection Regulation (GDPR), and even *"uberisation"* and disintermediation between organisations and customers. Beyond data, entire business processes are gradually moving to the cloud. This carries a risk of disruption of many value chains in favour of non-European digital platforms.

Hence, organisations must fully appreciate the *"transformational"* power of cloud computing. The choice of a solution is of course made based on how well it meets functional and technical criteria, but that choice also represents a binding long-term strategic decision. This is especially true considering that dependency on the cloud will only grow as digital transformation proceeds. Today, just 36% of European companies have adopted cloud computing[70], but this figure is expected to double by 2023.

It is therefore dangerous to succumb to fatalism and take European dependency for granted. Europe has lost a battle in not making a timely shift to cloud computing, but has not lost the war. It boasts not only high-performance industries fully engaged in digital transformation, but also dynamic digital service companies and cloud suppliers that have the capacity to be competitive on the global market. To be sure, it is essential to position oneself on tomorrow's technological game-changers, in particular quantum and edge computing as well as artificial intelligence. However, cloud computing is the foundation on which these technologies are built. There will be no digital sovereignty without infrastructure control.

OBJECTIVE Promote the emergence of European heavyweights in cloud and edge computing[71] while embedding these technologies in the 14 strategic industrial ecosystems identified by the European Commission.

68. European Commission, *Strategic dependencies and capacities*, 5 May 2021.
69. Ophélie Coelho, *Quand le décideur européen joue le jeu des big techs* [When European Decision-Makers Play the Big-Tech Game], Institut Rousseau, June 2021.
70. Estimated expenditure: €54 billion in 2020.
71. Edge computing consists of processing data as close as possible to the source of those data at the edge of the network.

RECOMMENDATIONS

While data sovereignty cannot tolerate any compromise, the EU currently has not much choice, technologically speaking, but to enter into agreements with external partners to gain a certain amount of control over its infrastructure. The market will not suffice to restore balance and bring about the emergence of European players able to compete with American and Chinese giants. Europe must quickly take comprehensive action with regard to its industrial policy:

- Raise awareness and thus transparency among players. Location is not the sole criterion for data sovereignty. It is also important to know how data are stored, used and collected, by whom, and under what contractual framework, and which extraterritorial laws apply to a cloud service (irrespective from the location of storage) that would oblige providers to transmit or disclose customer data based on non-EU statutory orders.

- Certify offers around the principles of reversibility, transparency, and interoperability. The Gaia-X project plays an essential role from this point of view, but care must be taken not to make any concessions if this project is to serve as a *"launching pad"* for technological sovereignty.

- Pursue industrial alliances within the framework of the European Commission's new industrial policy. The launch of the European alliance for Industrial Data, Edge and Cloud should be to strengthen the EU's industrial capacities in the global market for cloud end edge cloud solutions. It should also help to promote an EU model to cloud computing which is centred on European values such as data sovereignty as well as a technological approach that favours highly distributed, secure and energy-efficient data processing. To this end, the European Commission should aim to promote synergies with industry driven projects such as *"GAIA-X"* as well as Member State initiatives such as the currently prepared Important Project of Common European Interest on Cloud and Infrastructure Services (IPCEI-CIS). Together, these initiatives can contribute to the development and deployment of state-of-the-art Cloud and Edge Computing capacities from within Europe, providing businesses and public authorities with a real choice that meets the highest standards in terms of performance, data protection, security and sustainability. This tool, already used for microelectronics and batteries, has enabled Member States to make public grants to certain innovative projects since 2014. While this mechanism can be leveraged to bring about the emergence of European leaders in cloud computing, it must be simplified, and its eligibility requirements must be expanded. It also assumes reliance on industrial *"roots"*, public and private orders, and the necessary skills. Moreover, a new form of governance must be found. The informal industrial forum for IPCEIs, whose mandate ended in 2020, must be replaced by an executive committee able to make decisions[72].

