STUDY

Requested by the INGE committee

European Parliament

Strategic or critical infrastructures, a way to interfere in Europe: state of play and recommendations

Authors:

Paola TESSARI and Karolina MUTI

European Parliament Coordinator:

Policy Department for External Relations

Directorate General for External Policies of the Union

PE 653.637 – July 2021

EN

DIRECTORATE-GENERAL FOR EXTERNAL POLICIES
POLICY DEPARTMENT

STUDY

Strategic or critical infrastructures, a way to interfere in Europe: state of play and recommendations

ABSTRACT

Critical Infrastructures (CIs) provide vital economic and social functions to European Union (EU) citizens. However, they are challenged by a diverse range of threats, not only natural and accidental but also intentional. CIs' increasing reliance on technological advancements adds another element of complexity and vulnerability. Whilst their protection to date has been regulated by Directive 2008/114/EC, its scope of application has proved to be inadequate against an evolving landscape of security threats. Consequently, it is currently under revision. A careful analysis of CIs' status in the EU, covering the challenges to their functioning and measures in place for their safeguard, is therefore necessary to provide recommendations for the adoption of further instruments so as to equip CIs with increased protection and resilience.

EP/EXPO/INGE/FWC/2019-01/LOT4/R/02
July 2021 – PE 653.637

EN

AUTHORS

- Paola TESSARI, Researcher, Istituto Affari Internazionali (IAI), Italy
- Karolina MUTI, Researcher, Istituto Affari Internazionali (IAI), Italy

The authors would like to thank Ottavia Credi (IAI), Francesca Ghiretti (IAI), Martina Dazzi and Martina Camellini for their assistance and inputs to this study.

Coordinator: Trans European Policy Studies Association (TEPSA)

This study was originally requested by the European Parliament's Special Committee on Foreign Interference in all Democratic Processes in the European Union, including Disinformation (INGE).

CONTACTS IN THE EUROPEAN PARLIAMENT

Coordination: Jérôme LEGRAND, Policy Department for External Policies

Editorial assistant: Balázs REISS

Feedback is welcome. Please write to jerome.legrand@europarl.europa.eu

To obtain copies, please send a request to poldep-expo@europarl.europa.eu

VERSION

English-language manuscript completed on 5 May 2021.

Table of contents

List of Figures

List of acronyms

AI	Artificial Intelligence
ATM	Automatic Teller Machine
CAI	Comprehensive Agreement on Investment
CBRN	Chemical, Biological, Radiological, Nuclear
CFSP	Common Foreign and Security Policy
CI	Critical Infrastructure
CIP	Critical Infrastructure Protection
CIWIN	Critical Infrastructure Warning Information Network
CoE	Centre of Excellence
COTS	Commercially available Off-The-Shelf
CSDP	Common Security and Defence Policy
CTED	Counter-terrorism Executive Directorate
CULT	European Parliament Culture and Education Committee
CyCLONe	Cyber Crises Liaison Organisation Network
DDOS	Distributed Denial-of-Service
DG HOME	Directorate General for Migration and Home Affairs
DHS	Department of Homeland Security
DOS	Denial-of-Service
DSP	Digital Service Providers
EEAS	European Union External Action Service
EC	European Commission
ECI	European Critical Infrastructure
ED	Emergency Department
EDT	Emerging Disruptive Technology
EMA	European Medicines Agency
ENISA	European Union Agency for Cybersecurity
EP	European Parliament
EPCIP	European Programme for Critical Infrastructures Protection
ERCC	Emergency Response Coordination Centre
ERNCIP	Reference Network for Critical Infrastructures Protection

EU	European Union
EUR	Euros
EUROPOL	European Union's law enforcement agency
EUGS	European Union's Global Strategy
FDI	Foreign Direct Investment
GIS	Government Information Service
GRU	*Glavnoje Razvedyvatel'noje Upravlenije* [Russian Main Intelligence Directorate]
HVAC	Heating, Ventilation, Air Conditioning systems
Hybrid CoE	European Centre of Excellence for Countering Hybrid Threats
HMI	Human-Machine Interface
IAEA	International Atomic Energy Agency
ICS	Industrial Control Systems
ICT	Information and Communication Technology
ICU	Intensive Care Unit
IIA	Inception Impact Assessment
INTCEN	EU Intelligence and Situation Centre
Interpol	International Criminal Police Organization
IoT	Internet of Things
IPCEI	Important Projects of Common European Interest
IPT	Intelligent Public Transports
IS	Islamic State
ITDB	Incident and Trafficking Database
JRC	Joint Research Centre
MEP	Member of the European Parliament
MS	Member States
NATO	North Atlantic Treaty Organization
NATO StratCom CoE	NATO Strategic Communication Centre of Excellence
NHS	National Health Service
NIS	Network and Information Systems
OECD	Organisation for Economic Co-operation and Development
OEP	Office of Emergency Planning

OES	Operators of Essential Services
OT	Operational Technology
PCB	Printed-Circuit Board
PPP	Public-Private Partnership
RDD	Radiological Dispersal Device
SCADA	Supervisory Control And Data Acquisition
SME	Small and Medium-sized Enterprise
TESAT	Terrorism Situation and Trend Report
UAS	Unmanned Aerial System
UNDRR	United Nations Office for Disaster Risk Reduction
UNOCT	United Nations Office for Counterterrorism
USA	United States of America
USD	US Dollar
WHO	World Health Organization
WITS	World Integrated Trade Solution

Executive Summary

Background

Critical Infrastructures (CIs) are **essential for providing vital economic and social functions to European Union (EU) citizens.** The services they ensure, coupled with their cross-border nature and interdependencies, **make them increasingly vulnerable to diversified types of threats, not only natural and accidental but also intentional.**

The landscape of potential threats on EU soil has been changing and evolving with technological advancements and deep interconnectedness, paving the way for greater vulnerability to cyber-attacks. For instance, with the 'cascading failure' phenomenon there is a possibility that **the failure of one, single part of a given infrastructure could lead to the collapse of other components and eventually to serious damage across an entire network.**

Within the landscape of challenges to CIs, hybrid threats deserve a separate mention. **A hybrid action exploits vulnerabilities of democracies and institutions, benefitting from ambiguity in terms of detection and attribution as well as the intrinsic difficulty in classifying a hybrid event** due to the use of various measures – conventional and unconventional – in different areas – political, economic, cyber, military, civil – by the attacker. They form an effective asset in the hands of both state and non-state actors that seek to exploit the vulnerabilities of Member States (MS). Examples of hybrid strategy are the use of disinformation campaigns, interference in democratic and electoral processes or in MS education systems. Moreover, the growing digitalisation of services, increasingly reliant on the internet, comes with great challenges linked with cybersecurity risks.

Other less evident forms of interference from state and non-state actors have also been targeting the EU. One that has recently caused widespread concerns regards **Foreign Direct Investments (FDIs) in the EU by third countries such as China and Russia**. These investments are directed both towards standard commercial goods and products as well as strategic assets, services or entities, including CIs. Another aspect going beyond FDIs but equally related to CI's resilience is the increasing dependence of the EU from foreign suppliers of technology. The EU experiences a relatively high import dependence on many products and primary assets because decades of de-industrialisation have led to manufacturing and skill gaps in key sectors.

Concern has been growing also in relation to other form of interference towards educational and religious infrastructures. For instance, this is the case of China's Confucius Institutes, non-profit educational institutions funded by the government with the purpose of promoting Chinese language and culture.

Considering such evolving and expanding scenario, **a careful analysis of CIs' status in the EU, covering both challenges to their functioning and measures in place for their safeguard, is necessary to provide recommendations for the adoption of further instruments to equip CIs with increased protection and resilience.**

Main findings

The main EU-level instruments for responding to these forms of interferences are Directive 2008/114/EC – also referred to as European Critical Infrastructure (ECI) Directive – **and the Directive on Network Information System (NIS)**. Both directives have been subject to a review process which has underlined significant inadequacies in guaranteeing protection and resilience. Considering the

evolving and expanding scenario, the directives appear outdated and limited, not covering all forms of interferences – known and emerging – that threaten the EU.

Firstly, **the evaluation of Directive 2008/114/EC presented in the Inception Impact Assessment (IIA) issued by the European Commission in 2020 illustrates specific limitations hindering the protection of critical infrastructures.** Among these shortcomings:

- the Directive has a limited sectoral scope on energy and transport which does not consider other types of CIs that are essential to EU citizens;
- significant discrepancies in its implementation and overlapping obligations have been recorded at MS level;
- it has led to diversified risk assessment methodologies and insufficiently comprehensive coordination and response mechanisms;
- it does not consider the need for improvement in the exploration of synergies between various initiatives at EU level for Critical Infrastructure Protection (CIP);
- its focus is limited to protection and does not address resilience.

On such bases, **a new Proposal for a Directive of the European Parliament and the Council on the resilience of critical entities was published on 16 December 2020. The Proposal addresses these drawbacks to a large extent and includes some dedicated measures to ensure better security and protection of critical infrastructures.** This applies to a larger number of categories, including: banking; financial market infrastructure; health; drinking water; waste-water management; digital infrastructure; public administration; and space. The Proposal also calls for cooperation with other competent authorities, with specific reference to those designated under the Directive on Security of Network and Information Systems (NIS2 Directive). In fact, **The NIS Directive plays an important role in the protection of CIs, which are increasingly reliant on the internet and other types of networks and interconnections. NIS2 recognises how the digitalisation of services has expanded the threats landscape with increasingly sophisticated challenges.**

Significant novelties will be introduced thanks to these two proposals; the expansion of involved sectors, enhanced response capacities and coordination among the different actors at multiple levels are among the most significant. Other measures directly applicable at CI level are 'security by design' approaches and personnel training. Indeed, specific design and architectural elements of a facility can play a significant role in combatting potential threats to its functioning.

Recommendations

In this complex and ever-challenging scenario, **different approaches exist for improving the protection and resilience of CIs.** Measures and initiatives taken by the EU, together with ongoing revisions of major legal instruments, represent fundamental milestones towards enhanced security for critical infrastructures at both national and EU levels.

To be effective, they need to be implemented through a well-structured and coherent approach guided by the EU institutions, **the European Commission (EC) playing a leading role in what concerns legal and security measures, and the European Parliament (EP) in the aspects that relate to resilience of civil society and democratic institutions**, especially when facing hybrid threats and foreign interferences with CIs. In particular, EC agencies and bodies that could play a role in implementing legal and security measures for better protection and resilience of CIs are: the Directorate General for Migration and Home Affairs (DG HOME), the Joint Research Centre (JRC), Critical Infrastructure Warning Information Network (CIWIN) and the European Research Network on Critical Infrastructure Protection (ERNCIP). These actors could give **top-down support to MS in the correct implementation of the EC Proposal for a Directive of the European Parliament and the Council on the resilience of critical entities.**

At the European Parliament level several steps could be taken. Firstly, concrete actions from the Parliament could leverage its visibility, democratic value and authority, as well as its connection with MS through Members of the European Parliament (MEPs) who can co-participate in actively raising awareness with regard to CIs' resilience. **Targeted education, awareness-raising and strategic communication campaigns should be facilitated by the EP Liaison Offices and the EP Culture and Education Committee (CULT), with the involvement of the European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE) and in cooperation with partner organisations such as the NATO Strategic Communication Centre of Excellence (NATO StratCom CoE). A dedicated intergroup to discuss the topic of CIs' protection and resilience could be established**, meeting in joint formats with other intergroups such as: 'AI and Digital', 'Sky and Space', 'Sustainable, Long term Investments' and 'Competitive European Industry'.

Secondly, the EP legislative powers leave room for pro-active action aimed at increasing resilience and protection of CIs in all areas of intervention identified in this study, namely: legal, security and civil society.

Within its budgetary powers' framework, the Parliament should ensure and monitor that adequate EU funding is allocated to the support of MS in implementing the ECI Directive, as well as to education, training and dissemination activities.

In the area of civil society-related measures, by exploiting its tasks such as election observance, setting up inquiries or monitoring democratic processes in Europe, the EP is in the privileged position of being able to look at specific threats targeting democratic and electoral processes, civil society and citizens' behaviour. For what concerns hybrid threats, such as disinformation, relevant awareness-building actions have been undertaken by EU institutions, but their impact on and concrete outreach to civil society in the EU should be more closely monitored and periodically assessed.

Mindful that the functioning of CIs is a priority for both national and EU stakeholders in looking to ensure the successful implementation of these measures, the study concludes that the protection and

resilience of CIs require coordinated and joint efforts at different levels (national, local and EU). Accordingly, recommendations addressing all actors with a cross-cutting approach and aimed at different areas are provided.

1. Introduction

1.1. Objective and scope of the study

Critical Infrastructures (CIs) are defined at European Union (EU) level by Directive 2008/114/EC, which describes them as 'any system which is essential for providing vital economic and social functions: health, food, security, transport, energy, information systems, financial services'. Hence, the EU and Member States' (MS) authorities have been giving close attention to their protection and resilience.

CIs are vulnerable to diversified types of threats, not only natural and accidental but also intentional. The increasing reliance of CIs on technological advancements adds another element of complexity and vulnerability. The cybersphere, in particular, is subject to threats from which disruptive consequences are multiplied by the increasing interdependence and connection of CIs and the blurring of boundaries between the physical and online worlds. A real-world emergency situation such as the COVID-19 pandemic can be exploited by malicious actors operating and targeting the online dimension. One significant example at global level is that the World Health Organization (WHO) has registered a fivefold increase in the number of cyber-attacks since the pandemic broke out compared with the same period last year (WHO, 2020). Furthermore, the cross-border nature and interdependencies not only among multiple CIs, but also linking CIs with other services and facilities, make them particularly appealing targets for intentional disruption by foreign states and non-state actors.

Against this background, **the current framework represented by Directive 2008/114/EC seems inadequate in guaranteeing the protection and resilience of CIs. Its limited scope of application and the general underlying definitions have led to uneven implementation at Members States (MS) level. Hence, a more comprehensive and up-to-date approach is needed, which considers the mixture of known and potential vulnerabilities coupled with appropriate guidance to Member States**.

Accordingly, this study comes into play by presenting a detailed assessment of existing protection for CIs in the EU, as provided by Directive 2008/114/EC, and its implementation at national level. Mindful that different approaches exist to improve the security of CIs, encompassing not only procedures and operations but also the design of CIs themselves, this study will also aim to provide an overview of initiatives such as personnel training, security-by-design and other key developments resulting from EU partners' experiences. Through open sources and desk research, the evolving scenario of threats to CIs is addressed, with its peculiar vulnerabilities being linked to the increasing interdependence and connection of CIs.

The study's final objective lies in contributing to a more comprehensive and flexible approach for the protection and resilience of CIs. To do so, the conclusion provides local, national and EU institutional actors with suggestions on concrete actions to be undertaken with a view to improving existing levels of provisions.

1.2. Methodology: approach, sources, actors

The methodology adopted for this study is multi-level. An initial step focuses on analysing the available definitions and terminology related to CIs from both national and European perspectives. This first step is necessary to assess whether or not the definitions in use at EU level are adequate enough to address the variety of present as well as future multidimensional and cross-border threats.

The study's second step narrows down this approach to the national level. By comparing national definitions of CI in MS, the possible inclusion of other vital and cross-border services – beyond energy and transport as covered by the Directive 2008/114/EC – is considered, with the aim of formulating a potential alternative approach which could thereby widen the coverage. Vital and cross-border services are considered, together with interdependencies between multiple CIs in the EU. The main sources for this section comprise European Commission (EC) official documents, starting with Directive 2008/114/EC, which provides criteria for guiding Member States in the identification of European Critical infrastructures (ECIs).

The third step focuses closely on threat scenarios and is aimed at identifying the main challenges faced by critical infrastructures. Through open sources and desk research, the evolving scenario of threats is illustrated by considering geostrategic/international, European and national factors, as well as intentional (malicious, terroristic) and accidental actions. Specific attention is given to terrorism and hybrid threats, addressing the malicious use and advancement of technologies (e.g. employing drones not only to conduct an attack but also to gather sensitive information). The study analyses the cyber domain, with its peculiar vulnerabilities being linked to the increasing interdependence and connection of CIs.

This study's core section comprises an analysis of the Inception Impact Assessment (IIA) issued by the European Commission in 2020, which evaluates Directive 2008/114/EC and stresses the need for improvement in protecting key infrastructures. Starting from an assessment of this IIA, we consider the most recent proposals applicable to CIs, notably the Proposal for a Directive of the European Parliament and the Council on the resilience of critical entities. Considerable attention is given to analysing how such a proposal would provide those additional requirements identified by the IIA. Other documents issued in December 2020 are evaluated according to the same benchmark: the Communication on a Cybersecurity Strategy of the European Union and the Proposal for a Directive of the European Parliament and the Council on measures for a high common level of cybersecurity across the Union. The objective is to assess if and how these initiatives tackle and help solve the shortcomings identified. These documents are examined with the aim of identifying potential gaps and highlighting aspects that should be addressed more thoroughly.

Whenever considered relevant, lessons learned are drawn from EU partners' experiences, such as the United States (USA) (*Critical Infrastructure: Emerging Trends and Policy Considerations for Congress* and the US Cybersecurity and Infrastructure Security Agency Act of 2018) and Australia (Australian Government's Critical Infrastructure Centre Compliance Strategy) Public deliverables and relevant non classified information from the EU-funded project 'Development of new solutions for the protection of citizens and infrastructures against terrorist threats – EuProtect' are considered and further developed.

The concluding section of the study formulates a list of concrete tasks and actions designed to provide EU institutions and MS with recommendations on how to improve their actions towards increased protection and resilience of the ECIs at local, national and EU levels.

The scope of this analysis covers a number of topics directly related to CIs. The rationale behind our selection reflects priorities quoted in the EU Security Union Strategy, namely: CIs resilience, cybersecurity, public spaces protection, terrorism and radicalisation, hybrid threats and information exchange.

