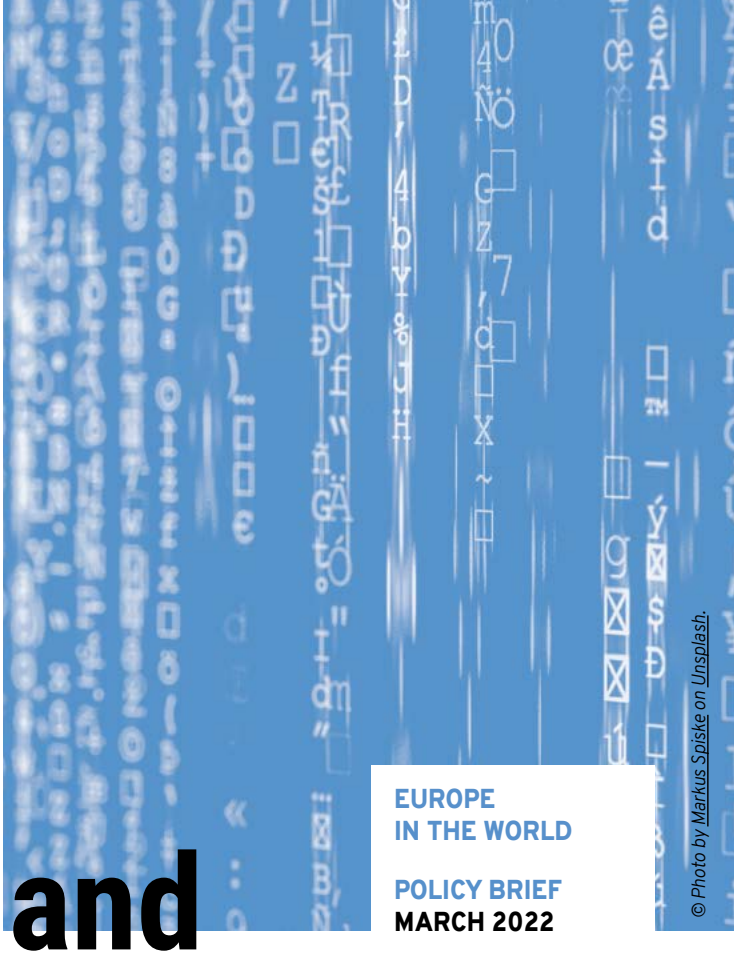
NOTRE EUROPE
Jacques Delors Institute
Penser l'Europe • Thinking Europe • Europa denken



© Photo by Markus Spiske on Unsplash.

EUROPE IN THE WORLD

POLICY BRIEF
MARCH 2022

#Defense
#Digital
#Security

European cybersecurity and data privacy

Threats and prospects

Arnault Barichella
Expert fellow on cybersecurity

I • Threats associated with cybersecurity and data privacy in Europe

I DIGITALIZATION OF CRITICAL INFRASTRUCTURE

Critical infrastructure across Europe has been undergoing a "digital revolution". While the nature of this revolution is complex, mechanical and analogue processes are gradually being replaced by computer software and digital technologies. Globalized competition and interconnections between firms or entities across different sectors have enhanced pressure to accelerate digitization. The imperative to rationalize production, consumption and distribution processes, the requirement to rapidly transfer information and data over long distances, along with a need to enhance internal communications between management sites and infrastructure have hastened the transition. Most infrastructure essential for the functioning of society is included: vital sectors such as the water supply, healthcare, transportation, communications, energy, along with key aspects of the economy, services, and security assets (police/military).

A variety of different types of digital systems have been relied upon in Europe, adapted to the specificities of each sector. This includes, for example, "industrial control systems" (ICS) and "supervisory control and data acquisition systems" (SCADA) for many industry-related fields, which enable the remote handling of equipment. This has contributed to optimizing the whole supply chain, providing a wider selection of tailored goods and services, with real time data from computer systems enabling the development of consumer profiles. These elements have considerably expanded the margins of manoeuvre for companies to enhance profits. Public sector entities have also benefitted from improved efficiency and rationalization. While offering many benefits, however,

the "digital revolution" is two-sided, since it has also generated acute new risks and threats in terms of cybersecurity and data privacy.