72. Patrice Anato, Michel Herbillon, "L'avenir de la politique industrielle européenne" [The Future of European Industrial Policy], *Information Report,* French National Assembly, 25 March 2021.

PROMOTE THE **DEVELOPMENT** OF A **EUROPEAN DIGITAL IDENTITY**

27

BACKGROUND Just 59% of the European population and 14 of the 27 Member States have a national digital identity system. However, the challenges raised by digital identity are essential for several reasons, in particular for the economy and the development of the internal market (legal basis of the eIDAS Regulation), European citizenship (education, access to healthcare, democratic participation and free movement), and the development of digital sovereignty. It is in fact inseparable from a common digital identity or a framework of interoperable national identities.

In general, digital identity affords users better control of their data and context-dependent dynamic use. It is a major mechanism for public transformation and the simplification of the citizen–state relationship. Digital identity also enables simplification and optimisation of so-called *"know your customer"* (KYC) guidelines, which are becoming increasingly common, as well as development of strategies for electronic health, personalised transport and frictionless payments.

The COVID-19 pandemic has only heightened the urgency of a European digital identity. If nothing is done, adoption of American or Chinese identification solutions will deprive Europe of intermediation laden with added value and cybersecurity benefits as well as the ability to enforce European law in the digital sphere. To meet this requirement, the European Commission set itself in its Digital Compass two objectives to be achieved by 2030: for 80% of Europeans to use a digital identification solution and for all EU public services to be available online.

In June 2021, the European Commission proposed a new version of the eIDAS Regulation. Its text provides for strengthening obligations to use trusted digital identities within both the public sector and the so-called *"regulated"* private sector. At the same time, its provisions call for greater flexibility in terms of required identity attributes, thus opening up digital identities to a wider variety of uses (banking, health, etc.). In addition to promoting the use of mobile devices, the proposal envisages more possibilities for certification of identity attributes by public and private services and proposes the creation of additional Europe-wide digital trust services such as archiving, including on a qualified level.

OBJECTIVE Adopt trusted digital identities in a manner suited to uses, at least for the public sector and for the regulated private sector.

RECOMMENDATIONS

- Promote the adoption of the new version of the European Commission's eIDAS Regulation.
- Encourage adoption of digital identities by the regulated private sector by introducing requirements for compliance, risk prevention, transparency and anti-money laundering/combatting the financing of terrorism (AML/CFT), and prevention of cyber risks through minimum consistent levels of trust (identification and authentication/federation), similar to those that exist in the financial sector (EU Revised Directive on Payment Services [PSD2]/French Monetary & Financial Code [CMF]).
- Promote, in addition to discussions with the European Parliament on the eIDAS Regulation, negotiations among Member States to rapidly deploy pilot projects with funding from the Digital Europe programme. The objective is to limit disparities among States, which will remain sovereign in matters of project implementation. The pilot projects could also make substantial contributions to decentralised, or self-sovereign, identity systems using blockchain technology.
- Defend, on an international level, the adoption of an open, interoperable standard, such as the Open Standards Identity API (OSIA)[73], enabling States to freely choose identity suppliers while ensuring real online interoperability with the levels of privacy and security required by Europeans. Indeed, France and the EU cannot remain indifferent to the *"API-fication"* movement, which is influencing identity information exchange protocols now as it did telecommunications and open banking yesterday.

73. The OSIA initiative is led by the Secure Identity Alliance.

ACCELERATE **IMPLEMENTATION** OF **REGULATION** OF **SYSTEMIC PLAYERS**

28

BACKGROUND The past 20 years have seen the rise of a handful of companies to the forefront of the digital industry. Through their innovative and diverse service offerings, these players have established themselves —in terms of number of users, market capitalisation and market share— in several segments to the point of totally structuring them (social media, cloud computing, operating systems, etc.)[74].