Throughout the study, the term 'Critical Infrastructure' (CI) is used to refer to CIs located in the EU in general. During their research, the authors have considered the term 'strategic infrastructure' to be synonymous with CI. Hence, no distinction is made between 'strategic' and 'critical' as used separately in the title of this study. In their national definitions, MS use mostly the term 'critical'. The term 'European Critical Infrastructure' (ECI) refers to 'critical infrastructure located in Member States the disruption or destruction of which would have a significant impact on at least two Member States', as defined in Article 2 of Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and assessment of the need to improve their protection – hereinafter referred to as *ECI Directive*. **The authors of this study consider positively the European Commission's attempt to introduce a more comprehensive terminology in the Proposal for a Directive of the European Parliament and the Council on the resilience of critical entities, from now on referred to as the *EC Proposal*. The term 'critical entity' mentioned in Article 2 of the EC Proposal is considered adequate and broad enough to encompass the proposed new types of CIs listed in the EC Proposal's Annex. However, as will be analysed more deeply in Section 6.1, the authors wish to stress that the list in this Annex should not be regarded as definitive.**

2. Definitions and possible expansion of the criteria

2.1 Definitions and terminology: analysis of the criteria that define an ECI

The current **legal framework for Critical Infrastructures' protection in the EU is provided by Directive 2008/114/EC of 8 December 2008,** which deals with the identification and designation of European Critical Infrastructures as well as assessing the need to improve their protection. The ECI Directive is the main instrument guiding Member States in identifying and designating Critical Infrastructures on their territory, especially those falling within the category of ECIs. **This designation serves the Directive's ultimate purpose, which is to provide a shared approach for assessing the need to improve protection of ECIs and establish some common measures contributing to their security**. The general approach adopted by this Directive ensures a common procedure for all Member States, preserving at the same time their autonomy in accordance with the principles of subsidiarity, proportionality and complementarity (European Commission, 2019). As illustrated under Article 2 of the Directive, a critical infrastructure means 'an asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions'. Article 2 also defines an ECI as: 'a critical infrastructure located in Member States the disruption or destruction of which would have a significant impact on at least two Member States. The significance of the impact shall be assessed in terms of cross-cutting criteria. This includes effects resulting from cross-sector dependencies on other types of infrastructure'. **To identify and designate an ECI, the Directive illustrates two categories of criteria that should guide Member States in this process: sectoral and cross-cutting. By 'sectoral criteria', the Directive means specific criteria which are peculiar to each infrastructure.** They can, for instance, be technical or functional elements, which help identify an infrastructure as critical. **'Cross-cutting criteria', by contrast, can be measured on**

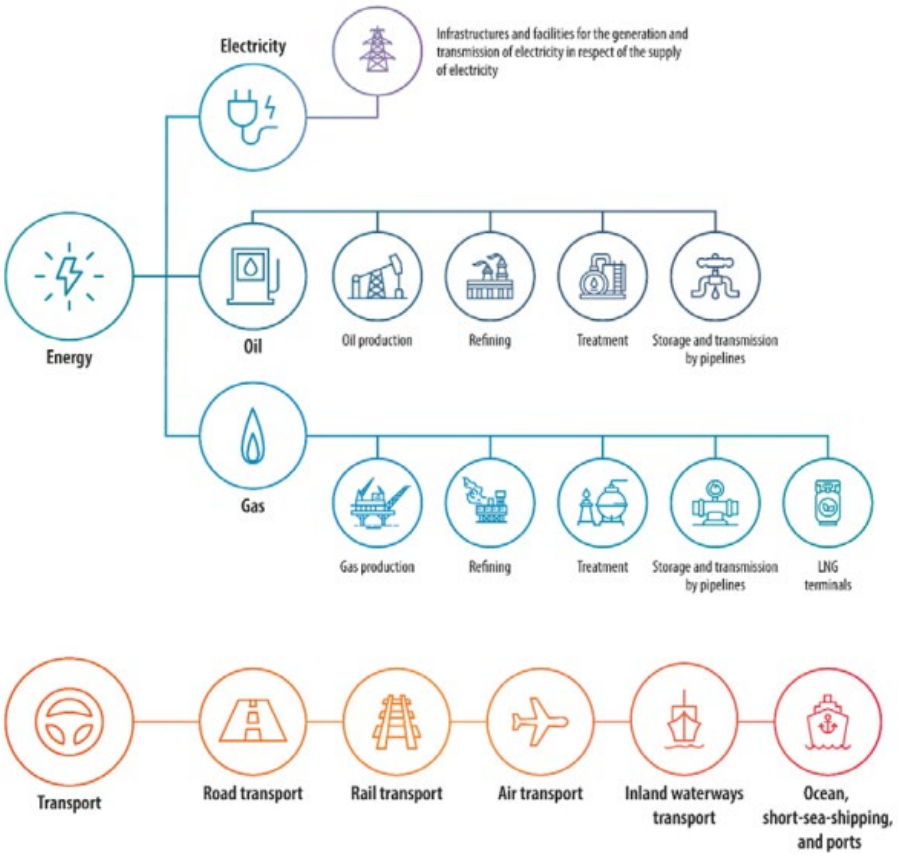
the basis of specific thresholds that are set in accordance with impact severity regarding the disruption or destruction of a particular infrastructure. Concerning cross-cutting criteria, Article 3 of the ECI Directive identifies the following:

- casualties criterion (assessed in terms of the potential number of fatalities or injuries);
- economic effects criterion (assessed in terms of the significance of economic loss and/or degradation of products or services; including potential environmental effects);
- public effects criterion (assessed in terms of the impact on public confidence, physical suffering and disruption of daily life, including the loss of essential services).

For the application of cross-cutting criteria, non-binding guidelines were published by the Joint Research Centre (JRC) in 2008. However, Member States also have the option of setting their own thresholds for each criterion, with or without referring to the EC guidelines (Thornton et al., 2008).

Having established key definitions and criteria, this Directive explicitly identifies the energy and transport sectors, along with their subsectors, as targets of its implementation. Originally, the scope of the Directive as proposed by the EC was significantly wider, also due to the impact of the 9/11 terrorist attack in the United States and the ones that followed for instance in Madrid and London. The less ambitious approach – covering only the energy and transport sectors – was adopted primarily due to MS reluctance to embrace a broad EU approach in an area of traditional national competence, but also based on certain legal considerations (European Commission, 2020c). As a result, during the negotiations leading up to adoption, a 'minimum common denominator' approach was agreed upon by MS (European Commission, 2020c). Such a focus follows the Directive's development of a 'first step in a step-by-step approach to identify and designate ECIs and assess the need to improve their protection', but anticipates the possibility of including other sectors within its scope, such as the information and communication technology (ICT) sector. As underlined by a previous study (OECD, 2019), **definitions and procedures provided by the Directive constitute a common approach which aims to leave flexibility in its application to the MS. However, some criticalities have emerged, for instance regarding the limited scope of application and the general character of definitions.** These elements have led to diversified interpretations by the MS, **resulting in a fragmented and heterogeneous implementation of the Directive at national level**. In this context, it is important to examine and compare national definitions of CIs in MS, exploring the possible inclusion of other vital and cross-border services – beyond energy and transport – with the aim of formulating a potential alternative approach.

Figure 1: Critical Infrastructures covered by ECI Directive (Anglemayer, 2021)



2.2 A tentative comparative analysis of CI definitions in MS and possible expansion of the categorisation: identifying other vital, interdependent and cross-border services

According to the ECI Directive, **CI is described as 'an asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions.'**

When adopting the ECI Directive, MS had to take into consideration that the EC definition was an attempt to standardise national understandings of CIs so as to align with an EU-level basis. **Several MS, such as Ireland, Estonia or Greece, immediately adopted the ECI Directive's definition. In the majority of cases, MS maintained their national CIs definitions alongside that of the EU**[1] (OECD, 2019). Selected national current and past definitions are considered in the following paragraphs to take stock of elements, concepts or terminology which are not included in the EU definition[2].

[1] MS that maintained a national definition of CI include inter alia: Austria, Belgium, Czech Republic, France, Finland, Germany, Latvia, the Netherlands, Poland, Portugal, Slovakia, Spain and Sweden.
[2] No publicly available list of CIs has been found. This can be due to the fact, that such information, especially for those CIs that are considered ECIs, is confidential.

In Belgium, which partially takes up the EU definition, a CI is defined as 'an installation, system or part thereof of federal interest', that, 'if disrupted or destroyed, would have a significant impact' (Service Public Fédéral Intérieur, 2011).

Finland's Cyber Security Strategy (Government of Finland, 2013) issued in 2013 defined CIs as 'structures and functions' that 'comprise physical facilities and structures as well as electronic functions and services'. The most recent Finnish Security Strategy for Society 2017 (Liekkilä, 2018) identifies 'Infrastructure and security of supply' as one of the 7 vital societal functions[3]. This Strategy states that vital societal functions are the result of:

- operational critical infrastructure;
- reliable critical services;
- and reliable critical production.

The approach used in Finland focuses on protecting 'what the critical infrastructure produces, not the units of it', which is at least partially in line with the EU's recent shift of focus from the protection of CIs as such to a broader concept of resilience intended as a way of protecting CIs' output, namely the services that it generates.

The French *Instruction Générale Interministérielle relative à la Securité des Activités D'Importance Vitale,* issued in 2014, defined 'vital' infrastructures as 'any establishment, facility or structure located on the national territory for which the damage, unavailability or destruction as a result of a malicious act, a sabotage or terrorism action would risk, directly or indirectly, to severely burden the war or the economic potential, the national security or the survivability of the nation, or to seriously affect the population's health or life' (Government of France, 2014). Whereas this definition is more precise than previous versions, clearly referring to a 'malicious action, sabotage and terrorism' and describing in more detail the results of such action, a recent factsheet issued by the French Secretariat-General for National Defence and Security regarding Critical Infrastructure Protection (CIP) in France gives a more concise definition: CIs are 'institutions, structures or facilities that provide the essential goods and services forming the backbone of French society and its way of life' (Government of France, 2017). The document identifies 12 sectors divided into 4 areas. The technological area comprises: communication, technologies and broadcasting, industry and space, as well as research. The latter is a key area which, despite its relevance for the EU, is not included in the EC Proposal.

The Spanish definition specifies that CIs are 'strategic' infrastructures whose functioning does not envisage 'alternative solutions'. The term 'strategic infrastructure' is further defined as 'installations, networks, systems, physical and technology information equipment that determine the functioning of essential services' (LISA Institute, 2019).

Finally, the United Kingdom's definition is reported here for information purposes only, in light of Brexit. CIs are described as 'those critical elements of infrastructure the loss or compromise of which would result in major detrimental impact on the availability, delivery or integrity of essential services, leading to severe economic or social consequences or to loss of life.' The elements are specified and include 'facilities, systems, sites, property, information, people, networks and processes' (Government of the United Kingdom, 2017).

The aforementioned definitions give an idea of how CIP has been considered at national level by MS**. The EC Proposal certainly represents a significant step towards a better definition of those sectors which are critical for the EU. That being said, there are several factors that indicate how the EU approach**

[3] Other vital societal functions stated in the document include: leadership, international and EU affairs, national defence, domestic security, economy, services for citizens and psychological resilience.

towards CIs should as much as possible remain open, flexible and modular. The current competitive international scenario in which the lines between peace and war are increasingly blurred, with war not always being openly declared (Marrone and Muti, 2020), could well result in an augmented reliance on tools such as interference and disruption of CIs, both by state and non-state malicious actors. In this sense, **the EU has to take into consideration that more types of essential services and critical entities will become targets of attacks in the future, beyond the categories already defined in the EC Proposal**. Targeting key services not classifiable as any type of entity among those identified in the Annex of the EC Proposal is exactly what a malicious actor who uses hybrid actions could try to do in the future. In this case, because of hybrid threats exploiting 'grey zones' in legislation and regulations, together with increasing attention being given to the EU and MS regarding the types of services considered in the Annex, malicious actions could shift towards those categories of services that are not falling within the EC Proposal's scope and will hence not benefit from the same level of attention by the EU and MS. This does not mean that the types of services currently considered by the EC Proposal will not suffer from intentional or unintentional threats. It is rather a matter of **using a highly adaptable approach that should allow for fast updates and modifications, envisaging the definition of more sub-types/sub-categories of services, adding new types, or cancelling others.** The EC Proposal should form the foundation for a comprehensive but flexible and 'light' critical services conceptual framework aimed at faster prevention, protection and response by MS.

Among additional sectors of intervention which are **not currently foreseen by the EC Proposal** but nevertheless worthy of attention and careful consideration **are: the chemical industry; emerging and disruptive technologies; education; as well as communication systems, including mass, social media and information services**. Other areas particularly important to be monitored include civil society together with democratic processes and institutions.

The chemical industry is particularly exposed to security and safety risks, both physical and cyber, malicious and accidental. Chemical precursors can be stolen and/or smuggled by terrorists or criminals who target supply routes or former laboratories, but also acquired from the black market or even from legitimate suppliers. Numerous examples point to the risks of chemists involved in intentional actions of this kind, from Chechnya to Russia, Iraq, or Afghanistan. In Europe, non-intentional activities such as industrial accidents leading to major human and environmental catastrophes continue to be relatively frequent, from the Seveso (Italy) industrial disaster in 1976, to the 2012 and 2014 explosions (with ammonium nitrate) in Toulouse (France) and Gorni Lom (Bulgaria). Each year, approximately 30 major industrial accidents happen in the EU (European Commission, 2017a). Outside EU territory, huge disasters include the explosion in the port of Beirut during August 2020, which were felt as far away as in Cyprus (Ramzy, 2020). The Seveso Directives (82/501/EEC, Seveso II Directive 96/82/EC, Seveso III Directive 2012/18/EU) regulate the EU's chemistry industry sector and are integrated with other EU policies, including CIP. Albeit the current regulations being considered adequate, a process of continual adjustment forms the basis of a successful approach. This is mainly due to the intense and rapid industrialisation over recent decades in the relatively 'newer' EU MS and in EU neighbouring countries, such as the Western Balkans or Eastern Europe, although industrial accidents are also happening in 'older' MS, such as France. Particular consideration should be given to cross-border risks linked to chemical plants established in intersection areas between EU and non-EU territory, not least because of differences in regulation and crisis management mechanisms.

Dependency on Emerging and Disruptive Technologies (EDTs), specific technologies, or raw materials from outside of the EU territory can determine serious liabilities in supply chains of products or services particularly important for daily life. Similarly, targeted investments by foreign stakeholders in these

technologies or materials in the EU and its neighbourhood warrant attention through their potential for interference in Europe by making it more vulnerable and dependent. As such, they should be considered for more systemic protection and resilience building.

A different type of interference targets weak points in societal structures typical of Western societies, including EU MS. Albeit not being considered CIs or critical services as such, they form important elements underpinning the correct functioning of European civil society by contributing to its stability, and have thus become targets of foreign stakeholders' hybrid strategies. These societal structures include information ecosystems (mass, social media and information services) and democratic (political and electoral) processes and institutions. For instance, a hybrid strategy targeting a MS through disinformation campaigns could provoke uncontrolled, irrational reactions from civil society leading to unpredictable consequences and potentially affecting supply chains or the functioning of those CIs which are also public spaces/soft targets. Interference with the education systems in MS (analysed further in section 4.2) should also be monitored as new developments could emerge in the future. These sectors do not provide an exhaustive list, but rather serve as selected examples of areas that would benefit from increased attention and monitoring.

Looking more closely at democratic processes, they appear to be threatened by a variety of malicious actions. Among these, EU democratic systems seem particularly vulnerable with regard to: integrity of elections and political advertising; spread of misinformation; interference with media freedom; as well as media pluralism (Robert Schuman Foundation, 2020).

For instance, interference with electoral processes can take place via cyber-attacks to meddle and falsify elections results. The use of electronic voting or the online transmission of results, while facilitating the electoral procedures, creates new vulnerabilities to cyber-attacks (Robert Schuman Foundation, 2020). Electoral processes have been increasingly reliant on the internet also with regard to online campaigning, which has enabled candidates to expand their target audience by increasing and diversifying their communications channels. At the same time, this has made democratic processes more vulnerable, exposing them to the dangers of disinformation. Such actions aim at distorting or spreading false information about candidates, political parties, or even national institutions and the actions of governments more broadly. This has been the case for instance with the disinformation campaign carried out by Russian sources in the context of the 2019 EP election (European Commission, 2020i).

Another element linked to the guarantee of free elections is transparency in parties' financing. External interference through financing – i.e. funding linked to foreign interests – is facilitated by the lack of transparency rules regarding donations in some MS or by very limited monitoring thereof (Robert Schuman Foundation, 2020).

These aspects have been recently tackled in detail by the European Democracy Action Plan, issued in December 2020, whose aim is to 'promote free and fair elections, strengthen media freedom and counter disinformation' (European Commission, 2020i). The plan is structured to enhance meaningful participation and empowerment of citizens, whose freedom of choice in a free and public space, without any manipulation, is a core principle at the basis of EU democracy (European Commission, 2020i). The plan is now in the very early steps of implementation and will run until 2023, when it is due to be evaluated to assess progress.

2.3 A look at soft targets: a special category of CIs

At national level, the ECI Directive's definition of critical infrastructures has been interpreted in different ways. Some refer to CI as infrastructures whose functioning is vital or essential to economic and social well-being, while others stress their importance for the State's functioning or national security

(OECD, 2008). Once element shared among the main definitions is a key focus on the consequences of an infrastructure failure, commonly deemed to have severe impacts on socio-economic well-being and public safety, including national security (OECD, 2008).

Given the inclusion of other entities in the category of critical infrastructures, '**soft targets' certainly warrant careful consideration. These can be defined as public spaces with intrinsic vulnerabilities resulting from their open nature, public character and easy access,** for instance due to the lack of security checks at points of entry (European Commission, 2017b). In addition, as they are often characterised by a high concentration of people, **they have become appealing to terrorists who aim at maximising the number of casualties in their actions**. The Brussels attacks in 2016, Barcelona in 2017 and Strasbourg in 2020 – which hit Christmas markets and pedestrian areas – confirm such trends in terrorist attacks, where the main targets are no longer institutional or religious sites, but more frequently open public spaces. Railway and subway transportation is also an example of a soft target.

Against this background, **the EU has undertaken several ad hoc initiatives specifically targeted at the protection of such spaces. Among these, it is worth mentioning the EU Action Plan to support the protection of public spaces** adopted in October 2017, not only to encourage exchanges of good practices and lessons learnt among MS but also to give support through funding and guidelines (European Commission, 2017b). The EU Action Plan provides examples of spaces which are to be considered soft targets without making an explicit distinction between them and CIs, such as, for instance, transport hubs (which also qualify as CI according to the ECI Directive definition). The Action Plan also explicitly expresses the EU's will to build upon actions and lessons learned from other initiatives related to public spaces, including the critical infrastructure protection measures (European Commission, 2017b). In December 2017**, the Action Plan was advanced with the establishment of a public-private Operators Forum, gathering representatives from Members States and operators of public spaces venues.** The public-private Operators forum established a cooperative approach that has continued through subgroups meetings to foster the Action Plan's objectives.

Due to its specific characteristics, which differ from those of other types of CIs, **protection measures for soft targets need to be adapted accordingly**. Their open nature, easy access and public character are features that make soft targets particularly vulnerable but are at the same time part of the solution in guaranteeing their security and safety. The open and public character of spaces facilitates monitoring and reporting by citizens. If civil society receives adequate education and guidelines on risks, their prevention and what actions can be undertaken, it could become a valuable resource, rather than a mere target, by identifying and reporting suspicious actions happening in a public space.

Capitalising on these factors requires the active involvement of citizens, who are main users of soft targets, in line with the concept of 'strategic citizen'[4] (Falk, 2020). Recent trends in terrorism[5] and the emergence of hybrid threats (experienced significantly during the COVID-19 pandemic) show how various aspects of civil society and its functioning are being exploited by malicious state and non-state actors. In light of the advantages which targeting civil society gives to the attacker, future threats are increasingly likely to exploit all those aspects that disrupt its operating correctly, from supply chains to interference with critical/essential services, up to intentionally provoking casualties or physical and psychological injuries to people. **Empowering the population and promoting a security and safety culture among citizens are key elements that should be considered more in crisis management at local, national and EU levels.**

[4] In a context of growing hybrid threats specifically targeting weak points in societies, the civil society is seen as a 'battlespace'. Therefore, the citizen as part of a civil society conceived as 'battlespace' is considered 'strategic'.
[5] See section 3.1.

Another element relevant for those CIs that are soft targets is to **apply a 'security by design' approach, ensuring that the space is designed and organised in such a way as to take into account potential malicious, terroristic, or non-intentional activities and their consequences on human behaviour by envisaging architectural shelters and planning adequate evacuation routes**. Soft targets that are characterised by intense flows of people (for instance a metro station during rush hour) have to consider crowd behaviour analysis. In a number of cases no weapon is needed to provoke casualties and injuries that occur simply because of how the crowd reacts. These are only some exemplifier reasons why soft targets are a category of CIs deserving particular attention on which the next section expands upon.

2.3.1 Religious infrastructures as soft targets: terrorism and foreign interference

Due to their highly symbolic value, religious infrastructures represent another potential terrorist target (Vasileios et al., 2018). Places of worship like churches, mosques and synagogues qualify as a type of soft targets (Kalvach et al., 2016), as they are characterised by spacious layouts, generally not equipped with sophisticated protective measures, and are meant to host large numbers of people. Between 1998 and 2019, almost 600 terrorist attacks against religious infrastructures of the most widespread faiths have taken place (Pethő-Kiss, 2020). In recent years, a rather worrying phenomenon has been spreading throughout Europe, with far-right terrorism targeting places of worship of cultures they identify as 'foreign'. This is a particularly alarming element given the speed at which political terrorism is spreading in the Western world (Institute for Economics & Peace, 2020).

Places of worship in Europe contribute to inter-faith dialogue and religious openness, but they can also represent a risk to security if targeted by foreign stakeholders as a means to exert influence within MS territories (Fiala, 2018). Religious infrastructures are seen by some foreign actors as potential assets to consolidate support networks of terrorist groups through funding. An example of this type of interference is the provision of funding to violent extremist groups aimed at sustaining attacks or potential recruits' travel expenses to areas controlled by the Islamic State (PACE, 2018). In particular, there are reasons to presume that investments are being funnelled towards conservative Islamic groups, such as the Muslim Brotherhood or Salafist associations (European Parliament, 2016). However, since individual states retain responsibility for national policies related to foreign financing of religious institutions and cultural centres, the EU encourages to strengthen relations with third countries facing problems of radicalisation in order to prevent this phenomenon (European Commission, 2016b).