These vulnerabilities are multi-faceted and have emerged under many different guises. For instance, while European networks used to be relatively closed under analogue and mechanical processes, digital technologies have opened up equipment and infrastructure to the Internet, leading to significant transfers and sharing of data with external systems. This has led to the multiplication of operators relying on the "Internet of Things" (IoT), which involves physical objects or devices connected to the Internet that exchange data and interact with other similar systems. Moreover, a number of sectors, such as industry, transportation, the water supply, energy and healthcare, often possess long-term investment cycles, which means they may rely on infrastructure that was built before cybersecurity was considered to be a major threat. Hence, equipment and systems were often not designed to protect against cyberattacks, but prioritized reliability instead. This also renders it harder to access the history of infrastructure configuration, which can increase difficulties to upgrade equipment today. In addition, many sectors possess unique or at least fairly distinct characteristics, which means that cyber protection systems often cannot easily be transferred from one sector to another.

Cyberattacks enable potential hackers to target multiple weak points simultaneously, unlike physical damage resulting from sabotage for example. In many cases, only a few vulnerable openings within a system are needed for a virus to subsequently spread across the whole network. This is exacerbated by the fact that digital systems are rapidly and continuously evolving through new software and system upgrades, which may contain so-called "zero-day" vulnerabilities. The latter involve cyber weaknesses that were not anticipated during the design of a new technology, and can remain undetected for years after subsequent commercialization. Time and again, human error and negligence are also responsible for the intrusion of a cyber virus, often due to a lack of training for personnel, which opens the door to hacking. Inadequate training for all sectors, including both public and private entities, is a recurring problem across Europe. Hence, **the risk of escalating system collapse is real, especially since different sectors are very much interconnected.** This means that a cyberattack originating in the energy industry, for example, may rapidly propagate to infect other key sectors like healthcare, transportation, communications, banking, finance/insurance, along with defence or the military, potentially bringing society to an abrupt halt.

TYPES OF CYBERATTACKS AND DATA PRIVACY BREACHES

The frequency and sophistication of cyberattacks has exponentially increased over the last few years. Due to the far-reaching ambit and scope of the digital revolution, practically all sectors have been impacted, even though there can be variations within different sub-fields. Such attacks increasingly target not only private sector firms but also public institutions like national departments and ministries, affecting both administrative offices and physical infrastructure, with the two often being interconnected. **Thousands of attacks are reported each year across Europe, with companies and institutions now facing cyber threats on a daily basis.** While they have emerged under numerous different configurations, cyberattacks can generally be divided into the following three broad categories:

1. Disrupting the supply or provision for a service.
2. Damaging equipment by affecting the integrity of systems and/or infrastructure.
3. Espionage to appropriate confidential information or data.

Cyberattacks may sometimes combine several of these characteristics, even though the majority of reported hacking continues to be linked to financial motivations. This usually involves cyber espionage to appropriate confidential information, often conducted by hackers forming part of a criminal organization, who then seek to sell stolen data onto the black market. The pattern has been exacerbated by the rise of "big data" platforms storing large amounts of personal data through outsourcing processes that are not always secure. In some

cases, these processes circumvent the safeguards provided by EU legislation on privacy protection (see below). The trend is towards a growing reliance on so-called "cloud computing" technologies, which use remote Internet servers often based in countries outside Europe to store and process massive quantities of data, as opposed to relying on local or personal servers.[1]

While largescale cyberespionage can be very profitable, it remains problematic to implement since it requires advanced technical IT competences and extensive resources to put together the operation over several months. Consequently, experts have indicated that **prominent countries have likely been sponsoring a growing number of cyberattacks over the last few years**, including through both monetary and organizational patronage. **Geopolitical dynamics are now widely believed to be a major factor behind a growing number of cyberattacks around the world, including in Europe.** Although geopolitically-motivated hacking often aims to disrupt or damage systems and equipment, cyber espionage has often been an underlying motivation.

Given the potentially highly destructive effects stemming from **cyberattacks, they may be considered to constitute an act of war**. Nevertheless, identifying the origin of a cyberattack continues to be very difficult, especially due to the frequent display of bogus flags by hacker groups. Hence, governments may launch large-scale cyber assaults, while not overtly revealing themselves. Identification can also be difficult due to the fact that there is on average a six to seven months' time-lag before discovery of a virus that has compromised equipment or a system, which exacerbates the challenge of developing an effective response. Moreover, while cyberattacks often target specific firms or institutions within a designated country, they subsequently tend to spread internationally. This is due to the globalization of digital technologies and economic interdependence, since large companies often possess subsidiaries around the world. The table below summarizes characteristics from several of the main cyberattacks that have hit Europe over the last few years:

(see table below)

II . Policy prospects on cybersecurity and data privacy in Europe

THE EU'S "COMPREHENSIVE" APPROACH TO CYBERSECURITY, DATA PRIVACY AND ARTIFICIAL INTELLIGENCE

In order to address the growing cybersecurity risks and threats stemming from the accelerating "digital revolution", the EU has gradually enacted a number of notable policies and legislation during the last few years. Over time, these have evolved to constitute a distinctive approach, which can be characterized as both "comprehensive" and "flexible".[2] The "comprehensive" element involves the EU's ambition to simultaneously tackle a wide range of different issues in relation to cybersecurity. This includes a focus on critical infrastructure in general, addressing both data security and data protection, growing attention to the emerging field of artificial intelligence (AI), along with potential links to the sustainable energy transition.