These companies operate digital platforms whose development model is based on collection of users' personal data. The network effect inherent to these digital platforms sometimes leads to monopolisation of services[75] and renders them essential and *"systemic"*. The biggest examples of such platforms are GAFAM (the American companies Google, Apple, Facebook, Amazon and Microsoft), followed by BATXH (the Chinese companies Baidu, Alibaba, Tencent, Xiaomi and Huawei). The digital single market is also subject to mergers, which carry risks of abusive practices and disruption of proper competition.

The dismantling of these actors —which impose their economic, social, and even political rules— is often evoked in the name of antitrust legislation. However, such a prospect seems unlikely given the strategic advantage that these companies represent for the digital powers and the technical and financial difficulties that a proper dismantling would create. Even if the acquisition of value by these giants is real, the dependence of our startups and companies on them for the development of their applications should not be underestimated.

Europe is not taking stock of this *"gigantism"* for lack of suitable digital regulation. In 2011, the EU approved Microsoft's acquisition of Skype; as a result, Microsoft alone then accounted for 85% of the video communication market[76]. This operation was a symptom of a broader gap between the EU's industrial policy and its competition law, as evidenced by the fact that it recently refused to form a European heavyweight in the rail industry while allowing the Chinese leader, with the support of its State, to enter the European domestic market. China, for its part, does not allow European companies in the sector to break into its own domestic market. This trend reflects a lack of control on foreign firms[77].

74. Alain David, Marion Lenne, "Les géants du numérique" [The Digital Giants], *Information Report,* Foreign Affairs Committee, French National Assembly, 2 June 2021.

75. "DMA: A New Role for Competition Authorities", *Institut Montaigne*, 26 February 2021.

76. European Commission, *COMP/M.6281, Microsoft/Skype,* 7 October 2011.

77. Patrice Anato, Michel Herbillon, "L'avenir de la politique industrielle européenne" [The Future of European Industrial Policy], *Information Report,* French National Assembly, 25 March 2021.

To ensure *"fairer"* markets, the European Commission presented the Digital Markets Act (DMA) in 2020. This act is intended to situate digital markets in a more equitable trading environment by imposing obligations on systemic players and promoting the emergence of small companies.

OBJECTIVE Strengthen the provisions of the Digital Markets Act (DMA) and accelerate the adoption thereof.

RECOMMENDATIONS

Given the stranglehold gatekeeping giants have on digital markets, a robust DMA will boost competition by introducing *ex ante* regulation, in addition to the *ex post* intervention of the competition authorities of the Member States.

- Strictly apply competition law to digital markets while taking into account strategic considerations as required by competition from systemic players.
- Clarify the distinction between the prerogatives of the EU's Directorate General for Competition (DG COMP) and national competition authorities to promote complementarity and synergies between them.
- Endow the European Commission with an economic intelligence service[78] responsible for analysing the behaviour of major foreign competitors, as well as mergers and acquisitions to restrict those likely to be predatory for EU businesses and innovation[79].

78. *Ibid.*

79. France, Germany and the Netherlands, *Strengthening the Digital Markets Act and Its Enforcement*, May 2021.

CONCLUSION

Under the motto ***"Relance, Puissance, Appartenance"*** [Recovery, Power, Belonging], the French Presidency of the Council of the European Union, which will take place in the first half of 2022, will have the task of fulfilling the three aspirations described in that motto in the digital realm. It will thus continue, if not initiate, a dynamic that will enable Europe to:

- Ensure ***"recovery"***. During the French Presidency, the EU will have to put its new industrial strategy on a launching pad, making every effort (in terms of public and private purchasing, technology transfer, etc.) to accelerate its digital transformation and have an industry in this domain.
- Become a digital ***"power"***. To cease being a mere *"colony"*, Europe must continue to promote a regulated, balanced and interoperable digital sphere in diplomatic forums while developing its own cybersecurity and cyber defence capabilities.
- Develop a sense of ***"belonging"***. In addition to strengthening its citizens' digital acculturation and training, the Union will have to reflect on its *"digital identity"*, which must be based on awareness of Member States' common destiny and on interoperable *ad hoc* systems.