Third-country governments could also exploit funding to places of worship in order to increase their political leverage. Therefore, the influence exerted by foreign countries through the funding of religious infrastructures can become a threat to the stability of religious communities and may have consequences at national level. A case that exemplifies both instances is Saudi Arabia's funding of religious infrastructures in the Western Balkans. In a 2017 report, the EU Institute for Security Studies (Lange et al., 2017) underlined how Saudi-funded mosques and schools facilitated the spread of the *Wahhabism* ultra-conservative doctrine in the Western Balkans. Through its political, economic and cultural ties within the region, based on the presence of a strong Muslim identity, Saudi Arabia tried to export its state-sanctioned version of conservative Islam in the Western Balkans. Through funds from the Saudi government, Islamic humanitarian centres and non-governmental organisations (NGOs), the moderate character of local Islam has been changed in its nature (Lilyanova, 2017b). The spread of this conservativism has led to the creation of a parallel education system and parallel religious institutions, called *'para-jamaats'*, which are not supported by the Islamic community. Moreover, according to Europol, during the same period a high number of foreign fighters joined *Daesh* from the Western Balkans (Europol, 2017). Overall, the influence of Saudi

Arabia in the region through funding has increased radicalisation in the Muslim community, albeit not being identifiable as single-cause explanation for its occurrence (Lilyanova, 2017b).

In conclusion, recalling a recent motion for a European Parliament resolution (European Parliament, 2020b), the EU must be cautious of the risks linked to foreign funding to religious infrastructures, which can be exploited to promote radical fundamentalism and extremism in Europe, and must take action to combat all kinds of illicit financing.

3. The status of CIs facing present and future threats

3.1 Threats evolution and state of the art

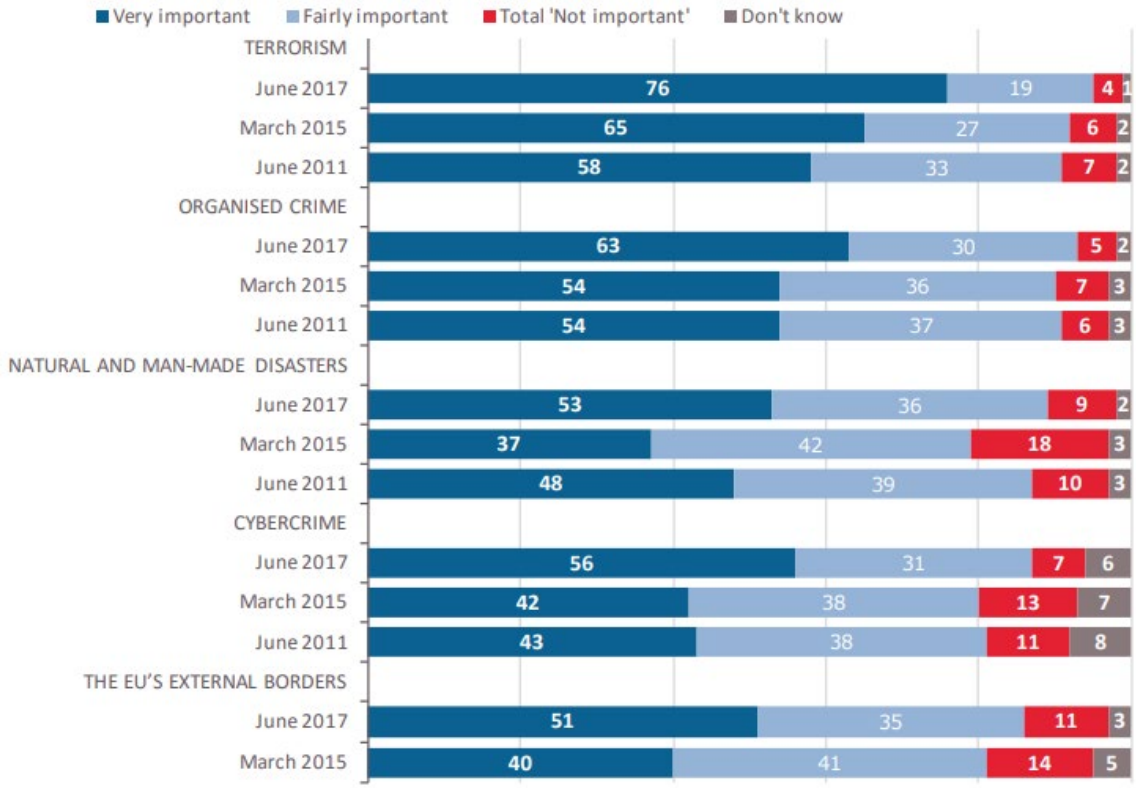
Threats against CIs have experienced a gradual evolution over time. With advances in technology and interconnectivity, **CIs are increasingly becoming complex hybrid entities (cyber and physical), extremely reliant on their connected components as well as each other** (Choraś et al., 2016). This potentially applies to all types of CIs, ranging from telecommunications to energy and transport sectors. A possible disruption in one infrastructure has the potential to cause a ripple effect, thereby impacting the entire network (EU-CIRCLE, 2016). In other words, a CI malfunctioning could compromise the normal functioning of society (European Union, 2008). **As demonstrated by the content of the ECI Directive, an all-hazard approach should be adopted when considering these risks,** not limiting the scope of consideration to anthropogenic threats – i.e. terrorist attacks, state-sponsored actions or industrial incidents – but rather widening the scope also to natural disasters – for instance earthquakes, flooding, hurricanes (Anglmayer, 2021).

A Eurobarometer survey conducted in 2017 revealed the **European public's deep concerns about terrorism, cybercrime, as well as natural and man-made disasters, with 95 % of respondents claiming that their main source of worry could be associated with terrorist activities** (European Commission, 2017d). Approximately **one year later, a public consultation conducted by the Commission showed how Europeans identified cyber-attacks and incidents affecting energy supplies as the two primary threats to CIs**, followed by natural calamities, state-sponsored attacks and terrorist activities (Anglmayer, 2021).

All these threats might have negative consequences affecting the EU's security and the well-being of its citizens (EU Science Hub, 2019). For example, **cyber-attacks to energy providers could cause: loss of power; power overloads; destruction of equipment; as well as damages to devices throughout the grid. Cascading effects could then bring down the power grid in more than one country. Natural disasters such as flooding or violent storms can also seriously impact national energy and transport sectors, leading to interruption of services through serious damages to the infrastructures**.

Moreover, the increased reliance on digital systems (see Section 3.3) introduces a new degree of flexibility, which could be exploited by malicious actors for criminal or even terrorist activities. For instance, the fact that most infrastructures resort to similar Commercially-available Off-The-Shelf (COTS) systems – such as Windows – makes it considerably easier for potential cyber attackers to target them; as attackers are already familiar with the functioning of the server. Increased digitalisation characterises CIs with a higher degree of connectivity, which, consequently, removes a series of obstacles for those attempting to hack a system.

Figure 2: Importance of specific challenges to the EU (European Commission, 2017d)



As stated by the EU Science Hub, '[s]ome threats cannot be foreseen'. Nevertheless, being able to identify current threats and outline potential trends is crucial when it comes to the security of CIs.

At some point in the near future, European countries are bound to experience a series of environmental changes which will inevitably affect their CIs (Forzieria et al., 2017). Climate-related incidents have the potential to affect the lifespan and effectiveness of CIs or even cause their destruction (EU-CIRCLE, 2016). The CIs that are most sensitive to natural hazards are those involved in the energy, transportation, marine and water management sectors (EU-CIRCLE, 2016).

Technological progress and large interconnection characterising today's CIs pave the way for new vulnerabilities. **CIs are heavily exposed to cyber-attacks (ENISA, 2020). In particular, they are threatened by the 'cascading failure' phenomenon** – as described earlier – consisting **of the possibility that failure in one, single part of a given infrastructure could lead to the collapse of other components, eventually leading to serious damage across an entire network** (Candelieri et al., 2019).

Threats in the **cybersphere are changing, gradually shifting from criminal actions mainly conducted by 'recreational' hackers or actors moved by financial motives, towards intelligence and destructive activities suspected of being conducted by state entities or criminal organisations**. Moreover, advances on the Internet of Things (IoT) have increased the risk of information security incidents implying severe consequences over CIs throughout Europe, ranging from industrial plants to environmental institutions, to transport infrastructures (NEC Corporation, 2016b; Torch Marketing and KNM Media, 2016). In the near future, it is likely not only that CIs will experience an increase in cyber threats (Europol, 2014), but that attempts of this kind will also have a higher degree of success (Choraś et al., 2016). This danger could heavily compromise the functioning of CIs, directly affecting the society relying on these systems and, indirectly, even cause disruption in neighbouring countries (ENISA, 2011).

A Distributed Denial-of-service (DDoS), for instance, has the potential to debilitate the targeted infrastructure, slowing down the system or causing severe delays in its regular functioning. Moreover, a malware attack could potentially shut down an entire service, causing serious disruption within society. Some types of malwares are able to affect technologies at the basis of the functioning of any advanced society's CIs, like supervisory control and data acquisition (SCADA) structures and human-machine interface (HMI) systems. The 2015 cyber-attack against Ukraine represents a fitting example where a malware infected the country's electrical infrastructure by targeting its SCADA system, causing saw power outages in Kiev and other western regions of the state. This instance also has demonstrated how incidents taking place in EU neighbouring countries could possibly have an impact on EU MS due to cross-borders interdependencies (European Parliament, 2021).

On a more general note, given the frequent dual-use character of Artificial Intelligence (AI) solutions, seemingly innocuous technologies such as face-recognition applications could be employed for malicious activities (Viganò, Loi and Yaghmaei, 2020).

Terrorism also continues to be perceived as a serious threat to CIs (Torch Marketing and KNM Media, 2016**). The 2017 comprehensive assessment of EU security policy (**European Commission, 2017b) **reported an 'unprecedented level of terrorist threat', matched with new, emerging threats,** such as Unmanned Aerial Systems (UASs, commonly known as drones).

Terrorists may resort to different types of weapons and materials to conduct their violent acts. Over the past 20 years, more than 2 000 terrorist incidents saw the employment of conventional weapons, namely explosive devices, firearms, or melee weapons[6]. **In recent years, Europe has been witnessing an increasing number of cases of vehicles ramming against soft targets**, endangering both people and physical structures. Similar incidents have occurred, for instance, in Nice and Berlin during 2016 as well as in Barcelona during 2017.

While explosive incidents seem to be reducing in number, **attacks conducted with firearms continue to represent a serious source of concern for CIs,** with these types of weapons having been and continuing to be used both in outdoor spaces and inside public facilities. The Paris shooting in November 2015 provides a well-known example. Due to stricter laws regulating the purchase and employment of firearms in Europe, when compared with the US, it is likely that European numbers will not match those in America. That being said, given their diffuse availability on the black market and their relative ease of use, the likelihood of firearms being employed within CIs should not be overlooked[7].

The main threat in terms of terrorist acts and the most likely trend to characterise future risks towards CIs is represented by melee weapons[8]. A relevant example is presented by the infamous London Bridge stabbing attack in 2017. These devices can be purchased or even manufactured without major impediments. Because of their frequent dual-use nature[9], melee weapons often go unnoticed and might be difficult to detect. These weapons have been used extensively over recent years in CI incidents, such as metro and railway station attacks, and given their highly attainable nature they are likely to remain the favourite means of assault by terrorists.

[6] Data were retrieved from Europol Terrorism Situation & Trend (TE-SAT) reports.
[7] According to a recent report by the RAND Corporation, Europe represents the largest market for arms trade on the dark web. For more information, see: G. Persi Paoli, et al., Behind the curtain – The illicit trade of firearms, explosives and ammunition on the dark web, RAND Corporation, 2017.
[8] Estimates based on data retrieved from the Global Terrorism Database.
[9] Common items such as kitchen knives and baseball sticks, for instance, have been repeatedly used by terrorists conducting indiscriminate acts of violence.

Terrorist threats to ECI also derive from non-state actors aiming to employ unconventional weapons to conduct their attacks – namely Chemical, Biological, Radiological, Nuclear (CBRN) devices and materials (see Section 3.2). Cases of attempted attacks with these agents continue to be reported in Europe[10]. Although attacks of this type are considerably fewer than those conducted with conventional weapons, technological advancements and widespread availability of information – especially online – might favour increased interest in CBRN weapons and materials on behalf of non-state actors.

One last category of devices should be taken into consideration when assessing terrorist threats towards CIs, namely drones. Their potential employment to conduct violent actions ranges from drones packed with explosive material crashing against a facility to drones flying over a secure structure and collecting sensitive data (Pompers and Tarini, 2017). For instance, the IS perpetrated its first attack with the use of a drone loaded with explosive in Syria against military units of Operation Euphrates Shield in 2016, causing three injuries. Since then, drone attacks by non-state actors have become more common (Balkan, 2016).

Though not technically a type of weapon, it is worth mentioning the danger represented by possible insider threats working within CIs. Individuals working inside an energy facility, an airport or even a hospital might gain sensitive knowledge which could be exploited against the very infrastructure in which they operate.

3.2 Conventional and CBRN threats: physical damage to CIs

Since the ECI Directive was adopted in 2008, **the landscape of potential threats on EU soil has changed significantly. Critical entities have always been vulnerable to so-called 'conventional threats' – in other words, natural or man-made accidental disasters** – caused by human errors as well as natural or technological reasons. Extreme weather events such as flooding, hurricanes and rising sea levels are bound to produce severe consequences for CIs (EEA, 2019). For instance, electrical infrastructure located in countries particularly vulnerable to some natural disasters such as Belgium, Croatia, Portugal and Slovenia are exposed to critical weather conditions, such as violent storms (Hallegatte, Rentschler and Rozenberg, 2019). The United Kingdom and the Netherlands also worry that climate change-related events will have a serious impact on their energy and transport sectors (UNDRR, 2020).

With regard to water supplies throughout Europe, the United Nations Office for Disaster Risk Reduction (UNDRR) predicts an increased water availability in Northern Europe and drier conditions in Southern Europe, with negative consequences on water supplies for the energy industry and a heightened risk of flooding across the region (UNDRR, 2020).

Considering this wide range of risks and threats facing CIs, **current measures in place as established by the ECI Directive are based on an 'all-hazards' approach which takes into account man-made, technological threats and natural disasters in the CI protection process. At the same time, the Directive itself gives priority to the threat of terrorism** (European Council, 2008).

This concern is motivated by the increasing number of terrorist attacks against CIs registered over recent years, especially in the domain of public transportation. The Western world has experienced a shift in attitude towards terrorist threats following the attacks of 11 September 2001, launched in the USA against the World Trade Centre and the Pentagon. Whilst prior to 9/11 terrorists mainly targeted institutional, high-value sites, following these incidents soft targets have become the primary objectives. Elements such as

[10] In 2018, Europol recorded three attempts to conduct large-scale CBRN terrorist attacks: in 2018 in Italy a person was arrested for plotting to use a chemical-biological mixture to contaminate drinking water; in Germany, a person allegedly linked to the IS was arrested upon planning to use a biological agent combined with explosive for an attack. In 2019, no cases were reported. See: TE-SAT reports 2019 and 2020.

soft targets' open nature and high degree of accessibility make them particularly vulnerable and within the reach of potential terrorist acts.

As noted in section 2.3, when it comes to soft targets a possible weak point consists in the open areas that often surround the sites – for instance, railway stations' entrance points are generally characterised by large spaces leading to the main hall. These can easily be targeted by malicious actors aiming to cause unrest. The EU itself has experienced a series of deadly attacks in the transport sectors: in Madrid in 2004, London in 2005 and Brussels in 2016.

While all past attacks against CIs have been perpetrated with the use of traditional weapons, **major concern has been expressed at EU level regarding the availability of CBRN material as well as the risk represented by their intentional use in terrorist actions. The dual-use character of CBRN agents, linked to their extensive use for civilian purposes, is particularly worrisome**. This is the case, for instance, with industrial products such as pesticides or agents used for the production of vaccines. Intentional CBRN incidents comprise:

- criminal acts such as the deliberate dumping or release of hazardous materials to avoid regulatory requirements;
- the malicious, but non-politically motivated poisoning of one or more individuals;
- terrorist acts that involve serious violence to persons or property for a political, religious or ideological purpose and/or that are a matter of national interest.

A CBRN attack would have severe consequences primarily for people and hinder the ability of an infrastructure to continue its normal operations. The direct consequences on the functioning of an infrastructure and its disruption differs according to several elements:

- type of agent;
- status (e.g. vapour, liquid, solid) and the means of delivery;
- other characteristics of the target.

With regard to the type of agent, **an attack against a CI through the dispersion of chemical, biological or radiological material will interrupt its functioning due to the procedure of decontaminating the affected area, an expensive process** which requires a long time to achieve. In certain instances, the level of damage may render recovery action unfeasible. In addition to these scenarios, any attack involving the use of a dirty bomb (the detonation of a Radiological Dispersal Device, or RDD) will also cause structural damage to buildings.

Referring to the status of an agent and the means of delivery, CIs are usually closed or partially closed buildings. These characteristics can, unfortunately, facilitate the internal diffusion of C, B and R agents in a number of ways, but particularly by suspension in air or dispersal through the HVAC systems (Heating, Ventilation, Air Conditioning).

Illicit use of CBRN within EU territory has been documented by the 2018 Terrorism Situation and Trend (TE-SAT) Report, which also records online exchanges of information and the planning of CBRN attacks, including propaganda and online tutorials (Europol, 2019). Attempts to perpetrate CBRN attacks in the EU were registered in 2018, while in 2019 no such incidents were reported (Europol, 2020). However, in 2019, the International Atomic Energy Agency (IAEA) Incident and Trafficking Database (ITDB) reported 189 incidents regarding unauthorised activities involving RN material, including trafficking or malicious use (IAEA, 2020). Moreover, terrorist organisations may not directly use CBRN materials, but they can target infrastructures in which these kinds of materials are stored. The types of CIs subject to such severe threats are, for example, hospitals hosting radioactive substances

or nuclear installations. This was the case, for instance, when two Belgian nuclear power plants were shut down in 2016 on suspicion of a potential attack by the IS. Nuclear installations have been the target of attempted attacks or sabotage for a long time and, given similar recent incidents[11], there might continue to be a similar trend in the future.

While recent events prove a more extensive use of traditional, especially dual-use weapons in attacks targeting critical entities, interest in the use of CBRN material by terrorists has continued to appear frequently in communication channels monitored by law enforcement agencies, including the internet and social media. Numerous experts and institutions agree on this point and warn about the likelihood of chemical or biological weapons being used in Europe (Europol, 2020).

3.3 Advancing technology and cyber threats: their role and impact on the interdependence and connection of CIs

The types of threats and their potential disruption to CIs can vary according to sectors and evolve with rapidly advancing technology. **CIs are becoming extremely dependent on each other, thereby giving rise to an increasing reliance on networks of connected devices. Interdependency has become a major characteristic in critical entities' functioning and an aspect that needs to be duly considered, especially given the adoption of further or revised measures for the protection of critical entities.**

Due to their high level of interconnectedness, any interruption to a CI service can generate immediate impact, leading in turn to disruption of other co-dependent infrastructures' functionality. A vivid example of this phenomenon, known as 'cascading failure', is the breakdown of production or distribution of energy in a country. This can rapidly affect railway transport, compromise emergency services and disrupt telecommunications or even cause failure in drinking water control and pumping systems.

Growing digitalisation of services, increasingly reliant on the internet, comes with great challenges linked with cybersecurity risks. Such connected systems have become hotspots for security breach attempts, for example in the transport sector. Here, increasing reliance on the use of ICT systems has given rise to 'Intelligent Public Transport' (IPT) services, which certainly offer greater efficiency and improved operations but are also subject to numerous vulnerabilities, including cyber threats. IPT assets are more complex than traditional transport systems as they combine both physical and cyber components. In other words, a bus is no longer a simple public transport vehicle, but is also a data collection and recording system, an information dissemination asset, a mobile Wi-Fi hub and a source of real-time intelligence. Furthermore, IPT presents a strong interconnection between the different components, so that failure in one can be carried over into successive components. In this context, IPT assets are subject to a greater range of security threats, both physical and cyber, which can affect ICT systems and data exchange processes. Digital transformation and related cyber threats can involve all kinds of transport systems, including railway, aviation and maritime networks. Potential disruption from a cyber-attack on public transport could take many forms. Cyber-attacks are able to target transportation security systems and undermine emergency alarms, potentially severely hampering quick reactions by ambulance and similar services in case of emergencies.

The aviation industry is also becoming increasingly reliant on connected networks and computers. Information security incidents are increasing, including cyber-attacks and ICT dependencies' disruptions.

[11] In 2013 and 2014, for instance, two different attacks were attempted against nuclear facilities based in Belgium, respectively at a nuclear research centre in the city of Mol and at Doel Nuclear Power Station. Nuclear facilities are also being threatened by cyber-attacks, as demonstrated by the 2016 incident occurred at the Gundremmingen Nuclear Power Plant (Germany).