Firstly, the "comprehensive" dimension is apparent in EU legislation on data privacy. The General Data Protection Regulation (GDPR), enacted in 2016 and operational since 2018, replaced the previous 1995 Data Protection Directive. The GDPR is notable since it aims to cover both "data protection" (restricting the unwarranted appropriation of personal data) and "data security" (rules to handle the processing of data once collected). The GDPR represents one of the world's most far-reaching legislative initiatives in this field, with comprehensive provisions that are strictly enforced and sanctions for non-compliance, potentially tallying up to €20 million or 4% of global annual revenues for private entities.

Secondly, the EU Commission has recently indicated its intention to develop a European

1 Barichella A. (2019), *The US-EU Rivalry for Data Protection: Energy Sector Implications*, Édito Énergie, Ifri.
2 Barichella A. (2018), *Cybersecurity in the energy sector: a comparative analysis between Europe and the United States*, Études de l'Ifri, Ifri.

Year	Name	Target	Consequences	Objective	Assailant
2015	Black Energy	Ukrainian electricity network	• 30+ electrical operators disconnected from the network for several hours. • 200,000+ people impacted. • Infrastructure severely damaged. • Spread to a number of EU countries with commercial ties to Ukraine.	• Supply disruption • Equipment damage	• Russia suspected
2017	NotPetya	Ukrainian critical infrastructure & computer network	• 30% of all computer systems in Ukraine infected. • $10 billion in damages. • One million people affected (in banking, national ministries, electricity operators, newspapers, etc.) • Spread to EU countries with commercial ties to Ukraine.	• Supply disruption • Equipment damage • Possible espionage	• Russia suspected
2017	WannaCry	Global attack affecting more than 150 countries (including a majority of EU member states)	• Unprecedented global cyberattack. • Use of data encryption to demand ransom payments. • Diversity of affected sectors: UK's NHS; German federal railway; France's carmaker Renault; Italian university computer labs; telecom and energy firms in Spain and Portugal. • Several billion dollars in damage.	• Espionage • Ransomware	• North Korea suspected
2022	Wiper + Distributed Denial of Service (DDOS)	Ukrainian critical infrastructure, banking system, military and governmental websites	• Aim to shut down websites and wipe out data on infected equipment, by flooding systems with massive volumes of requests until collapse. • Regular large-scale cyberattacks destabilize Ukraine before and during Russian invasion. • "Hybrid warfare": cyberattacks + conventional military assaults. • Risk of propagation to neighbouring EU member states.	• Supply disruption • Equipment damage • Possible espionage	• Russia

approach to artificial intelligence. The Commission will adopt a risk-based framework built on the twin pillars of excellence and trust, so as to boost research and industrial capacity, as well as ensure the protection of fundamental rights. The EU has emphasised that a resilient Europe fit for the coming "Digital Decade" is one where people and businesses benefit from improvements in industry and day-to-day life generated by artificial intelligence. The comprehensive dimension is discernible in the EU's Artificial Intelligence Act, a draft regulation proposed in 2021 that aims to establish a common regulatory framework on AI which would apply to all sectors (save the military), as well as to all different types of AI. The proposed act sets out four categories for regulating AI, ranging from prohibited to low risk, with a European-wide AI algorithm registry and a human oversight by design procedure for high-risk AI sectors, such as energy or healthcare.

Thirdly, while the accelerating digitization of the energy industry has brought many economic benefits, it has also considerably enhanced cybersecurity risks within this highly strategic sector, partly due to the rise of smart grids and the mass deployment of smart meters. On the "comprehensive" side, it is notable that **the EU's clean energy legislation has consistently sought to incorporate a cybersecurity component over the last few years**, starting with the Clean Energy for all Europeans package announced in 2016. For instance, this led to a revision of the EU Regulation on the Internal Market for Electricity in 2019, which provided for the development of a "cybersecurity network code" in the power sector, and includes a focus on renewable energies. A "smart grids task force" was created in 2017 to prepare this network code, and the "European Green Deal" also contains provisions to upgrade and reinforce the latter.