In tomorrow's digital Europe, cybersecurity must be at once a cornerstone and a spearhead: a cornerstone to ensure collective resilience in a context of digital transformation, and a spearhead to defend and promote European interests in a world marked by the *"return of powers"* and by global strategies in which cyber affairs occupy a growing place. Power cannot be solely digital, but it must have a digital dimension.

Far from signifying a withdrawal into itself, the digital sovereignty to which Europe aspires is on the contrary a historic opportunity for it to find its way, both internally and internationally.

Within the EU, although matters of digital affairs unite more than they divide, arrival at a consensus among 27 Member States always takes time. Given the urgency of the challenges, including challenges related to industrial policy, *ad hoc* cooperation and associations must be encouraged in order to quickly restore Europe as a driving force. New alliances on key technologies such as semiconductors, cloud computing and artificial intelligence will consolidate Europe as such.

Globally, the EU has a voice, despite the United States–China duopoly. Protection of personal data, transparency of algorithms, prohibition of hack-back, the fight against the proliferation of cyber weapons, and the promotion of an open, free, stable and secure digital sphere: in all these matters, Europe endeavours to chart a middle course, rejecting totalitarianism of any kind. While it is an exaggeration to say that Europe's actions are awaited, they are indeed watched. This does not confer any rights upon Europe; on the contrary, it creates requirements for the continent.

First and foremost, it creates an **operational** requirement: Europeans must be able to respond to the proliferation and sophistication of cyber threats, as well as security vulnerabilities anywhere they may be present in the digital sphere, including in information, as democracies are by nature more vulnerable to manipulation of information. Next, it creates an **ethical** requirement: whereas concessions can conceivably be made in terms of technological sovereignty, for tactical reasons, users' sovereignty over their identities and personal data is non-negotiable. Finally, it creates a **political** requirement: to accept technological progress and benefit from globalisation and digital transformation, European citizens expect a strong, innovative Union.

To succeed, Europe must play the long game. The six months of the French presidency will be an anecdote in the annals of history. As stated in the digital strategy presented by the European Commission in March 2021, the entire decade must be digital, and the success of today's policies can only be measured in 2030. This means that the French presidency is beholden to a methodological requirement: more than create new structures in an environment already loaded with them, it must deepen, coordinate, network and set the pace of existing ones. This must be done in coordination with Germany, Portugal and Slovenia, which preceded France in the presidency, as well as with the Czech Republic and Sweden, which will follow France in it.

France is often criticised for seeing the EU only through the prism of its own interests; it will have to shift its focus sufficiently to defend not purely French but European interests. There will be no European power without clearly defined common interests.

This Europe of cybersecurity will need to strike a balance between necessary pooling of standards and capabilities and respect for the sovereignty of each Member State, which remains inviolable in attacks on defence and national security. Thus, more capabilities at European level does not mean less capabilities in each Member State—on the contrary.

This more collective, more collaborative Europe is focusing its efforts on the security of critical infrastructure, the protection of the single market and, more recently, the regulation of content and platforms. However, the fight against cybercrime remains overly neglected, even with the EU playing an important role in the progress of the Budapest Convention and in improving conditions of access to digital evidence (e-evidence regulation). **Cybersecurity is achieved with a combination of information systems security, the fight against cybercrime, and cyber defence**. Each of these three crucial elements plays an essential role in forging a *"European shield"*. In truth, the ambition would be more to create a European *"testudo formation"* that protects against threats from every angle, with each Member State being required to create its own shield that is interoperable with all the other shields and reinforced where needed by a collective mechanism of prevention, repression or defence.