The consequences of cyber-attacks on airports could include network failures, security check disruption, passenger delays and cancelled flights, which all lead to a loss of confidence, reputational damage and ultimately financial loss. A potential threat scenario sees a cyber attacker gaining a privileged level of access and/or holding a legitimate user's credentials in order to disrupt check-in services. Once a check-in system is compromised, the criminal can attack connected systems and databases (cascading failure) causing: interruptions or even blackouts to the whole aviation system; issues in disembarking and loading procedures; serious disruptions to airside operations; and greater potential for terrorist acts (e.g. loading of explosives or illegal products in luggage).

Ports are also critical infrastructures particularly vulnerable to cyber-attacks that can disrupt activities related to maritime cargo, passengers and vehicle transports or fishing. The propagation of ransomware can lead to a total shutdown of port operations. Considering the example of the Suez Canal, attention should be placed over risks posed by hostile actors – both state and non-state entities – that might be intentioned to harm its infrastructure. Such threats include potential cyber-attacks, a particularly worrying concern given the vulnerability in Suez's ICT structure (Coates and Greenway, 2021). Such prospect represents a feasible possibility, which would dramatically endanger maritime trade as well as the protection of undersea communication cables.

Looking at sea-based infrastructures and services, **undersea cables merit specific attention, not least because of significant Chinese investments in the field. Building or buying fibre-optic cables is part of Beijing's wider strategy to become leader in providing digital infrastructures and connectivity worldwide** – the so-called Digital Silk Road (Council on Foreign Relations, 2020). China's goal is to expand the use of its own technologies and standards, thereby increasing interoperability with those of countries overseas, especially in emerging digital ecosystems, to create dependencies (Arcesati, 2021). The country wants to expand its influence on networks of fibre-optic undersea cables – both by buying or building them – in the Baltic, Mediterranean and Arctic seas (Arcesati, 2021). This is an aspect that the EU should monitor more closely, since Chinese military forces are working actively on undersea surveillance and monitoring capabilities, leveraging civilian-military integration in this field (Arcesati, 2021).

When it comes to other essential services, energy suppliers such as electricity and gas companies face the same typical threats that plague other industries. **Unique interdependencies between virtual systems and physical infrastructure in the energy supply industry create high risks**. Thus, protecting intercommunication between smart grid networks' devices is vitally important. **Negative consequences could include: loss of power; power overloads; destruction of equipment; and damage to devices throughout the grid.** Devastating cascading effects could then bring down the power grid itself in more than one country. Cyber criminals can affect power plants in different ways, for instance by causing havoc to the entire system operation, causing dangerous excess power provision (potentially damaging equipment) or power cuts. Attacks through malware infection can cause loss of communications and control of the network, leading to a halt in energy production. Denial-of-service (DoS) attacks and distributed DoS (DDoS) attacks[12] can delay, block or corrupt information causing unavailability of power or information exchange in the smart grid. Cyber-attacks can affect power transmission, remotely disconnecting services. This can lead to power disruption within a city or region, including potential long-term damage to equipment, emission of flammable gas, or compromise of sensor, company or even customer data. An example of such an attack against the energy sector (electric network) occurred during 2015 in Ukraine. The attack resulted in a serious disruption of service and blackout, with 27 substations and approximately 225 000 end-users affected. It was part of a larger attack aimed at destabilising the Ukrainian government

[12] These attacks are sophisticated attacks designed to 'flood the network with superfluous traffic' (Cisco 2020), resulting for instance in low network performance.

by targeting power stations, mining and railway infrastructure. The goal was to paralyse public and critical infrastructure by disabling Industrial Control Systems (ICS).

By expanding the scope of the analysis to include other essential services, such as the financial sector, it is important to underline that this is also characterised by deep interdependency between different inter-connected components. These include banks, non-bank financial institutions and a wide range of financial services such as payment service providers, investment companies and markets. **Due to this extensive interconnection, a cyber-attack against one component in any of the EU Member States could produce considerable cascading effects across the whole European financial system. The effects of cyber-attacks on financial sector functioning can lead to a lack of service availability or to a failure of wider infrastructures**. Lack of service availability can cause payment systems to fail across nations, online banking could become inaccessible and cash payments along with reliable information about bank accounts would be unavailable. Cross-border and domestic transactions between banks operating through the affected payment system might not be settled. All transactions involved at one stage or another within the attacked retail payment system would be halted, including the withdrawal of money from Automated Teller Machines (ATMs) or the use of cards for store payments or e-commerce. This would create major liquidity issues, affecting a significant part of society. Directly attacking infrastructures upon which financial systems rely could also result in systemic stability implications, including the disruption of utilities such as: transport; telecommunications; cable companies and technology companies, including providers of data storage or cloud computing along with other services. An attack on multiple power grids, including cross-border services, could overwhelm the defences supported by individual institutions. Especially important is the impact on real-time operations flowing not only through the affected financial institutions but also broader market and payment systems, with ensuing delays or even temporary shut-down. This would further result in a broad loss of confidence, materialising in a reduced volume of operations and increased volatility in market prices of financial instruments.

Technological advancement also applies to the health sector, which has been transformed and improved by the introduction of interconnected assets. In this context, 'Smart Hospitals' are now offering remarkable advantages for their users.

A Smart Hospital can be defined as a 'hospital that relies on optimised and automated processes built on an ICT environment of interconnected assets, based particularly on the Internet of things (IoT), to improve existing patient care procedures and introduce new capabilities'. This advanced system presents significant vulnerabilities related to cybersecurity-related issues: malware, data breaches, medical device tampering, hijacking, skimming, or DoS attacks. These can all severely affect smart hospitals assets and the functioning of the whole infrastructure. Attackers can disrupt the communication network and the identification system; gain access to facilities; interfere with the correct operation of medical devices; alter results; and disclose or steal confidential information, thus hampering the provision of essential medical services. One of the largest attacks on the healthcare sector was the 2017 ransomware attack against the National Health Service (NHS) across England, which disrupted hospital and general practitioners' appointments. Over the last year, cyber-attacks on the healthcare system have increased both in the USA and in Europe, where different healthcare facilities have been shut down for days, with urgent surgeries postponed, new patients redirected, closure of labs and inaccessibility of medical records.

In addition to these categories of attacks which severely impact the functioning of infrastructures and provision of services, it is important to note that the cyber domain also collects an incredibly high amount of data. Hence, cyber-attacks can target two types of data with the aim of disclosing them for criminal purposes: business and technical data; as well as personal data affecting citizens' confidentiality and privacy.

Figure 3: Smart Hospital assets (ENISA, 2016)

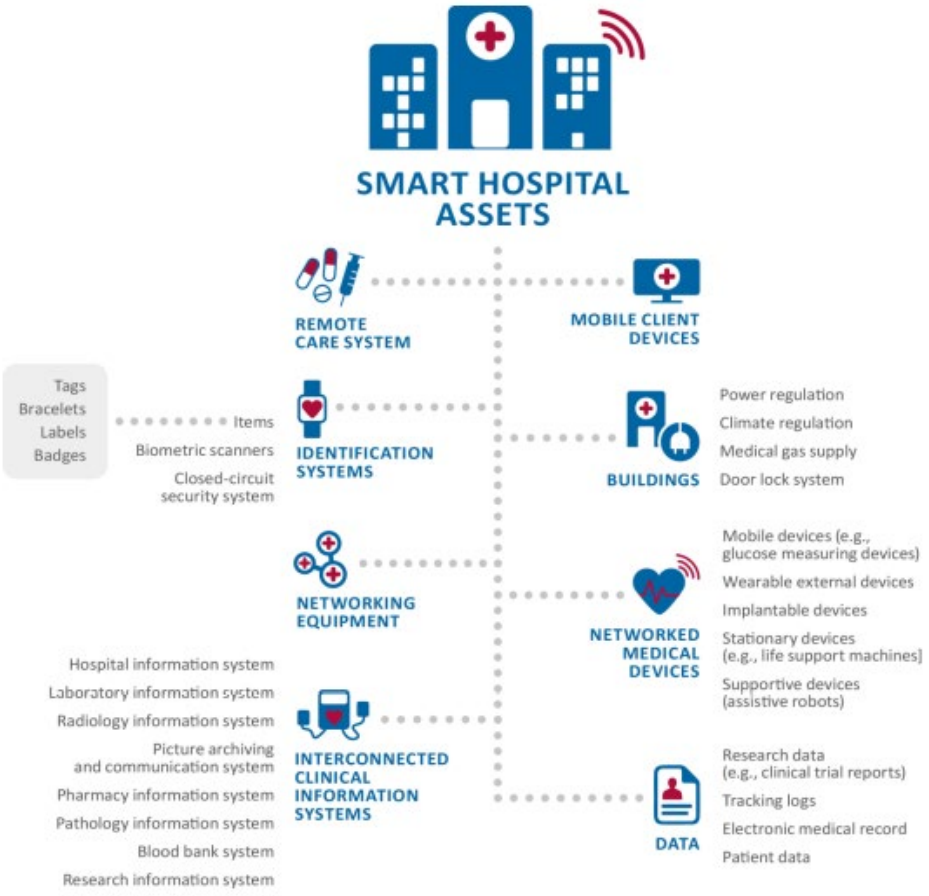


Figure 4: Top 15 Cyber threats (ENISA, 2020)

3.4 EU dependence on foreign technologies

Advancing technology has impacted CIs not only in terms of increased vulnerability, but also with regard to dependence on foreign suppliers for certain categories of equipment. Evaluating the level of EU dependence on foreign technology is not straightforward, as no way of checking the 'suppliers of the suppliers' currently exist (Fiott and Theodosospoulos, 2020). **The EU experiences a relatively high import dependence on many products and primary assets because decades of de-industrialisation have led to manufacturing and skill gaps in key sectors** (Fiott and Theodosospoulos, 2020).

For this reason, EU Member States are pushing towards increasing digital sovereignty to securitise critical infrastructures. There is a need to promote EU computing power, data control and secure connectivity (Breton, 2020a), even though this would still not address the question of security of supply for raw materials. Thierry Breton, European Commissioner for the Internal Market, stressed Europe's potential to act as a leader in the sector, provided it seizes the opportunities offered by data, microelectronics and connectivity (Breton, 2020b).

In order to fill these gaps and reduce its reliance on imported technologies, Europe is investing in different fields. **First, to resist the dominant position of US cloud service providers – such as Amazon, Microsoft and Google – and to overcome the fear of being 'locked out' from US cloud systems, the EU is developing GAIA-X, a 'federated' computing network with specific European security standards. Second, Europe is trying to ease its dependence on components, processors and microprocessors, chips and sensors, which sit at the origin of many strategic value chains such as those for connected cars, phones, IoT, high performance computers and edge computers. Third, MS are trying to master battery technology, a market currently dominated by Asian companies holding 88 % of global lithium-ion manufacturing capacity, with more than 50 % in China alone** (Kelly, 2020). **Finally, Europe is fighting to build a secure and sustainable supply of raw materials, especially metals and rare-earth elements[13] used to produce batteries and renewable energy equipment, which are mainly in the hand of Beijing.** As emphasised by European Commission President Ursula Von der Leyen, it is critical that the EU bloc masters and takes ownership of key available technologies, including quantum computing, Artificial Intelligence (AI), blockchain and chip technologies (Kelly, 2020).

In 2020, the top EU import products were computers and electronic products (15 %), crude petroleum and natural gas (8.7 % of total imports) (Eurostat, 2020a).

The EU is also highly dependent on Russian imports of coal, iron, steel and petroleum products. However, Russia does not hold leverage on MS since oil prices are at historically low levels and represent the main source of revenues for the country. In 2018, the EU dependency rate was equal to 58 %, which means that more than half of the EU's energy needs were met by net imports. Almost two thirds of the extra-EU's crude oil imports (30 %), three quarters of the EU's imports of natural gas and three quarters of solid fuel – mostly coal – imports (42 %) came from Russia (40 %).

During 2020, in four Member States (Estonia, Slovakia, Hungary and Finland) more than 75 % of imports in petroleum oils came from Russia. Ten Member States (Bulgaria, Czechia, Estonia, Latvia, Hungary, Austria, Romania, Slovenia, Slovakia and Finland) imported more than 75 % of their natural gas from Russia. The import share for the largest MS were: less than 25 % for Spain, France and the Netherlands; between 25 % and 50 % for Italy and between 50 % and 75 % for Germany (Eurostat, 2021).

MS also heavily rely on technologies imported from the USA and China, a dependency which has been highlighted by the disruption in supply chains for certain products during the COVID-19

[13] Rare-earth elements are 17 metals used to produce high-tech devices.

emergency. The EU foreign technologies dependency crisis is a growing and vivid threat which affects not only domestic industries and infrastructures in various Member States, but also their security.

To protect CIs, firms develop sophisticated technologies; however, this may lead to the creation of vulnerabilities that governments are slow to understand and/or regulate. This is evident in the context of digital technologies and digital infrastructures like the development of algorithms and/or the use of big data (Fiott and Parkes, 2019). Unregulated cloud data storage, mass surveillance and data collection are a threat to state sovereignty, a crisis worsened by the lack of locally produced cryptography, operating systems, applications and data storage facilities (Spacepol, 2020).

In 2019, more than half of the EU-27 imports of high-tech products from non-EU countries came from China (32.5 %) and the USA (22.5 %) (Eurostat, 2020b).

European states are heavily dependent on China for automatic data processing machines (33.8 %, i.e. computers), telecommunications equipment (33.5 %, i.e. hardware used for telecommunication purposes, from transmission lines and communication satellites to radios, answering machines and smartphones) and electric power machinery (31.8 %) (Fiott and Theodosospoulos, 2020). For example, telecoms operators in Germany and France rely mainly on Chinese equipment (Grieger, 2019). China's rise on the technological landscape has been a key impetus for the growing global concern over security risk in network infrastructures supply chains.

In 2018, the European Union imported 58.48 % (USD 21 448 010.42 K[14]) of machines; parts and accessories of automatic data processing, magnetic or optical readers, digital processing units from China (WITS, 2018). Other countries exporting these utilities to the EU are Thailand (USD 3 461 433.57 K), the Republic of Korea (USD 2 411 164.14 K) and the USA (USD 1 912 522.78 K) (WITS, 2018).

Capable and competitive Chinese producers dominate critical inputs used in upstream production for many industries. This includes essential building blocks for many high-tech electronical products. Critical inputs are, for example, a proper Printed-Circuit Board (PCB) and accompanying diodes, optoelectronics, or resistors; the most advanced microchip is useless without such components, which are mainly imported in the EU from China (Zenglein, 2020). In fact, most global suppliers source components and processes either from their own China-based production facilities or from second- or third-tier component manufacturers based in China.

Moreover, the impellent necessity of adopting 5G infrastructures exposes the EU to a difficult choice: favouring its security ally, the USA, which dominates the software sector, or China, the leading US competitor and main supplier of hardware on the international market (Rühling and Seaman, 2019).

5G's significance for the next generation of technologies is indisputable and so is its critical role in helping countries achieve digital transformation and economic success. Not only does it offer faster and better connection speeds and greater capacity, but it also transforms the way people interact with online services and will enable industries to automate and optimise processes that it is not yet possible to automate today (Jie and Hakmeh, 2020).

In addition to the geopolitical struggle, the nature of this new service poses a threat to national security. In fact, due to new characteristics of the 5G network architecture, mobile network operators will have to rely increasingly on suppliers. Thus, the **risk profile of individual suppliers** will become particularly important

[14] K is a metric corresponding to Trade Value USD 1000.

(NIS Cooperation Group, 2019) and major dependencies on a single one will raise exposure to potential supply interruption.

Huawei, the main Chinese supplier of 5G technology, is also one of the main partners in the PEACE Cable International Network Co. The system is owned by Hengtong Group, offering carrier neutral services to its customers across the shortest direct route connectivity. The key differentiator between PEACE and many of its competitors is the open nature of its network. According to Xiaohua Sun, Chief Operation Officer of PEACE Cable, open access would reduce costs both for PEACE and its end users. PEACE's goal is twofold: on the one hand, they aim to offer interconnection to Asia, Africa and Europe by building market differentiation; on the other hand, they intend to reduce latency in connectivity operations, thus allowing enhanced commercial and consumer applications. PEACE has also signed a partnership with Orange, a France telecommunication company, and PCCW Global, a telecommunication provider based in Hong Kong (PEACE Cable, 2018).

The PEACE Cable system, spanning 12 000 kilometres, will connect three continents and use Interxion's Marseille MRS2 data centre as its landing station (Swinhoe, 2021). By 2019, China has become a landing point, owner, or supplier for 11.4 % of the world's undersea cables and such proportion might grow to 20 % between 2025 and 2030 (Fouquet, 2021).

Subsea cables carry over 95 % of all international data (Martin, 2019) – far more than the amount transmitted by satellite technology. The cables will largely serve to make service faster for Chinese companies doing business in Europe and Africa but will also represent a strategical asset in the hand of China, particularly from the viewpoint of the USA. Since China is not dependent on the EU market thanks to its diversified economy (Fiott and Theodosospoulos, 2020), it could take advantage of European vulnerabilities.

From a national security perspective, governments that wish to limit the use of foreign technology in their critical ICT infrastructure – and military equipment – have tended to design legislation to prevent the procurement of foreign technology for sensitive applications, or to prevent foreign ownership of infrastructure owners/operators (Shead, 2021).

In Germany, for example, a new national cybersecurity strategy is currently being drafted, which will restructure the version currently in force from 2016. The document is expected to be adopted in the spring of 2021 and, with a view to protecting critical infrastructures, it will focus on: ensuring digital sovereignty; making IT security measurable; usability; security by design; and further promotion of Public-Private Partnerships (PPPs). It will not only take into account operators of critical infrastructures, as it has been the case in the past, but also manufacturers and suppliers of hardware and software (Kipker, 2021).

Less attention has been paid to the routing of supply chains of domestic ICT manufacturers. For example, one source of vulnerability can be pinpointed to micro-chips used to power cars, phones, high performance computers, defence systems and AI. Nevertheless, Europe accounts for less than 10 % of their global production. Chips largely come from extra-EU manufacturers including: Nvidia, Qualcomm and Intel in the USA; Foxconn in China; Samsung in South Korea; or TSMC in Taiwan, which China views as a breakaway province (Shead, 2021).

Although most chips are manufactured in the USA, South Korea and Taiwan, vulnerabilities could be introduced through Chinese sub-components at various stages in the fabrication process (The Economist Intelligence Unit, 2014).

On the contrary, when it comes to the employment of software, the quasi-monopoly of US companies leaves no room to domestic suppliers. The Cloud infrastructure (I-Cloud) is one of the services in the hand of the USA. Due to the dependence the world is developing over IT resources offered by I-Cloud (e.g.

computing and storage), this infrastructure has the potential to become as important as the electrical one. It suffices to think that, during February 2017, the correct functioning of the internet was threatened by a mere typo at one of the leading I-Cloud providers. The two main competitors in the field are Amazon and Microsoft, two giants which will be difficult to reach for the newborn European project GAIA-X (Juttner, 2017).

US big tech companies provide many of the vital infrastructures for the world economy, from communications platforms to internet cables and cloud computing facilities. They are also expanding even more into public services, from healthcare to defence contracting and policing. In particular, the contact tracing dispute exemplifies how tech giants' control of digital infrastructure gives them substantial political power. In addition to smartphone hardware, US tech giants control a substantial proportion of communications networks and data centres which power modern digital economies. Undersea cables carrying internet traffic once provided by traditional telecommunications companies subject to extensive regulation are now increasingly owned by Facebook, Google's parent company Alphabet and other tech giants expanding beyond consumer services. Europe's dependence on US providers also leaves its citizens' data vulnerable to state surveillance (Griffin, 2020).

In 2018, Google (with 8.5 % partial ownership, 1.3 % sole ownership), Facebook, Amazon and Microsoft owned or leased more than half of the undersea bandwidth. Currently, Google alone owns six active submarine cables and plans to have eight more ready within two years. Google owns 63 605 miles of cable, Facebook 57 079 miles, Amazon 18 987 miles, while Microsoft 'just' 4 104 miles (Zimmer, 2020).