Fourthly, when it comes to critical infrastructure in general, EU legislation and policies date back to the 2006 Programme for Critical Infrastructure Protection and the 2008 Critical Infrastructure Directive, which set broad and general guidelines for member states. More recently, the 2016 Directive on the Security of Network and Information Systems (NIS) has become the principal legislative framework in this area. It established common EU norms for the cybersecurity of "operators of essential services" (OES), which include a broad range of infrastructure considered to be essential for the proper functioning of society. As a follow-up, the EU Cybersecurity Act was finalized in 2019, setting out augmented procedures for the enactment of the NIS Directive, whilst also launching an EU-wide certification system for an extensive array of digital products and services, with the aim to create **an internal cybersecurity market**.

FLEXIBILITY IN THE EU'S APPROACH: MULTISPEED NATIONAL PARADIGMS

While the benefits stemming from the "comprehensive" aspect of the EU's policy approach are apparent, the same cannot be said of the "flexible" element. The latter is linked to the fact that Member States have in most cases been provided with a wide margin for manoeuvre and high level of autonomy in the implementation of EU norms and standards. For instance, as per the NIS Directive, each Member State has responsibility to develop its own national cybersecurity strategy. Although an EU cybersecurity strategy was set out in 2013 and upgraded in 2020, it is limited to providing general recommendations, leaving Member States to establish details at the national level. This is also notable in the function of the regional regulatory entity in this area, initially known as ENISA, but now referred to as the EU Agency for Cybersecurity. The 2019 Cybersecurity Act granted the latter a permanent mandate and an increased budget, along with new tools to support countries in enacting the NIS Directive. While ENISA's ambit is comprehensive since it addresses all sectors, its competences remain narrow as it focuses mostly on aggregating and disseminating data, providing advice to member states and encouraging collaboration. As a result, it lacks any binding framework to enforce conformity with EU standards.

This situation is also apparent in the fact that the NIS Directive requires each Member State to set up a "Computer Security Incident Response Team" (CSIRT). All national CSIRTs were assembled into a common European network, along with the creation of a "Cooperation Group", incorporating the

EU Commission and member state cyber agencies. As with ENISA however, these frameworks lack the requisite competences, such as sanctions, needed to enforce conformity with EU-level standards. This responsibility is ascribed instead to member state authorities, which are free to determine the level of authority they wish to attribute to their national CSIRTs. The latter has resulted in the emergence of **stark disparities and a highly differentiated paradigm in terms of the effectiveness for CSIRTs across Europe**. A similar state of affairs is also discernible for more specialized sectors like energy. For instance, the 2019 EU Regulation on Risk Preparedness in the Electricity Sector aims to establish a European approach to confront a wide range of threats, including cybersecurity. However, member states are left free once again to develop their own standards through the preparation of national risk preparedness plans, which are only lightly coordinated by an EU "Electricity Coordination Group". Although the details of the "Artificial Intelligence Act" have yet to be fully fleshed out, it appears as though the proposed legislation will likewise afford a wide margin for manoeuvre to member states in the enactment of EU norms.

For these reasons, flexibility in the EU's policy approach has led to the emergence of a multi-speed paradigm, where the effectiveness of national cybersecurity frameworks is highly variable from one country to another. Wide latitude and autonomy afforded to member states has enabled countries that possess sufficient financial and logistical means, along with the requisite infrastructure and technical expertise, to develop extensive cybersecurity frameworks at the national level. This includes large and influential countries like France and Germany, along with several other member states in northern Europe, which have consistently surpassed EU norms and standards. For instance, France's National Cybersecurity Agency (*Agence nationale de la sécurité des systèmes d'information* – ANSSI, created in 2009) is generally considered to be amongst the most developed not only in the EU, but also globally. It possesses extensive competences to enforce compliance with rigorous national cybersecurity rules. These are based on a Military Programming Law (*loi de programmation militaire*), first enacted in 2013 and then updated in 2018 to cover the period from 2019-25. Amongst other things, the law established strict and binding cybersecurity standards for more than 200 "operators of vital importance". This was supplemented in 2016 by "sectorial decrees" (*arrêtés sectoriels*), whereby France became the first country to establish detailed requirements specifically adapted to the characteristics of different sectors such as gas and hydrocarbons, electricity or nuclear.