The above recommendations, which emerged from a discussion amongst many French and European experts from the public and private sectors, may seem to reiterate ideas that have already been put forward and programmes that are in progress or planned. They are merely intended to illustrate that which should underpin the dynamics of the French Presidency of the Council of the EU. **This presidency must first put European cybersecurity in perspective and accentuate its political and strategic dimensions by placing European citizens at the heart of the debate.** These citizens —both consumers and victims— expect Europe to protect them in their identity, security and decision-making autonomy. Without abandoning the discourse focused on organisations, infrastructure and companies, it is important to afford citizens a place in a collective vision of a European future that brings progress and security for all. **The French presidency must breathe new life into such a vision at a time when the COVID-19 pandemic is driving people away from a solidarity mentality and prodding them into looking out for themselves alone.**

ACKNOWLEDGEMENTS

The FIC Agora would like to thank everybody who was interviewed or consulted in the preparation of this White Paper:

Henri d'AGRAIN, General Delegate of CIGREF

Gilles BABINET, Co-president of the French National Digital Council (CNNum)

Bertrand BADIE, Professor at Sciences Po Paris

Karine BANNELIER, Lecturer at the University of Grenoble Alpes

Annegret BENDIEK, Researcher associated with the German Institute for International and Security Affairs (SWP)

Bernard BENHAMOU, Secretary General of the Institute of Digital Sovereignty (ISN)

Paula BROUILLARD MOLINA, Communication and Media Officer at the DG Connect

Théodore CHRISTAKIS, Professor at the University of Grenoble Alpes

Mireille CLAPOT, Member of the French Parliament and President of the French Higher Commission for Digital and Postal Services

Tanguy de COATPONT, Director General of Kaspersky Lab France

Christian DAVIOT, Former Strategic Advisor to the Managing Director of the French National Agency for the Security of Information Systems (ANSSI)

Olivier EZRATTY, Independent consultant and specialist in digital technologies

Guy de FELCOURT, Expert on digital identity issues and co-organiser of the ID FORUM

Brigadier general Éric FREYSSINET, Deputy Commander of the French Gendarmerie for Cyberspace, Ministry of the Interior

Jean-Noël de GALZAIN, Founder of Wallix and President of Hexatrust

Lieutenant colonel Étienne GIRARD, Head of the EU office of the French Directorate for International Cooperation (DCI), Ministry of the Interior

Benoît GRUNEMWALD, Cybersecurity expert at ESET

Yoann KASSIANIDES, General Delegate of the Alliance for Digital Trust (ACN)

Wolfgang KOPF, Senior Vice President Group Public and Regulatory Affairs at Deutsche Telekom

André LOESEKRUG-PIETRI, President of the Joint European Disruptive Initiative (JEDI)

Julien NOCETTI, Researcher associated with the French Institute of International Relations (IFRI)

Aurélien PALIX, Deputy Director of Networks and Digital Uses at the French Directorate General for Enterprise (DGE), Ministry of the Economy and Finance

Army general (Rtd) Jean-Paul PALOMÉROS, Former Supreme Allied Commander Transformation at NATO

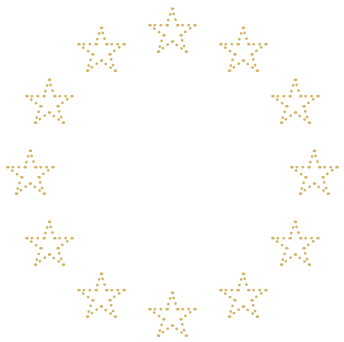
Sylvain ROURI, Executive Director at OVHcloud

Tadej RUPEL, Ambassador and National Coordinator for External Aspects of Digitalization, AI & Cyber Security of Slovenia

Rayna STAMBOLIYSKA, Vice President of Governance and Public Affairs at YesWeHack

Major general Didier TISSEYRE, Commander of Cyber Defence of the French Ministry for the Armed Forces

The opinions expressed in this White Paper are not binding on the above-mentioned individuals or the institutions that they represent.



Agora FIC

FORUM-FIC.COM