3.5 Other forms of interference: a focus on hybrid threats

Among unconventional threats, hybrid threats warrant special mention. These embrace a vast range of synchronised, deliberate actions as well as a mix of new and well-known tools – the latter being employed in new ways (Giannopoulos, Smith and Theocharidou, 2021) – with malign intent. **Targeting CIs to interfere and disrupt their functioning is classified as hybrid action. According to the European Centre of Excellence for Countering Hybrid Threats** (Hybrid CoE), **a hybrid threat is 'an action conducted by state or non-state actors, whose goal is to undermine or harm a target by influencing its decision-making at the local, regional, state or institutional level'** (Normark, 2019). A hybrid action exploits vulnerabilities of democracies and institutions, benefitting from ambiguity not only in terms of detection and attribution, but also because of the intrinsic difficulty in classifying a hybrid event due to the use of various measures – conventional and unconventional – in different areas (political, economic, cyber, military, civil) by the attacker. A coordinated hybrid action targets junctures among different dimensions such as (1) local/regional/national/international levels; (2) internal and external; (3) legal and illegal; (4) peace and war. This blurs the lines that traditionally serve to identify and label a threat as well as manage its consequences and response. A hybrid action will try to exploit democratic, legal, procedural or institutional gaps, vulnerabilities and uncertainties. In operational terms, a hybrid action (or set of actions) often interferes in areas where a number of stakeholders are involved in the process and no specific and sole authority is responsible for managing such an event, making the whole response mechanism slower and more complex.

Interferences with the functioning of critical infrastructures, under the form of attacks, disturbances or attempts to disrupt their performance and provision of essential services are considered as a type of hybrid threat. **CI interferences classifiable as 'hybrid' can encompass a number of actions (ENISA, 2019). Firstly, a CI can be damaged physically. Secondly, the 'essential' nature of services provided by a CI makes it easier to create and/or exploit dependencies, when key services belong or are managed by third states or private actors. Foreign Direct Investments (FDIs)** – for example by China or Russia – **and**

the ability to enter the market within CI sectors represent a considerable challenge. Thirdly, espionage (industrial or cyber) and theft of information is another aspect particularly challenging, given the fast technological advancements that force CI security measures to be constantly updated. Fourthly, media control and the spread of disinformation can have an indirect impact on CIs by influencing citizens' behaviour in a harmful way for the protection of CIs and crisis management processes. During a crisis, panic or the lack of correct information encouraged by disinformation can lead to uncontrolled behaviour by people, targeting a specific essential service, provoking shortfalls or putting its correct functioning under pressure due to overload. Civil society in this sense can be a 'battlespace' (Falk, 2020), requiring a set of actions that should increase its resilience, ranging from social trust building to education and awareness-raising, to ensuring the quality of information produced by social and mass media.

Hybrid threats will increasingly challenge the EU. They are an effective asset in the hands of both state and non-state actors that want to exploit MS' vulnerabilities. Offensive activities currently carry advantages for perpetrators in comparison with defensive actions due to difficulties in the attribution of an attack as well as the cost-effectiveness and ubiquity of offensive actions, which are relatively 'cheap' in terms of personnel and resources. The intrinsic nature of hybrid threats can affect a continually changing set of targets and has potentially no limits in switching from one essential service category to another. Consequently, the Proposal for a Directive on the resilience of critical entities that introduces a broader terminology and embraces a number of new categories that are potential targets for hybrid attacks is a step in the right direction. The Joint Communications on a Joint Framework on countering hybrid threats (European Commission, 2016a) and on increasing resilience and bolstering capabilities to address hybrid threats (European Commission, 2018) issued by the Commission provide a set of actions that should promote a holistic approach to counter hybrid threats in the EU. This is aimed at creating synergies between EU instruments and actors involved, from updating strategic communications to establishing common tools for the protection of CI and coordinating with the North Atlantic Treaty Organization (NATO). The European Commission, in cooperation with MS and stakeholders, 'will identify common tools, including indicators, with a view to improve protection and resilience of critical infrastructure against hybrid threats in relevant sectors' (European Commission, 2016a).

Significant progress has been made since 2016 and a number of actions have already been implemented, such as the establishment of an EU Centre of Excellence for Countering Hybrid Threats or the Hybrid Fusion Cell inside the EU Intelligence and Situation Centre (EU INTCEN), to streamline information, thereby increasing synergies and coordination. Nevertheless, there is still inevitably fragmentation both at EU level (inter-agency) and among MS. The Hybrid Fusion Cell composition envisages analytical components specialised in CBRN threats, counterintelligence and cyber (EEAS, 2018).

4. Chinese and Russian presence and/or interference in CIs

4.1 Chinese Foreign Direct Investments (FDIs)

In recent years, there has been widespread concern about FDIs in the EU by third countries, such as China and Russia. These investments are directed both towards standard commercial goods and products as well as strategic assets, services or entities, including CIs within the EU. Chinese investments in ECIs have been steadily growing since 2008, reaching USD 36.5 billion in 2016 (Le Corre, 2018). The country is reportedly looking to expand investment in European infrastructures still further, in the context for example of its Belt and Road initiative (Le Corre, 2018). However, it is worth noting that Chinese CI investments in the EU, peaking in 2016-2017, cannot be framed as 'malicious' *tout court*. After

the economic crisis that hit the EU, having started in 2008, FDIs from Beijing were welcomed by many EU MS as a way of solving their economic problems by relying on privatisation. The lack of appetite from European private investors at that time to engage in privatisation efforts through the EU or the absence – at times – of any other serious investor, coupled with accommodating rules and procedures, concurred to create favourable conditions for FDIs from China. Acquiring the port of Piraeus in Greece (majority share 51 %) during 2016 is an example. Privatisation, in the absence of adequate EU and MS mechanisms or the lack of jurisdiction, could play an enabling role for FDI.

Attempts to expand China's economic influence in the EU and exploit dependencies are not limited merely to FDIs as a way of acquiring CIs. Another component of Chinese presence is represented by state-owned firms offering their services in key areas, such as highway construction, ports, and communications infrastructure (Richet, 2017), or in the management of these entities. China provides these firms with dedicated funds financed by specific banks to operate in a chosen region (Richet, 2017). This is so for the strategically located port of Sines in Portugal, or the construction of a railway connecting Hungary with Slovakia. A distinction thus has to be made among FDIs between those which imply property acquisitions and other which entail complementary actions aimed at, inter alia, building and providing management for some of these infrastructures.

Another aspect going beyond FDIs, but equally related to the resilience of CIs in the EU, is the increasing role of China in providing materials and technologies for essential services (Le Corre, 2018). This risks an overdependence on Beijing in some critical services, supply chains or entities.

A particularly well-known, recent case concerns the development of 5G networks in the EU on behalf of Chinese company Huawei, which is considered to be linked to the Chinese government. This episode sheds light on the worrying implication of China's economic influence in the Union, linked with threats of sabotage and espionage (Cartwright, 2021).

Concerns are rising about the country's respect of intellectual property rights, risks related to price distortions and unequal conditions for market access, together with Chinese discrimination against EU companies in the context of government tenders in the Chinese market (Zenelli, 2019). At the political level, this concern about a potential growth in China's footprint regarding ECIs or CIs in the EU poses some crucial issues related to reciprocity and fair competition in the economy, technological leadership and strategic assets (Zenelli, 2019).

Considering sectors that are recently proving to be critical and fall under the scope of the EC Proposal on critical entities, the health sector is worthy of specific mention. China's intervention in the EU has been increasing since the COVID-19 pandemic, by delivering medical supplies to EU countries (Wong, 2020). The pandemic opened the doors to another dimension of diplomacy, the so-called 'mask diplomacy'. It is worth recalling that China was among the first donors of medical supplies to Italy and Spain, the two countries that were most severely hit in the pandemic's early days. To some experts, this can be seen as an attempt to enhance China's status of 'responsible global leader' (Wong, 2020). In March last year, the European Commission President Von der Leyen expressed concerns about the economic effects of the pandemic weakening strategic European sectors by exposing them to foreign actors. She mentioned, inter alia, the public health and medical sectors (Euractiv, 2020). Nevertheless, Europe has continued to register additional incoming investments from China in the energy, automotive, real estate, industrial and ICT sectors (Le Corre, 2018). As mentioned above, the sector of maritime transport has also received increasing attention, with Chinese companies purchasing seaports and container terminals in Greece, Spain, the Netherlands and France (Babst, 2020).

Against this backdrop, **the current situation on EU FDIs by China is not as worrying as it may initially appear**, for a variety of reasons. Firstly, MS are today much more aware of attempts and risks associated with FDIs by competitors such as China. Some of them welcomed Chinese FDIs at the beginning, for instance Poland and other '16+1' format countries[15] or Greece, but have changed their attitude over time, resulting in stricter national controls on FDIs, which in turn makes investing in the EU more difficult for Beijing. Secondly, China's purchasing power has diminished during recent years and consequently Beijing now has to select with more accuracy sectors in which to invest. These two factors have of late contributed to various failed attempts by China to invest in the EU's CIs, thereby limiting its success despite the continuing relevance of the China's overall economic influence in the EU. Thirdly, the majority of MS are also members of NATO. The Atlantic Alliance is progressively focusing its attention on China and will increasingly do so in the future, as demonstrated by the NATO 2030 Reflection Group's Report (NATO, 2020) as well as the US security agenda. In this geopolitical context, MS that are also NATO allies – especially those depending more on the USA for their security, such as Poland – will probably limit the expansion of Chinese FDIs in CIs and strategic assets, not only for security reasons, but also because of pressure from the USA and within the Alliance.

In the EU's Neighbourhood and in particular the Western Balkans, China (but also Russia and to a minor extent some Gulf countries such as Saudi Arabia) are facilitated in their efforts to broaden influence in a number of sectors, from FDIs to religious infrastructures. Even if most countries in the region are candidates or potential candidates for EU membership, they have yet to put in place all the mechanisms that could help protect their critical entities from foreign interference and cannot rely on a coordinated protection effort such as the one being pursued by the EU.

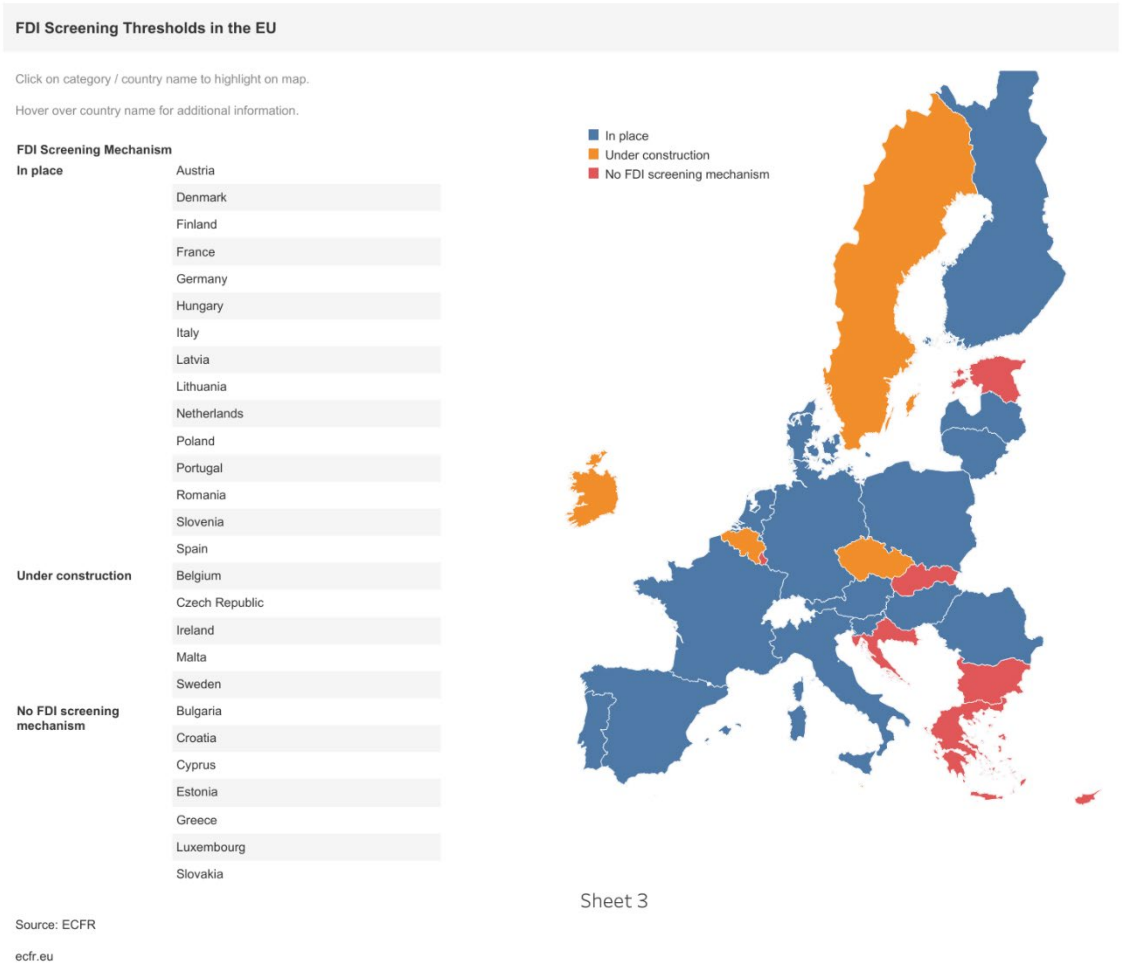
China has been investing in and offering loans to Western Balkan countries for over a decade (Shopov, 2021). Montenegro, for example, has developed a deep dependency on China, which holds one-quarter of the country's national debt (Hopkins, 2021). China lent Montenegro sizable resources[16] for the construction of the Bar-Boljare highway connecting the country to its Serbian neighbour. Unable to repay its debt due in July 2021 Montenegro asked the EU for assistance, claiming that failing to provide support would have meant making it even more dependent on the Asian investor. However, in April 2021 the EU turned down Montenegro's request, albeit agreeing to assist the country with the construction of the highway (Strupczewski, 2021).

Hence, relations with China present a mixture of challenges and opportunities. China is now the EU's second biggest trading partner after the USA and conversely the EU is China's biggest trading partner (European Commission, 2021). The EU will thus pursue a continual engagement with China through constructive dialogues and exchanges. In so doing, it needs to adopt an approach that safeguards its security and its values. At the heart of this approach lies the Comprehensive Agreement on Investment (CAI) aimed at creating a 'better balance in the EU-China trade relationship' (European Commission, 2020a). MS should actively engage in the implementation of the Foreign Investment Screening Regulation, approved in March 2019 and implemented by 15 MS as of November 2020 (European Commission, 2020d). The Regulation requires MS to notify the Commission about FDIs cases falling under their national screening procedures and provide information on the investments if requested (Reuter, 2020). The Commission does not have the power to stop an FDI, which remains exclusively a MS prerogative regarding national security and under domestic legislation when it comes to strategic assets and CIs. However, the Commission and other MS can issue opinions on proposed investments or takeovers and raise their

[15] The 16+1 format is an initiative launched by China in 2012 to expand cooperation between Beijing and Central European MS and Balkan countries, notably: Albania, Bosnia and Herzegovina, Bulgaria, Croatia, Czech Republic, Estonia, Hungary, Latvia, Lithuania, Macedonia, Montenegro, Poland, Romania, Serbia, Slovakia and Slovenia.
[16] China lent Montenegro EUR 1 000 million in 2014.

concerns, which are not legally binding but can have a 'signalling effect' (Reuter, 2020). Those MS that did not have national investment screening mechanisms in place are required to indicate a point of contact for FDI and submit annual reports summarising inward FDI activity (Reuter, 2020).

Figure 5: FDI Screening Thresholds in the EU (European Council on Foreign Relations, 2020)



In order to curb an increasing dependency on China and considering the growing privatisation if CIs, the EU could prioritise the allocation of funds to private sectors investments in critical areas. Particular attention should be given in the EU to the plan for green energy transition, mindful that materials for renewable energy systems are largely imported from China (Cartwright, 2021).

Furthermore, with Chinese attempts to expand control over the EU's ports, renewed efforts for a consistent exchange between the EU and other strategic partners in the maritime security domain will be pursued, with priority given to NATO (Babst, 2020).

Despite EU institutions' increasing attention on this topic, MS' more cautious attitude and the limited success of some Chinese FDIs attempts, the risk will of course persist into the future. China continues to seek expansion in its economic, geopolitical and diplomatic presence in the EU as well as its neighbourhood, which carries uncertainty for the EU and the resilience of its CIs. For instance, the penetration of foreign interests in the EU can take various forms, such as: attempts to influence like-minded political officials and decision-makers in the EU; co-opting scholars and journalists; paying newspapers and online media in MS to publish content promoting a positive view of China and its interests; or establishing think tanks (Benner et al., 2018). In the case of CIs, this attempt results not only in FDIs, but also in co-opting

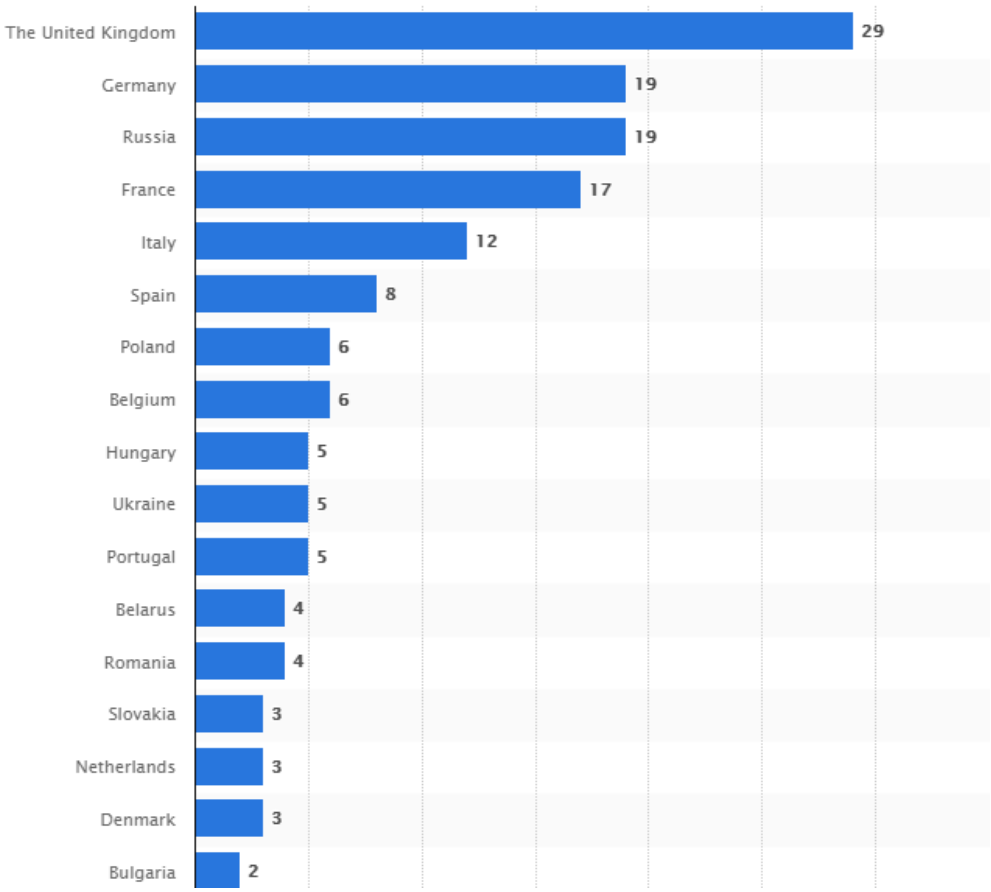
former EU political officials in rival countries' strategic infrastructures (such as Gazprom or Huawei) to exploit their information, expertise and knowledge in order to be more effective in expanding their influence and interests in Europe. This is an insidious threat since it builds on internal divisions among MS; criticisms towards the EU, the democratic system and the values they represent; and affinities of some parties and groups across Europe towards other illiberal models. EU institutions should start a reflection process on what tools could better serve to mitigate the risks posed by this condition.

As aforementioned, a further risk is connected with the expansion of China in the Western Balkans and particularly in the region's CIs. While Western Balkans states cannot benefit from EU protection mechanisms with reference to FDIs, their geographical proximity to Europe could result in cross-border risks for ECIs and CIs in the EU. At the same time, because most of the countries in the region are likely to join the EU at some point, Chinese and Russian investments in the region's CIs become problematic.

4.2 Chinese interference through education and cultural infrastructures

In the education sector, another type of interference can be pursued through 'soft power' and cultural instruments. This is exemplified by China's Confucius Institutes, non-profit educational institutions funded by the government with the purpose of promoting Chinese language and culture. The Institutes have established a number of partnerships with universities in 146 countries, counting 525 Confucius Institutes at colleges and universities worldwide in 2017 (NATO StratCom CoE).