A number of other countries, however, have lacked adequate resources, expertise or infrastructure to develop a similarly high level of cybersecurity norms. For instance, countries such as Bulgaria, Greece and Slovakia were late to produce a national cybersecurity strategy and CSIRT, while others like Portugal, Croatia and Latvia have been criticized for still lacking an adequate framework on cybersecurity in critical infrastructure.[3] This situation of a multi-speed Europe bears some resemblance to other policy areas such as Schengen or the euro. Yet, it is especially problematic in the area of cybersecurity, given the high level of interconnection between member states due to the rules of the single market and the legal framework of the EU integration process. Hence, countries with the least developed cybersecurity standards constitute weak links, which can enable cyber viruses to infiltrate the EU network before spreading to other member states and potentially infecting the entire system. This is precisely what happened during a number of cyberattacks over the last few years, described in the above table.

One of the main obstacles to greater harmonization of European cybersecurity norms has been the fact that Member States are hesitant to share classified information with their neighbours, along with a general reluctance to transfer additional competences towards EU institutions. This explains why implementation of the NIS Directive has been problematic, leading to fragmentation in the internal market at different levels. In

3 Barichella (2018).

response to this, the Commission submitted a proposal in December 2021 for an upgraded second NIS Directive which aims to reinforce cybersecurity requirements, tackle the security of supply chains, consolidate reporting obligations, as well as enhance supervisory and enforcement processes, including via more harmonized sanctions across member states. The NIS2 proposal also seeks to broaden the ambit of the initial directive by incorporating more entities and additional sectors, with the objective of an alignment with those sectors covered by EU norms for the protection of physical infrastructure.[4]

While the NIS2 Directive would undoubtedly constitute an improvement, the proposal may be insufficient, particularly with respect to the problem of weak links. Thus, in spite of proposals on more harmonized sanctions, for example, member states would remain in charge of establishing the detailed requirements for their own national cybersecurity frameworks, thus perpetuating the issue of differentiated standards across the EU. One way to enhance the harmonization of cyber norms might be to establish stronger linkages between EU legislation in this area and the EU's Common Security and Defence Policy (CSDP). This could help to encourage greater information-sharing between member states. Likewise, in order to compensate for the problem of weak links, collaboration on cybersecurity between EU countries and the United States could be strengthened, through frameworks such as NATO, which organizes a yearly cyber exercise known as "Locked Shields".

Overall, given the acceleration of the "digital revolution" and the exponential increase in the number and sophistication of cyberattacks affecting practically all sectors, reinforcing EU policies and legislation in this area should be an utmost priority for decision-makers in Europe. The escalation of international tensions over Ukraine further emphasizes the importance of this. Large-scale cyberattacks were launched in the months and weeks preceding the Russian invasion in order to destabilize the country, targeting critical infrastructure, the banking system, along with military and governmental websites; this included reliance on so-called "wiper" and "distributed denial of service" (DDOS) attacks – see above table. Due to digital interconnectivity, the risk of propagation to neighbouring EU member states is real.[5] The Russian military has continued to rely on "hybrid warfare" tactics, combining cyberattacks with conventional military activities in Ukraine, as had been the case during the incursions into Georgia in 2008 and Crimea in 2014. •

4 The Commission introduced in parallel another proposal for a new Directive on the Resilience of Critical Entities, which would focus on reinforcing EU norms for the physical protection of infrastructure (as opposed to cybersecurity, covered under the NIS Directive). The aim is to align sectors covered under these two directives, including: energy, transport, banking, financial market infrastructures, health, drinking water, waste water, digital infrastructure and outer space.

5 In response, the EU has announced the launching of a "cyber rapid-response team" (CRRT) made-up of cyber experts to be deployed across Europe. This includes volunteers from six member states (Lithuania, Netherlands, Poland, Estonia, Romania and Croatia) to help Ukraine defend itself against these cyberattacks.

Managing Editor: Sébastien Maillard • The document may be reproduced in part or in full on the dual condition that its meaning is not distorted and that the source is mentioned • The views expressed are those of the author(s) and do not necessarily reflect those of the publisher • The Jacques Delors Institute cannot be held responsible for the use which any third party may make of the document • Original version • Edited by Anne-Julia Manaranche • © Jacques Delors Institute

Institut Jacques Delors
Penser l'Europe • Thinking Europe • Europa Denken
18 rue de Londres 75009 Paris, France • www.delorsinstitute.eu
T +33 (0)1 44 58 97 97 • info@delorsinstitute.eu

NOTRE EUROPE Jacques Delors Institute
Penser l'Europe • Thinking Europe • Europa denken
PREMIER MINISTRE Liberté Égalité Fraternité
L'Europe pour les citoyens