Figure 6: Number of Confucius Institutes in Europe as of December 2018, by country (Statista, 2020)



In 2014 several instances of censorship were exposed, revealing the tight control exerted by the Institutes' governing body *Hanban* and the Chinese Ministry of Education, prompting several universities in the USA and Europe to not renew their contracts (NATO StratCom CoE). These episodes contributed significantly to the perception of Confucius Institutes as instruments of Chinese influence.

As of December 2020, China had established almost 200 Confucius Institutes in the EU. In 2015, accusations of espionage by the Belgian State Security Services resulted in the expulsion of the director of the Chinese Institute and contributed to the termination of cooperation between the Brussels-based Confucius Institute and the Free University of Brussels (European Parliament, 2020a). Similarly, this policy was adopted by German universities in Dortmund and Hamburg, as well as in Sweden. The Confucius Institutes have also been accused of being 'propaganda machines' and of using universities to steal scientific and technological knowledge (European Parliament, 2020a).

4.3 Russian and Chinese cyber-attacks

Russia's cyber interferences in the EU have been alarmingly constant and persistent in recent years. Since 2004, Russia has conducted cyber-attacks in several countries across Europe (Limnell, 2021). For instance, in 2007 financial infrastructures in Estonia were targeted by Russian hackers, which perpetrated a very consistent series of offensives, including DDoS episodes (European Parliament, 2020a; Holcomb, 2020).

France and Germany have both been targets of Russian cyber-attacks. In 2015, the German Parliament suffered a cyber-attack aimed at its information system which compromised its functioning for a prolonged period of time. The incident was attributed to Russia's Main Intelligence Directorate (*Glavnoje Razvedyvatel'noje Upravlenije* – GRU) which denied any involvement in the action (Associated Press, 2020). In February 2021, a Russian hacker group linked to GRU breached several infrastructures based in France, severely compromising the country's supply chain (Cerulus, 2021). Despite Russia's denial, it is suspected that the country interfered with elections both in Paris and Berlin (European Parliament, 2020).

The infamous *WannaCry*, *NotPetya* and *Operation Cloud Hopper* attacks[17] of 2017 have been traced back to Russian hackers (Limnell, 2021) as well. The latter allegedly also saw the involvement of a Chinese firm (Haitai Technology Development) and even the Chinese Ministry of State Security (Deutsche Welle, 2020; Cerulus, 2018).

Russia has been at the centre of disinformation campaigns directed against the EU and there has been evidence of Russian-linked groups working with the aim of undermining elections through cyber-espionage activities (ENISA, 2019). Moreover, Russia plays a key role in the EU energy sector with several MS relying on energy supplies from Moscow. The construction of the new Nord Stream 2 pipeline, running from Russia to Germany across the Baltic Sea, has caused considerable political turmoil within the EU (Fiott and Parkes, 2019).

In June 2020, the EU accused China of having conducted cyber-attacks against European healthcare infrastructures that were involved in the management of the COVID-19 pandemic, including the European Medicines Agency (Stolton, 2020). In 2021, it was discovered that both Chinese and Russian individuals and organisations were behind the malicious attacks which led to sensitive documents about the coronavirus pandemic to be stolen and leaked online (Reuters, 2021). Reportedly, the attackers were especially interested in the vaccine developed by Pfizer and BioNTech and both companies attested there was

[17] WannaCry is a ransomware virus that infected numerous computers impeding users' access. NotPetya is a variant of the Petya malware able to block computer and steal personal data. Operation Cloud Hopper was a global cyber espionage campaign that targeted information systems of multinational companies.

unauthorised access to documents concerning their product. Yet, neither Russia nor China admitted committing these violations.

5. An unprecedented challenge to CIs: the COVID-19 pandemic

Health and medical facilities, regarded as critical infrastructures by EU citizens, have been deeply impacted by the COVID-19 pandemic. **Amongst numerous unsettling effects caused by the pandemic throughout society, there has been widespread disruption to the healthcare sector in a number of countries both within and outside the EU**. A comprehensive study about the status of CIs has not been able to disregard the pandemic's various effects on this sector, starting with hospitals' inability to deal with the massive surge of patients in need of medical assistance. In the face of such an unprecedented emergency, healthcare facilities experienced severe overcrowding and have been unable to provide intensive care to all the people showing severe symptoms or hospitalise all infected patients, who were often forced to wait for many hours in ambulances.

Disruptions caused by COVID-19 have prevented healthcare systems from ensuring adequate medical services to non-COVID-19 patients. In many cases, critical medical activities such as transplants experienced serious delays and risked being suspended. Non-emergency treatments were often cancelled, to avoid the risk of infecting patients. Due to overcrowded departments and wards, people's access to doctors, drugs and Intensive Care Units (ICUs) has been extremely limited, even for patients with chronic and complex medical conditions. The pandemic has also led to a higher demand for mental health services, with the consequential risk of causing increased pressure for already vulnerable and stretched health systems.

Care providers have reportedly struggled to ensure medical care to those in need, due to the absence of adequate intervention paths with specific COVID-19 protocols and procedures. The lack of coordination and communication has intensified the emergency situation. Coordination has been lacking not only within hospitals, but also among different medical facilities and often at international level. This has particularly negative consequences for information-sharing activities. Additionally, primary care providers have found it difficult to provide continuity of care and switch to new methods of service delivery, such as telemedicine, telemonitoring and other e-health solutions.

Another critical issue has been the unavailability of vital resources. The lack of intensive care beds, respirators, protective equipment as well as medical personnel and adequately trained health workers has severely impacted the daily functioning of healthcare infrastructures during the pandemic. The disruption of transport – due inter alia to closed borders, cancelled flights and transnational limitations – has significantly exacerbated this problem, interrupting global supply chains. Furthermore, hospitals and other health facilities have experienced security incidents such as the theft of masks, gloves, protective clothing and disinfectant gel during the crisis.

The pandemic has caused entire hospitals to be reorganised, rapidly changing the life and work habits of many. In addition to contamination risks and extended work shifts, many healthcare workers have been forced to change their way of working, switching from specialist wards to the treating of COVID-19 patients, with consequent high levels of stress and serious repercussions on their physical and mental well-being. While areas dedicated to non-COVID-19 patients contracted out their business, different healthcare facilities devoted a limited number of hospitals or wards to these activities, allowing others to concentrate their resources on treating patients affected by COVID-19. Emergency departments have had to rearrange their activities entirely so that pre-triage work could be undertaken in a dedicated area, one person at a time and at the very moment of arrival, to avoid possible contacts between COVID-19 positive patients and all others. Specific routes for COVID-19 testing, separated from the usual Emergency Department (ED) route have been established for those with acute

symptoms. Finally, COVID-19 positive patients have been transferred to infectious disease units or to internal medicine ward clusters, exclusively dedicated to management of COVID-19 cases.

Hospitals have also been affected by overload and disruption to international telecommunications, insufficient communication procedures and unprecedented attention placed on them by the rest of society. Healthcare facilities and medical staff have had to deal with media, fake news and misinformation in addition to inevitable concerns from patients' relatives as well as issues deriving from language barriers and cultural differences amongst foreign patients.

Alongside these complex issues, healthcare institutions and medical research centres are in any event particularly vulnerable to cyber threats and have been especially so during the COVID-19 pandemic with the ensuing particularly high demand. In April 2020, the International Criminal Police Organization (Interpol) published a report showing a global rise in cyber-attacks relating to the COVID-19 spread. Given the wide extent to which the healthcare sector relies on ICT, cyber-attacks have the potential to be exceptionally disruptive.

Cyber-attacks on medical CIs can coax their victims into downloading malicious apps, opening phishing emails covered up as official outbreak updates but, in reality, distributing malwares via attachments or links, or even add spywares or malwares in publicly available COVID-19-related maps and websites. The targets of these attacks are not only ordinary individuals but also public and private companies in the healthcare industry. During the COVID-19 crisis, even medical manufacturers working to meet the global demand for COVID-19 essential goods are under threat.

Universities and research centres are also being plagued by a myriad of cyber threats, which target their intellectual property, research data and confidential patient details that may be disclosed or stolen. This has been particularly dangerous with respect to medical academic institutions involved in the development of vaccines or innovative treatments, as cyber criminals and state-sponsored espionage have posed risks in terms of accessing information to exploit commercial opportunities.

6. Analysis of the approaches and initiatives in place to face the security threats

6.1 The Proposal for a Directive on the resilience of critical entities and other relevant EU documents: in depth analysis based on the Inception Impact Assessment

Directive 114/2008/EC has been subjected to an extensive evaluation process, starting in 2012. More recently, in June 2020**, the Inception Impact Assessment (IIA) on the Proposal for measures to enhance the protection and resilience of critical infrastructure was published to tackle inadequacies in existing measures highlighted by the evaluation process, mindful also of increasing inter-dependencies and evolving risks**. This IIA provided the basis for revision of the ECI Directive, which resulted in the new Proposal for a Directive of the European Parliament and the Council on the resilience of critical entities published on 16 December 2020. This section provides a close analysis on how the EC Proposal deals with gaps identified by the IIA. Other documents which will be evaluated according to the same benchmark are the Communication on cybersecurity strategy and the Review of the Directive on security of network and information systems.

The IIA illustrated different drawbacks in the framework provided by the ECI Directive, listing specific elements in the protection of critical infrastructures that appear to be only partially or insufficiently tackled.

Firstly, the IIA argues that national 'implementation of the ECI Directive is characterised by discrepancies and overlapping obligations, leading to an uneven playing field for operators'. More precisely, while the ECI Directive succeeded in providing a comprehensive approach and guidelines for the designation of CIs and ECIs, the IIA highlights how it still leaves ample room for interpretation and – consequently – application at national level varies from country to country. The Proposal, for its part, aims for a more uniform application at national level by providing six specific definitions which are relevant to its scope, as listed in Article 2: 'critical entity', 'resilience', 'incident', 'infrastructure', 'essential service' and 'risk'. Furthermore, to support this aim for uniformity, a correct and homogenous implementation of the Directive across MS implies a very smooth and well-coordinated connection across various levels: EU to MS; national competent authorities to critical entities operators; and national authorities to local level/third actors involved. Regular EU and national mechanisms should be put in place to ensure adequate communication and coordination along with the involvement of all relevant stakeholders at EU, national, regional, local and CI level. Nevertheless, despite great attention being given to national competent authorities and operators' responsibilities, the new Directive does not explain in sufficient enough detail exactly how the EU will support and guide MS in the implementation process. Accordingly, to avoid the risk of difficulties across the Union, greater attention must be directed towards providing MS support. Dedicated courses and webinars should be given to ensure that the Directive is ultimately successfully and homogenously implemented. Direct support by the EU could also entail training for critical entities' operators divided by sectors, so as to maximise information exchange and the sharing of lessons learned for those at operational level.

When it comes to risk assessment, the IIA also argues that 'methodologies vary and coordination and response mechanisms are not sufficiently comprehensive in the current framework'. The concept of risk assessment and its implementation are extensively addressed in the EC Proposal. The Proposal takes a significant step further in providing common criteria for MS to identify what qualifies as a critical entity and, by illustrating the key elements of risk assessment, on which outcome MS should base the designation of critical entities. The Proposal also provides for specific reference to the main instruments that are to be considered for risk assessment by MS (for instance, Decision No 1313/2013/EU of the European Parliament and of the Council). Any comprehensive risk assessment should consider a diversified range of risks. Regarding threat scenarios, the Proposal is aimed to 'account for all relevant natural and man-made risks, including accidents, natural disasters, public health emergencies, antagonistic threats, including terrorist offences pursuant to Directive (EU) 2017/541 of the European Parliament and of the Council'. The EU Agenda on counterterrorism is also listed as a reference document for the implementation of the risk assessment to support a comprehensive identification of threats.

Secondly, the IIA specifies that consideration should be given to possible improvement in the exploration of synergies between various initiatives at EU level which have already developed frameworks for CIP. In this regard, it is worth underlining that the Proposal calls for cooperation with other competent authorities, placing specific reference to those designated under the Directive on Security of Network and Information Systems (NIS2 Directive). Cooperation and coordination between the two Directives are notably innovative, considering that in the existing framework neither the ECI Directive nor the NIS Directive contains such a reference.

Looking at other existing initiatives addressed in Section 6.3 of this study, an attempt should be made to explore further synergies with the EU Strategic Compass, a joint effort by all MS to conduct a common threat assessment based inter alia on information gathered from national intelligence services. Specific

attention should be given to the existence of information or conclusions with implications for EU critical entities. Furthermore, at NATO level suggestions have been made regarding the identification of resilience objectives that should be made clearer and measurable at national level, so as to guarantee a set of minimum standards amongst MS. These standards should take into consideration the level of resistance within infrastructure and technologies (Sabatino, 2021).

The ECI Directive's limited sectoral scope is one of its most contested aspects. As underlined in the IIA, this approach restricts application of the Directive to a narrow set of sectors, while also paying insufficient attention to interdependencies and the possible cascading effect of incidents deriving from increasing sectoral interconnection. In this regard, the Proposal introduces remarkable changes, starting by opting for the term 'entity' to replace 'infrastructure', which allows for broader inclusion. Moreover, while the ECI Directive specifically applies only to the transport and energy sectors, the Proposed Directive significantly expands its scope of application. Notably, on the basis of interdependencies among sectors, the Proposed Directive covers: energy, transport, banking, financial market infrastructure, health, drinking water, wastewater, digital infrastructure, public administration and space. The inclusion of such additional sectors is a considerable step forward with respect to the 2008 ECI Directive. Nevertheless, further expansion and inclusion of sectors should be considered. To do so, the legal framework that will substitute the ECI Directive should from the outset consider that other sectors and/or subsectors which have yet to emerge could be added to the list at a later stage. Accordingly, the framework should thus be structured in such a way as to facilitate new additions in a modular and linear manner, given that future crises could escalate the need for rapid regulation of new sectors or specific subsectors. The inclusion of additional sectors is closely linked to their interdependencies which, in turn, require careful consideration of disruptions' cascading effect. Interdependencies and increased connections among sectors are addressed through the links between the Proposed Directive and the NIS2 Directive. While the former deals with physical security and the latter with cyber, the ECI Proposal leaves room for application to other entities pertaining to the digital infrastructure sector that should be treated as equivalent to critical entities.

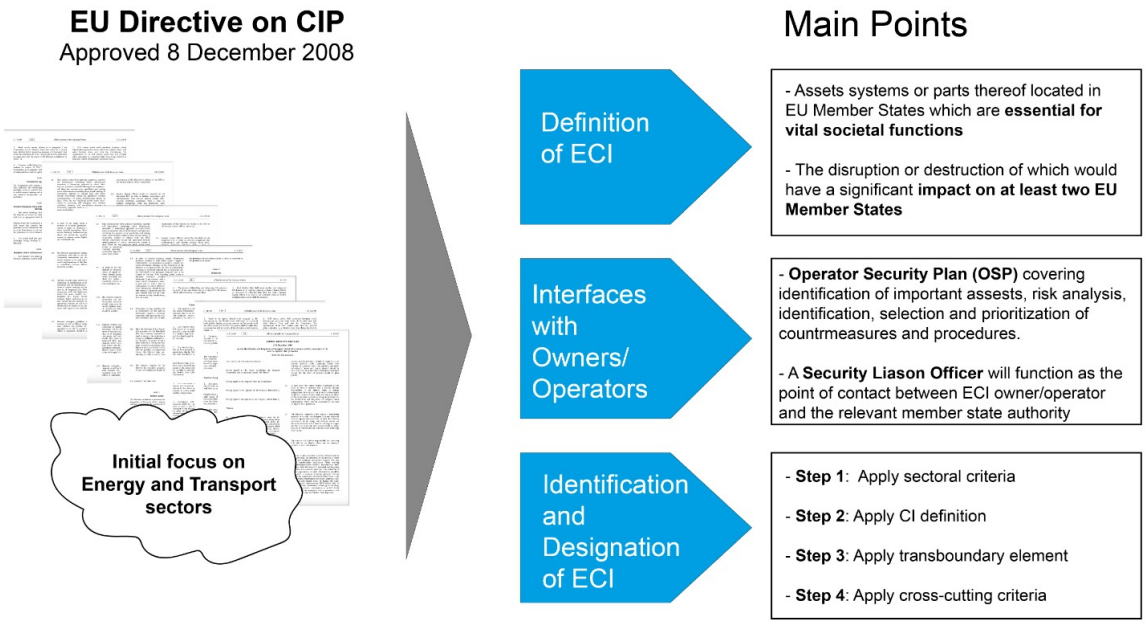
Another limitation of the current ECI Directive, according to the Inception Impact Assessment, is that it focuses exclusively on protection, rather than resilience. In light of this, the Proposed Directive adopts a notable change of perspective by addressing resilience as its main objective. Compared with the ECI Directive, the Proposed Directive makes a profound shift from protection to resilience. Under Article 3, MS are required to produce a strategy on critical entities resilience to set out objectives and policy measures with a view to achieving and maintaining high levels of resilience. Article 14 of the Proposed Directive also indicates that critical entities are those providing essential services to or in more than one third of Member States, thus reinforcing the cross-border approach.

The IIA evaluation also deems coordination and response mechanisms insufficiently comprehensive. An important novelty introduced by the Proposal in relation to these elements is the possibility of an advisory mission to assess the measures implemented, with involvement from the EU Emergency Response Coordination Centre (ERCC). This would provide specific assistance to critical entity operators in their anticipation of risks and adaptation of systems based on expert guidance.

The IIA refers to the additional burden of including reporting requirements imposed by the ECI Directive on infrastructure operators and owners. While reporting obligations remain in place, the current Proposal also establishes a Critical Entities Resilience Group (Article 16) that can support the European Commission and MS in implementing this Directive. To be effective in assisting MS and particularly infrastructure operators, the composition of this Group would need to include representatives in charge of the ECI's

management at operational level. Failing this, the second-best option could be to ensure the participation of CI representatives and operators in a trans-European forum which could convene at least once a year.

Figure 7: Summary of Council Directive 2008/114/EC (European Commission, 2012)



6.2 EU Cybersecurity Strategy and the proposal for a revised Directive on Security of Network and Information Systems (NIS 2 Directive)

On 16 December 2020, **the EC and the High Representative of the Union for Foreign Affairs and Security Policy presented a new Cybersecurity Strategy aimed at increasing Europe's resilience against cyber threats, thereby ensuring citizens and businesses more reliable services. This new Strategy should also strengthen EU leadership in setting international cyberspace norms and bolster cooperation with global partners to provide a safe online environment that guarantees the rule of law, fundamental freedoms and democratic values** (European Commission, 2020e). The innovations advanced in this new Cybersecurity Strategy are numerous.

For instance, it is suggested that a network of Security Operations Centres should be established across the Union, supported by AI, which will be able to identify signs of cyber-attacks and respond in time to prevent serious damage occurring. In essence this will be a 'Cyber shield' (European Commission, 2020e). Small and medium-sized enterprises (SMEs) will receive support under the Digital Innovation Hubs and additional efforts will be invested in research and innovation as well as developing stronger expertise in cybersecurity. The EC is envisaging a new Joint Cyber Unit (European Commission, 2020e) to strengthen cooperation between EU bodies and national authorities responsible for dealing with cyber-attacks and the High Representative has also proposed strengthening the EU Cyber Diplomacy Toolbox to counter malicious cyber activities (European Commission, 2020e). Under this new Strategy, the EU will further enhance cyber-defence cooperation and capabilities, as well as cooperation with international partners, the multi-stakeholder community and third countries. An EU External Cyber Capacity Building Agenda will be created. The EU will also establish an EU Cyber Diplomacy Network to promote its vision of cyberspace and core values. Finally, the new Cybersecurity Strategy envisages large investments in the EU's digital transition, specifically through the Digital Europe Programme, Horizon Europe and the Recovery Plan for Europe. The

Commission also aims at strengthening industrial and technological cybersecurity capacities across the Union, inter alia through projects financed by the EU and national budgets. Under the new Cybersecurity Strategy, implementation of the EU 5G Toolbox in MS is also encouraged (European Commission, 2020e).

The level of activism envisaged in the Cybersecurity strategy is without doubt an important step towards a more proactive role by the EU in this field and, in part, a re-organisation of EU cyber tools. It significantly covers many gaps identified in the Inception Impact Assessment. Nevertheless, it is not clear how the coordination of these measures alongside non-cyber threats will be achieved.

Beside this Cybersecurity Strategy, the EC has adopted a proposal for a revised NIS2 Directive so as to address deficiencies identified in the previous NIS Directive. This proposal is aimed at improving EU response capacities both in the field of cybersecurity and at the level of cyber-resilience within critical public and private infrastructures (European Commission, 2020f) **taking into account the evolving cybersecurity threat landscape** (European Parliament, 2021).

The NIS2 proposed Directive recognises how the digitalisation of services has expanded the threats landscape with increasingly sophisticated challenges.

This NIS2 Directive is conceived to reach a few, well-defined objectives (European Parliament, 2021). It aims at increasing the level of cyber-resilience of businesses operating across all relevant sectors and ensuring their alignment in terms of resilience abilities. In order to reach these goals, the new proposal broadens the previous Directive's scope by covering all medium and large companies whose activities are deemed important for the correct functioning of the economy and society as a whole. In addition, NIS2 defines a list of elements which companies should take into consideration when evaluating their resilience standards and establishes a risk management approach introducing a minimum number of basic security elements common to all businesses which should be applied. Security of supply chains and supplier relationships are also enhanced in the proposal, compared to the previous NIS Directive, by requiring individual companies to address potential cybersecurity risks.

In addition to the sectors already covered by the previous Directive (i.e. healthcare, transport, finance, water, energy, digital services and infrastructures), NIS2 broadens its focus to a series of other areas including, but not limited to: space, chemical and pharmaceutical manufacturing and public administration (European Commission, 2020f).

Regarding the categories already covered by the NIS Directive, one contested element which led to divergent implementations and interpretations was the distinction among categories of operators of essential services (OES); such as energy or transport providers and digital service providers (DSPs, i.e. online marketplaces, online search engines and cloud computing services). This distinction implies, in the NIS Directive, a differentiated approach covering on the one hand all digital service providers, but on the other hand leaving MS discretion in the identification of operators of essential services. The proposal for NIS2 removes the distinction between operators of essential services and providers of digital services, establishing that all medium- and large-sized enterprises in the sectors covered by NIS2 have to comply with the measures.

The proposal also aims at enhancing MS' collective capability to prepare, understand and respond to adverse events. This may be achieved by increasing levels of trust between competent authorities which, in turn, would make then more willing to share relevant information among each other. The NIS2 proposal requires enhanced complementary measures and information exchanges between the two in relation to both cyber and non-cyber resilience.

Since the NIS Directive gives significant flexibility to MS transpositions in their national legal systems, it has consequently been implemented in divergent ways. Such differences are particularly evident with regard to reporting obligations of security breaches and incident reporting, as well as measures related to supervision and enforcement of the NIS. The NIS2 Directive proposal, under Article 5, tries to uniform the application by introducing requirements for MS to establish a cybersecurity strategy, containing strategic objectives and appropriate policy and regulatory measures, with a view to achieving and maintaining high levels of cybersecurity. NIS2 introduces stricter supervisory measures for national authorities and stringent enforcement requirements. Under Article 31, it introduces administrative fines up to EUR 10 million or 2 % of the entities' total worldwide turnover, whichever is higher. Another significant novelty regarding MS implementation is the establishment of a European vulnerability registry (Article 6) and a Registry for essential and important entities (Article 25).

In order to achieve increased preparedness, the Directive establishes a clear *modus operandi* for crisis situations. At European level, the new Directive proposal contemplates simultaneous coordination between the Commission and the European Union Agency for Cybersecurity (ENISA) in carrying out risk assessments of critical supply chains. Under NIS2, the Cooperation Group's role in producing strategic policies on emerging technologies and trends will be broadened. NIS2 envisions an EU crisis management framework, coupled with a Cyber Crises Liaison Organisation Network (EU-CyCLONe), aimed at contributing to the EU's emergency response to large-scale cross-border cyber incidents, supported by a Secretariat provided by ENISA (ENISA, 2020).

6.3 Overview of the main EU initiatives and lessons learned from extra EU partners

The European Union Global Strategy (EUGS) issued in 2016 is a key document in guiding EU Common Foreign and Security Policy (CFSP) (EEAS, 2016). This Strategy introduces the concept of resilience, in line with the new approach of the Proposal for a New Directive on the resilience of critical entities and marking a shift from the previous focus on protection. The Strategy also introduces the notions of comprehensive approach and horizontal coherence between MS and specifies that 'the EU will support the swift recovery of MS in the event of attacks through enhanced efforts on security of supply, the protection of critical infrastructure and strengthening the voluntary framework for cyber crisis management'. This document also states that the EU will increase its focus on cybersecurity and 'technological capabilities aimed at mitigating threats and the resilience of critical infrastructure, networks and services'. **A range of positive developments and EU actions – from the EC Proposal to the NIS2 Directive – demonstrate that over the last 5 years significant progress has been made on enhancing the understanding, awareness and management of challenges faced by CIs**.

The EU Security Union Strategy published in July 2020 takes one further step (Sánchez Nicolás, 2020). The document will cover the next 5 years from 2020, identifying four areas of intervention: physical and cyber infrastructures, new and emerging threats, terrorism and organised crime, and the security ecosystem (European Commission, 2020). In so doing, it adopts a broader perspective that is aligned with the diversified range of threats that challenge EU security.

CIs are the EU's main topic of interest under the 'Future-proof Security Environment' heading, together with cybersecurity and protection of public spaces. Notably, this Strategy considers as outdated the existing EU framework for protection and resilience of critical infrastructures. It emphasises that increasing interdependencies 'mean that disruptions in one sector can have an immediate impact on operations in others' and that the legislative framework needs to address increased interconnectedness and inter-

dependency by adopting both physical and cyber measures. This focus on interconnection and inter-dependence is recurrent in other EU instruments analysed by this study, representing a crucial aspect for the successful implementation of CI security measures.

Furthermore, the Strategy highlights how MS have implemented existing legislation 'in different ways', exercising 'a margin of discretion', by adopting inter alia diverse reporting regimes for operators providing essential services. This is what happened in the case of ECI and NIS Directives, leading to fragmentation by making coordination more difficult, particularly in border regions. At the same time, the Strategy argues that the framework for CIP needs to be accompanied by 'sector-specific initiatives to tackle the specific risks faced by critical infrastructures such as in transport, space, energy, finance and health'. In particular, the EC is working on initiatives concerning the energy, finance and digital sectors. Increasing dependence on online services brings into question their resilience to internet disruptions. Offering CIs a 'channel for secure communications' is mentioned as a key element to protect digital assets in the EU and nationally, thereby also limiting dependency on infrastructures and services located outside of Europe.

Figure 8: EU Security Union Strategy (European Commission, 2020b)

One initiative that is currently in progress for presentation in 2022 is the EU Strategic Compass. The Compass, to which all MS are working and contributing, is aimed at providing a new security policy document building on the EUGS and establishing a common EU threat analysis (Germany's Presidency of the Council of the European Union, 2020). The objective is to reach consensus on a common vision of the security environment and priority threats that the EU should address. The structured strategic dialogue that MS undertook also relies on national intelligence services submitting information and inputs as a combined exercise. The Compass is divided into four sections, each addressing one aspect of the EU Common Security and Defence Policy (CSDP), namely:

- capabilities,
- resilience,
- crisis management,
- and partnerships.

From a CIP perspective, the Compass provides an opportunity to address the matter of the critical entities under the *Resilience* heading, especially with regard to persisting differences among MS –underlined by both the EC Proposal and the EU Security Union Strategy. Based on the Compass' joint intelligence analysis, a dedicated Working Group could address fragmentation in implementing EU Directives, looking particularly into the interpretation of guidelines and diverging perceptions as well as aspects specific to each MS.

Experiences and lessons learned on CIP by other organisations and extra EU-countries should guide and inform EU action. For instance, *'The protection of critical infrastructure against terrorist attacks: Compendium of good practices'* (CTED, UNOCT and Interpol, 2018) is a joint document issued in 2018 by the United Nations Office on Counterterrorism, United Nations Security Council's Counter-Terrorism Committee Executive Directorate and the International Criminal Police Organization (Interpol). This document provides a comprehensive analysis of many CIP aspects: specific terrorist threats to CIs; the development of a national strategy on CIs' risk reduction; the definition of which infrastructures are 'critical'; as well as suggestions on multi-agency approaches and international cooperation. Many case studies are included based on different national activities. The compendium is a complete and detailed guiding paper that can act as a point of reference and an overview of actions taking place worldwide.

In the USA, various tasks related to CIP were centralised under the National Homeland Security Agency with the rationale – shared by key members of Congress – that 'dispersion of homeland security-related functions across federal departments and agencies whose missions were not primarily security related had left the nation vulnerable to terrorist attacks' (Humphreys, 2019). Consolidation was thought to 'ensure clearer lines of executive authority, centralisation of relevant counterterrorism functions, and better inter-agency coordination'. Through the *2002 Homeland Security Act* (Congress of the United States, 2002), a number of infrastructural security functions in areas such as business, finance, commerce, energy, public health, agriculture and environmental protection were transferred to the Department of Homeland Security (DHS) and incorporated under four major directorates. Its goal was to institutionalise CIP through the establishment of a 'purpose-built' department as a 'top federal priority under a unified leadership'. DHS is composed of independent agencies that retain considerable autonomy, which results in CIP still being a 'highly distributed enterprise that competes for limited resources with other priorities across the federal government'. This attempt to centralise the organisational structure and functions under a common authority by Washington should be regarded as an important example for the EU which suffers from an incomparably higher level of fragmentation due to the difficulties in coordinating 27 MS (Congress of the United States, 2018). Managing competition between different parties, between CIs in the same sector or between different sectors of CIs is another lesson to be learned from the US, especially considering that their number will increase significantly if the EC Proposal is adopted. Competitive dynamics have to be taken into account.

When it comes to the cyber domain, the *US Cybersecurity and Infrastructure Security Agency Act* of 2018 is another development, which should be carefully analysed. The establishment of an Agency responsible for both cybersecurity and infrastructure security seems to be in line with the need to centralise and limit fragmentation. The Agency is divided into three departments: cybersecurity, infrastructure security and emergency communication. **The third department deserves particular attention from a European perspective, since considerable problems with emergency or crisis communication persist in several MS, as recently demonstrated by the COVID-19 health crisis. Emergency communication is also another aspect not adequately considered in either the EC Proposal or the Inception Impact Assessment.** The US example could serve as a basis to address this issue in the EU. The Act specifies that in the selection and re-allocation of personnel for the Agency, analysts from the private sector should be hired as well as analysts with the right expertise.

On the opposite side of the world, Australia seems to have reached a similar conclusion. The Australian Government's *Critical Infrastructure Centre Compliance Strategy* mentions that partnership with industry has proven to be an 'effective mechanism to build organisational and sectorial resilience', due inter alia to information sharing between the government and industry.

6.4 Current existing approaches for the resilience of CIs: security by design and personnel training

Different approaches exist for improving the protection and resilience of CIs, not only in terms of procedures and operations but also with regard to the design of CIs themselves. This section will outline two main approaches: security by design and personnel training.

The specific design and architectural elements of a facility can play a significant role in combatting potential threats to its functioning. On European soil, access to key infrastructures such as transport centres or health facilities is free and unrestricted (unless emergency measures have been put in place, such as security checkpoints). Of particular concern are infrastructures, which may host dangerous materials, such as energy providers or medical facilities.

As underlined in the EU Action Plan for the protection of public spaces**, the physical resistance and protection of buildings, along with other measures of 'security by design' are among the major technical solutions to increase infrastructure security, particularly open public spaces** (European Commission, 2017b). Within the development of an infrastructure, this Action Plan underlines how **physical measures for security should be taken into account from the outset. Among these, protective measures in design concepts such as barriers and detection equipment can prevent the intrusion of malevolent actors by, for instance, blocking and thereby preventing attacks with ramming vehicles** (European Commission, 2017b). Protection measures to be considered in the design of venues can also include shelters and dedicated spaces inside the infrastructure with enhanced security and/or physical barriers to safeguard the public from any emergency incident within the location. **The adoption of such protective measures should be coupled with the other main approach for enhancing infrastructure security, namely the provision of appropriate training for all personnel involved, especially those with responsibilities in operational and physical protection.**

Training should address a dual purpose. Firstly, it should aim at providing a thorough understanding of potential security threats and developing a security culture amongst personnel that is primarily involved in safeguarding the CI within which they work. Secondly, supplying instruments to identify possible dangerous situations and providing management training should prepare all personnel for rapid and effective response to any security threat. To be successful, training programmes should be focussed on the identification of role specific training needs related to clearly defined risk exposure and appropriate for a particular service provision. Besides specific needs related to different infrastructure categories and personnel, it is also vital to spot other potential threats which may not be immediately recognised by all security personnel and could, therefore, lead them to underestimate the danger of particular situation. The training of personnel is crucial to develop a security culture and raise awareness in particular regarding 'insider threats': the possibility of an attack by or with the support of at least one facility operator or someone working inside.

When thinking about specific physical protection measures to be designed for a critical infrastructure, a crucial element to consider is that each has its own characteristics and nature. Some have large open areas that need to be preserved, being functional to their service provision. Conversely, others are closed or partially closed. For certain infrastructures, security can be enhanced when access is limited or entry checks

are in place, while others are open and easily accessible by numerous diverse users. Consequently, **it is impossible to apply a unique and homogenous approach for the introduction of physical protection measures. Initiatives and guidelines adopted at EU level form an essential and crucial instrument for supporting Member States in their adoption and implementation of security measures**.

6.5 The importance of public-private cooperation

Widening the scope of CIP and resilience framework as put forward in the EC Proposal raises once again the issue of effective public-private cooperation**. Most CIs in the EU are actually privately owned, with direct consequences for crisis management processes, cooperation with public institutions and the overall infrastructure resilience. Private operators who are responsible for managing CIs do make them resilient and improve their security as well as safety. However, this cannot happen without systemic, continual cooperation and support from public authorities at local, national and EU levels**. Cooperation should take a twofold approach by being directed both from public to private stakeholders involved in CIs as well as from EU institutions to those at national and local levels. In the EC Proposal not enough attention is dedicated to how the European Commission and relevant EU institutions will support MS in making sure that the Directive is properly implemented. A key challenge identified in the IIA concerns the fragmentation and discrepancies in implementation by MS (European Commission, 2020l). By augmenting the number of sectors labelled as critical entities, the EC Proposal risks indirectly increasing fragmentation not only among MS, but also among different categories of critical entities within MS, as well as any specific category of entity across MS. This could be one of the most demanding aspects of the Proposal's implementation. Differences between private and public actors involved in the process are related regarding, inter alia: their goals and mission; functioning; internal rules; normative aspects and legal status; and operational procedures. Countless differences exist not only between public and private stakeholders in general but also between new sectors considered by the EC Proposal. If the Commission wants to look back on a successful and effective implementation of this Proposal in the upcoming years, it should invest time, expertise and the necessary resources now in providing adequate support to MS. On their side, MS have to do the same from a centralised national basis towards the local level and private stakeholders. Private CIs' owners and operators need to see that they are supported at local, national and EU levels so as to guarantee good performance.

The Meridian Process[18] is an open forum initiative gathering senior government officials and policy makers who deal with Critical Information Infrastructure Protection. It has identified certain factors that are necessary for improving public-private cooperation, namely: trust, value, respect, realistic expectations and a code of conduct (CTED, UNOCT and Interpol, 2018). These elements acknowledge the human factor's importance, in the sense that cooperation is made effective by a constructive, informed and positive relationship among people based on human as well as organisational trust and respect. The 'value' factor indicates that the relation has to be 'win-win' in the medium to long term. Concrete benefits in line with the entity's goals and mission need to be clear to the parties involved. A code of conduct can guarantee a greater level of predictability and a more structured relationship where all parties know what to expect from one another, thus avoiding misunderstandings whilst at the same time being aware of mutual limitations. Another relevant element in this sense is the ability to define the scope and form of any cooperation clearly, together with goals, mission and available budget (CTED, UNOCT and Interpol, 2018).

The Meridian Process, the Infrastructure Security Partnership Council and the public-private Operators Forum launched by the EU within the overall framework of the EU Forum on protection of public spaces

[18] See Meridian: connecting and protecting.

are just a few examples of formats that are thought to facilitate public and private sector information-sharing, lessons learned and constructive exchanges.

7. Conclusions: recommendations to the local, national and EU actors and institutions

Ensuring the functioning of CIs is a priority both for national and EU stakeholders. As illustrated by this study, the challenges facing CIs have continued to evolve over time. Particularly worrisome are the **dangers that come with technological advancements such as digitalisation and various systems' growing reliance on web services and connected networks**.

The measures and initiatives taken by the EU, together with ongoing revisions of major legal instruments, represent fundamental milestones towards enhanced security at both national and EU levels for critical infrastructures. To ensure their successful implementation, mindful of expanding the range of measures that can contribute to the security of CI, a set of recommendations is presented below. Since the **protection and resilience of CIs require coordinated and joint efforts at different levels (national, local and EU) and at different times**, the recommendations identified are **addressed to all actors with a cross-cutting approach and systematised according to their potential realisation in the short to long term.**

7.1 Recommendations to the European Commission on the further elaboration and implementation of legal measures for the protection and resilience of CIs

Related to the elaboration and adoption of **new legal measures** – a process triggered by the new EC Proposal Directive in December last year and currently ongoing – some recommendations in this first category should be considered as applicable in the short term. They are followed by another **set of suggestions** for the medium to long term. **They are conceived as actions that could be undertaken by the EC and implemented by agencies and/or bodies as specified in each recommendation.**

1. **One of the ECI Directive's most contested aspects is its diversified interpretation and implementation at national level.** To avoid similar outcomes with the new legal framework currently being discussed, following its presentation in December 2020, continual support from the EU to competent MS authorities should be guaranteed, for instance through the **Critical Entities Resilience Group** to be established in accordance with the Proposal for a new Directive on the resilience of critical entities. To take advantage of the review process that the ECI Directive is undergoing, **well-coordinated connection and communication channels at various levels** should be established in the short term: from the EU to MS; from MS/competent authorities to critical entities operators; and from MS/authorities to local level/third actors involved. This action should be implemented by and participated in as much as possible by the **CIP Points of Contact Group** (composed of competent MS authorities' representatives) and by the **Critical Infrastructure Warning Information Network (CIWIN)** in the framework of the European Programme for Critical Infrastructures Protection (EPCIP) – under the authority of the **Directorate General for Migration and Home Affairs (DG HOME)** –, which aims at **fostering cooperation with MS and supporting them in enhancing the resilience of CIs.**

2. **Key services not classifiable as those identified in the Annex of the Proposal** for a Directive of the European Parliament and of the Council on the resilience of critical entities **represent vulnerable targets for malicious actors.** This is because **those service categories do not fall within the EC Proposal's scope and hence will not benefit from the same level of attention** by the EU and MS. For this reason, in the upcoming steps towards finalising adoption of the Directive, a highly adaptable approach allowing for fast updates and modifications is called for, envisaging the definition of more subtypes/sub-categories of services, adding new types or cancelling others. This could be implemented in an effective way by **involving the JRC and its European Research Network on Critical Infrastructure Protection (ERNCIP)**. **A dedicated Working Group could be established by the JRC, led by ERNCIP and with the participation of representatives from the CIWIN and the CIP Point of contact Group, to monitor and evaluate new subcategories.** Among additional types of services which are not currently foreseen by the EC Proposal and that deserve attention and careful consideration are: the **chemical industry; emerging and potentially disruptive technologies; education**; **democratic institutions** and processes; communication system including **mass media**, **social media and information services**.

3. In line with previous recommendations, careful consideration should be given to the **cascading effect of disruptions hitting a CI**. For this reason, the EC Proposal's scope of application should not be considered exhaustive, but rather facilitate its adaptation through an **approach based on a threats, risks and vulnerability assessment conducted by the JRC together with the EEAS Intelligence and Situation Centre**. The aim should be to design a **modular, 'plug in' method** to ensure rapid **adaptability and flexibility**, thus leaving room to the inclusion of new CIs that might emerge as critical and essential for their own characteristics and/or for connection and interdependencies with other CIs in the long run. The EC Proposal should be considered the cornerstone of critical entities' protection and resilience, sitting at the core of an approach that should be adaptable to changing circumstances over time.

4. Considering the wide range of risks and threats facing CIs, **an all-hazards approach should be maintained**, guide future actions in the adoption of new measures and be preserved in the long term. An all-hazard approach takes into account man-made, technological threats and natural disasters in the critical infrastructure protection process. Technological progress and large interconnection characterising today's CIs pave the way for new vulnerabilities. Hence, careful consideration should be given to emerging challenges such as cyber-attacks and hybrid threats.

5. **Ad hoc workshops and seminars** could be organised in the near future, by the European Commission through the **ERNCIP Project Platform or the CIWIN Platform** on the adoption of new measures, with a twofold aim to (1) raise awareness about the status, challenges and dangers faced by CI, and (2) offer assistance for a more homogenous transposition of measures at local levels by taking into account existing national measures, the extent to which they guarantee sufficient protection of CI, as well as potential overlaps and/or gaps. Courses and webinars could be organised with the **participation of: CI contact points, as designed under the ECI Directive; the EU Forum on the Protection of Public Spaces (composed by the Policy Group with representatives from MS authorities, the Operators' and the Practitioners' Forums); the Partnership for Security in Public Spaces**; as well as **sectoral experts** identified by the MS. In so doing, a dedicated approach can be ensured through a methodology that is tailored to the needs and risks of the CI involved, thus contributing to a more successful implementation of the measures formulated.

6. In the medium to long term, effective support and coordination should be based on the **proper investment of time, expertise and necessary funding from the EU to support MS**. Dedicated and

adequate budget provision by the European Commission through its funding programmes (such as the upcoming **Horizon Europe, the Strategic Forum for Important Projects of Common European Interest – IPCEI**) should be envisaged, with particular attention to education and training, information-exchange and dissemination activities. The same applies to MS and national support towards CIs owners and operators. In the long run, adequate budget for CIP and resilience should be guaranteed in the next Multiannual Financial Framework by MS.

7. With a view towards longer-term actions, **synergies, cooperation and coordination** between EU measures specifically dedicated to CI sectors should be pursued at operational level. This is the case, for instance, with initiatives related to the **EU Action Plan for protection of public spaces and the Action Plan to enhance preparedness against CBRN security risks**.

8. Cooperation and coordination should also include the **exchange of best practices not only between MS but also at local level among owners and operators of CI from different categories**. **Interoperability**, including **interagency communication**, should be ensured through **rapid, secured communication channels** and shared operation plans. MS should make greater use of the **CIWIN Platform**. Although MS have hitherto required its use to be voluntary and not mandatory, its potential as a means of communication and repository of best practices makes it an invaluable instrument for access at national and EU levels equally.

9. The **EEAS** (in particular through the **Intelligence and Situation Centre** and the **Hybrid Cell**) in cooperation with the Commission should make an attempt to **explore synergies with the EU Strategic Compass**, an effort among all EU MS to conduct a **common threat assessment** based also on information gathered **from national intelligence services**. Specific attention should be given to issues or conclusions which may have **implications for EU critical entities**. At NATO level, suggestions have been made regarding the **identification of resilience objectives that should be clearer and measurable at national level**, thereby guaranteeing minimum standards shared amongst the MS. Such standards should take into consideration infrastructure and technologies' levels of resistance.

10. Looking at the measures to be established once the new Directive on the resilience of critical entities has been approved and entered into force, the **composition of the Critical Entities Resilience Group** (foreseen under Article 16) **should comprise representatives in charge of operational levels within ECI management.** If this is not feasible, the second-best option could be to ensure the **participation of CI representatives and operators in a trans-European forum where they can convene at least once a year**. **Advisory missions of assistance from the ERCC for operators of critical entities** such as those envisioned in the Proposal for a new Directive on the resilience of critical entities are a crucial element in helping MS under ERCC guidance.

7.2 Recommendations to the European Commission and other bodies on the adoption of CI security measures

1. In the medium term, CI owners should invest in **security measures**, some of which are already present in certain CIs, for instance through controlled or limited access or emergency shutdown systems. Others measures that could be considered for CIs with easier access for the public and characterised by a high density of people can include **shelters and dedicated spaces inside the infrastructure with enhanced security and/or physical barriers to safeguard the public** from emergency incidents within the location, as well as **adequate evacuation corridors and areas**, notably in the case of **crowded infrastructures** but also public spaces.

2. **All sectors** considered in the **EC Proposal** are particularly **vulnerable to cyber-attacks**. The financial, space, transports, health and energy sectors would all benefit from increasing overall awareness levels **on cyber threats, cybersecurity and cyber safety among** – but not limited to – **CI personnel.**

3. In the medium and long-term, competent MS authorities and bodies, such as the **Civil Protection, the Ministry of Home Affairs (through its law enforcement agencies) and the Ministry of Defence should provide the wider public with adequate education and information on risk prevention**, together with guidelines on what actions can be undertaken and those that should be avoided. This aspect can promote a more active role for citizens in the whole crisis management cycle, from awareness in the prevention phase to correct behaviours during the response phase. **Empowered and educated citizens can be a valuable resource not only in the management of natural disasters,** but also by identifying and **reporting suspicious actions**, going **beyond** the vision of **civil society as a mere target** of malicious actions. Recent trends in terrorism and the rise of hybrid threats (experienced significantly in the COVID-19 pandemic) demonstrate how various aspects of civil society and its functioning are being exploited by malicious state and non-state actors. Given the advantages which targeting civil society gives to an attacker, future threats are increasingly likely to exploit all those aspects that disrupt operations, from supply chains to interference with critical/essential services. Such actions are aimed at intentionally causing casualties or physical and psychological injuries to people.

4. Attacks to CIs have seen the use of explosives and firearms as well **as growing interest in** the use of **CBRN agents**. Hence, in the short to medium term, CI owners should introduce detection technologies for the diversified range of possible weapons entering CIs facilitating prompt identification of their presence to prevent an attack.

5. In the medium to long-term, targeted funding to support MS in implementing physical protection measures and training of personnel could be explored by the European Commission through dedicated measures directly targeting CIs.

6. In **public-private cooperation**, a **trust and respect-based approach** should be actively implemented and not be taken for granted. This will serve to **reduce unpredictability, avoid misunderstandings and increase information-sharing**. Concrete steps in this direction can be undertaken in the short, medium, and long term by the EC through **ERNCIP and CIWIN** with inputs from the **CIP Point of Contacts Group** and selected **experts**.

7. Similarly, in public-private cooperation clear definitions of the scope and mutual goals are necessary to **create realistic expectations from both parts.**

8. Attacks on CIs are one of many synchronised tools or actions that can be used by malicious actor who adopt a horizontal hybrid strategy. Yet, CI protection and resilience is often conceived by operators as a separate area, resulting in a lack of awareness and knowledge on how hybrid threats evolve and act. A top-down effort has to be made by the EC through DG HOME with inputs from MS, the EEAS (for example through the Hybrid Cell), the European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE) and the NATO Strategic Communications Centre of Excellence (NATO StratCom CoE) in the framework of the cooperation based on the 2016 Joint EU-NATO Declaration. This would serve to raise awareness on hybrid threats and especially on their synchronised, multifaceted nature. This education, training and communication effort should be directed in the short, medium and long term towards private stakeholders (CIs owners and operators) as well as local authorities (for example, mayors) and institutions which have limited access to general security

assessments and strategies or could legitimately lack knowledge on strategies utilised by third countries such as China or Russia.

7.3 Implications and recommendations for the European Parliament

The European Parliament, due to its visibility, democratic value and authority and connection with MS through MEPs, can co-participate in actively raising awareness with regard to CIs resilience and protection, playing the role of facilitator towards MS' Parliamentary Assemblies at the national level and towards civil society. This is a particularly important function since the management of threats to CIs, especially when part of a synchronised hybrid strategy, usually is not under the responsibility of one centralised, governmental authority. This aspect makes them difficult to tackle with a top-down governmental approach. Rather, **widespread preparedness, effective management and responsiveness, especially among local and national authorities as well as among civil population, should be pursued and encouraged by the EP through its channels, starting from the EP Liaison Offices in MS. This requires a flexible, multi-level, coherent EU legal framework which the EP can contribute to shape**. Not least because, with regard to CIP and resilience legal and security measures, it is the European Commission, rather than the Parliament, which plays a key role. **Civil society-related measures are those where the EP can have the largest impact** and most of the following recommendations are dedicated to such action.

The legislative, supervisory and budgetary powers of the Parliament leave room for pro-active actions aimed at increasing resilience and protection of CIs in each of the areas of intervention identified in Section 5 of this study, namely: legal, security and civil society, with particular attention to the latter where the EP can contribute the most based on its role and functions.

In the framework of its budgetary powers, the EP should ensure and monitor that, in line with recommendation nr.6 (Legal measures, Section 7.1), **adequate funding is allocated by the EU to the support of MS in the implementation of the ECI Directive**, as well as to education, training and dissemination activities. Funding allocation to CIs should also look at the most critical private sectors, for instance at the framework of the EU Plan for green energy transition, mindful that materials for renewable energy systems are largely imported from other countries. **The EU should create 'domestic' alternatives for Chinese investments especially in those areas, entities and infrastructures considered as critical.**

Amongst civil society-related measures, due to its institutional DNA and democratic nature, the EP can play a unique role that no other EU institution can undertake. By exploiting its tasks such as election observation, setting up inquiries or monitoring democratic processes in Europe**, the EP has a privileged position to look at specific threats targeting democratic and electoral processes, civil society and citizens' behaviour. Raising awareness on these topics, especially among the European population and CIs operators should become a clearer objective of the EP.**

The EP should develop more extensively its **awareness-raising campaigns on disinformation and hybrid threats** which target European civil society, including by **informing Europeans on who are the state or non-state actors that use such tools and for what aims**. Better awareness by civil society on who these actors are and what their goal is could foster a more critical evaluation when being a target of disinformation campaign.

If the EP is ready to play a role in this process, it should **open – in collaboration with the Hybrid CoE and the EP Liaison Offices in MS – a channel for citizens who want to report disinformation campaigns on social media** (Facebook, Instagram, Twitter, and so on) especially for, but not limited to, electoral periods. The establishment of a direct connection between the EP and citizens on this relevant topic, for instance through the creation of a **dedicated digital application (an 'app') and by involving the EP**

Information Offices in MS, could potentially benefit the EP in several ways. Firstly, by increasing the EP's awareness on critical situations and targets of disinformation in any given moment and in advance with respect to official reporting mechanisms. Secondly, by augmenting trust between the EP and civil society. Thirdly, by exercising pressure on social media owners to intervene more promptly.

For **electoral processes**, **dedicated teams monitoring social media** before elections in a given country should be established with a task of rapid reporting.

In the outreach to civil society, especially on **hybrid threats**, it is not enough for the EU to establish the right mechanisms, tools and an adequate **strategic communication** if European citizens remain unaware of these efforts and in MS nobody comes to know about them. Particular attention should be dedicated to **monitoring and periodically assessing their impact, including the number of EU citizens that awareness-raising campaigns reach**. In other words, it is crucial to make sure that communication efforts on hybrid threats, especially disinformation, reach everyone. The use of social media could be an asset.

Each of these actions require coordination and adequate resources in terms of time, personnel, skills, and funding. Enlarging the scope and objectives of **the Hybrid CoE and the EP Liaison Offices** in MS, and strengthening their capacity by augmenting the number of personnel could be a first step towards a more ambitious attitude by the EP in this field.

7.4 Recommendations to the European Parliament on civil society-centered measures for the protection and resilience of CIs

1. **An intergroup dedicated to protection and resilience of critical entities could be established in the EP** temporarily, to increase informal exchanges and spread information on this subject between MEPs. This could be done involving in a **joint format** also **MEPs** from other intergroups related with the topic, such as the **'AI and Digital', 'Sky and Space', 'Sustainable, Long term Investments' and 'Competitive European Industry'** intergroups.

2. In a similar format, a joint meeting between the **Security and Defence, Human Rights and AI and Digital Committees in the EP** could be promoted specifically on resilience and protection of CIs.

3. **Targeted education, awareness-raising and strategic communication** campaigns should be **facilitated by the EP Liaison Offices and the EP Culture and Education Committee**, with the involvement of the **Hybrid CoE** and in cooperation with **NATO StratCom**. They should target EU citizens with the aim of **explaining the complexity of hybrid actions** by providing **concrete examples**. Such efforts should be based on a general assumption that **empowering society** by giving responsibility to/responsibilising citizens is a powerful and underexplored tool for building successful prevention and response to certain threats. With regard to specific content and its dissemination, partnerships with Universities in the EU could be established in order to reach a vast network and exploit existing educational infrastructures. Using effectively mass and social media could help reach all population groups.

4. **Academia, think tanks and experts** from different security fields can participate in the drafting of courses and information material, as well as teaching. Necessary **expertise** should include a **mix of security and more CI-specific knowledge**.

5. When facing a crisis or emergency related to a hybrid attack on a CI, traditional and social media can be 'allies' or 'threat multipliers' in the crisis and communication management towards civil society. Poor quality of media contributes to the **spread of fake news and disinformation** with a **risk**, for

instance, of **uncontrolled citizens' behaviour that can damage the correct functioning of a CI**. The **EC strategy on disinformation contains a Code of Practice for the media, coupled with the Joint Action Plan on Disinformation,** which are valuable tools in increasing media literacy and critical thinking within civil society. However, additional checks on how MS implement these instruments internally could shed light on a more detailed state of the art response on media literacy and 'permeability' to disinformation.

6. **An assessment of how and if the Code of Practice is being used by MS media** could be of help. In addition to the Code of Practice, **a voluntary Code of Conduct** could be established for the media, specifically on how to communicate in case of a security-related threats such as a CI disruption. The Code should be established in compliance with freedom of speech, human rights, as well as democratic and liberal values. Some form of incentive for those media that comply with the Code could be envisaged.

7. The communication strategy of some MS, for instance during the health crisis due to COVID-19, has been highly disorganised and incoherent, favouring the spread of incorrect information. **Guidelines for strategic communication addressed to citizens during a public health crisis** should be established at EU level. Communication should be brief, clear and direct.

References

Alsop, T. 'Classifying computers and software', Acccess2Market, European Union, 2020.

Anglmayer, I., 'European critical infrastructure – Revision of Directive 2008/114/EC', European Parliamentary Research Service (EPRS), European Parliament, February 2021.

Arcesati, R., 'China's Digital Silk Road and Undersea Cables: Prospects and Threats Posed to the EU', German Marshal Fund Online Event of 19 March 2021.

Babst, S., 'It's time for NATO and the EU to have a serious conversation about China', *Friends of Europe*, September 2020.

Balkan, S. 'Daesh's drone strategy technology and the rise of innovative terrorism', SETA Report, 2017.

Benner, T. et al., 'Responding to China's Growing Political Influence in Europe', GPPI and MERICS, February 2018.

Breton, T., 'Europe: The Keys To Sovereignty', European Commission, September 2020a.

Breton, T. 'Speech at the Hannover Messe Digital Days', July 2020b.

Candelieri, A. et al., 'Vulnerability of public transportation networks against directed attacks and cascading failures', *Public Transport* No. 11, February 2019, pp. 27–49.

Cartwright, G., 'EU must be wary of wider Chinese threat regarding critical infrastructure', *EU Today*, March 2021.

Cisco website, 2020.

Choraś, M. et al., 'Cyber Threats Impacting Critical Infrastructures', in *Managing the Complexity of Critical Infrastructures, Studies in Systems, Decision and Control,* Vol. 90, February 2016, pp. 139-161.

Coates, V. and Greenway, R., 'The Next Suez Threat? A Big Hack', in *Bloomberg*, 30 March 2021.

Congress of the United States, *Cybersecurity and Infrastructure Security Agency Act,* 2018.

Congress of the United States, *Homeland Security Act*, 2002.

Council on Foreign Relations, 'Assessing China's Digital Silk Road Initiative', 2020.

Deutsche Welle, 'Unter dem Deckmantel der Hilfsbereitschaft', 14 December 2016.

EEA (European Environment Agency), 'Adaptation challenges and opportunities for the European energy system – Building a climate-resilient low-carbon energy system', *EEA Report* No 1, 2019.

EEAS (European External Action Service), 'A Europe that Protects: Countering Hybrid Threats', June 2018.

EEAS (European External Action Service), 'Shared Vision, Common Action: A Stronger Europe – A Global Strategy for the European Union's Foreign And Security Policy', June 2016.

ENISA, 'Cyber Security Strategy for Germany', 2011.

ENISA, 'Main incidents in the EU and worldwide – ENISA Threat Landscape', October 2020.

ENISA, 'Blue OLEx 2020: the European Union Member States launch the Cyber Crisis Liaison Organisation Network (CyCLONe)', 2020.

ENISA, 'Smart Hospitals. Security and Resilience for Smart Health Service and Infrastructures', November 2016.

ENISA, 'Threat Landscape Report 2018 -15 Top Cyberthreats and Trends', January 2019.

EU Science Hub, 'Critical infrastructure protection', August 2019.

EU-CIRCLE, 'Impacts of Climate Change and Extreme Weather Events on Critical Infrastructure – State of the Art Review and Taxonomy of Existing Knowledge', July 2016.

Euractiv Network, 'How effective is China's 'mask diplomacy' in Europe?', EURACTIV.com, 26 March 2020.

European Commission, 'Countries and regions: China', in Trade Policy, February 2021.

European Commission, 'EU and China reach agreement in principle on investment', Press Release of 30 December 2020a.

European Commission, 'EU Security Union Strategy: connecting the dots in a new security ecosystem', Press release of 24 July 2020b.

European Commission, 'Evaluation study of Council Directive 2008/114 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection', 2020c.

European Commission, 'Factsheet on the EU investment screening framework', November 2020d.

European Commission, 'New EU Cybersecurity Strategy and new rules to make physical and digital critical entities more resilient', Press Release of 16 December 2020e.

European Commission, 'Proposal for directive on measures for high common level of cybersecurity across the Union', December 2020f.

European Commission, 'The Directive on security of network and information systems (NIS Directive)', December 2020g.

European Commission, 'The EU's Cybersecurity Strategy in the Digital Decade', JOIN/2020/18 final, December 2020h.

European Commission, Press release, 'European Democracy Action Plan: making EU democracies stronger', December 2020i.

European Commission, Inception Impact Assessment on the Proposal for measures to enhance the protection and resilience of critical infrastructure, June 2020l.

European Commission, 'Joint Communication to the European Parliament, the European Council and the Council – Increasing resilience and bolstering capabilities to address hybrid threats', JOIN/2018/16 final, June 2018.

European Commission, 'Major accidents hazards from disasters to success', 2017a.

European Commission, 'Action Plan to support the protection of public spaces', COM(2017) 612 final, 2017b.

European Commission, 'Comprehensive Assessment of EU Security Policy', SWD(2017) 278 final, July 2017c.

European Commission, 'Europeans' attitudes towards security', *Special Eurobarometer* 464b, December 2017d.

European Commission, 'Joint Framework on countering hybrid threats: a European Union response', JOIN/2016/018 final, April 2016a.

European Commission, 'Communication from the Commission to the European parliament, the Council, the European economic and social committee and the committee of the regions supporting the prevention of radicalisation leading to violent extremism', 2016b.

European Commission, 'European Commission Staff working document on the review of the European Programme for Critical, Infrastructure Protection (EPCIP)', 2012.

European Commission, DG Home website, 'Protection'.

European Parliament, 'A Europe Fit for the Digital Age – Review of the Directive on Security of Network and Information Systems', *Legislative Train Schedule*, February 2021.

European Parliament, 'Question for written answer E-006751/2020 to the Commission: Confucius Institutes in the EU', Parliamentary Question by De Man F. (ID), December 2020a.

European Parliament, Motion for a European Parliament resolution on foreign funding of radical Islam in Europe, B9-0087/202028, January 2020b.

European Parliament, Question for written answer E-000840-17 to the Commission: Foreign funding for Islamic centres in Italy, Parliamentary question by Fontana L. (ENF), 6 February 2017.

European Parliament, Question for written answer E-008494/2016/rev.1 to the Commission: Foreign funding, Parliamentary questions by Rübig P. (PPE), 16 November 2016.

European Union, Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, Official Journal of the European Union L 345/75, December 2008.

Europol, 'Attacks on critical Infrastructures', 2014.

Europol, 'Terrorism Situation and Trend Report 2020 (TE-SAT)', June 2020.

Europol, 'Terrorism Situation and Trend Report 2019 (TE-SAT)', June 2019.

Europol, 'Terrorism Situation and Trend Report 2017 (TE-SAT), June 2017.

Eurostat, 'EU imports of energy products – recent developments', June 2021.

Eurostat, 'International trade in goods – a statistical picture. Extra EU trade in goods', 2020a.

Eurostat, 'From where do we import energy and how dependent are we?' *Shedding light on energy in the EU*, 2020b.

Eurostat, 'Production and international trade in high-tech products', 2020c.

Falk, B. J., 'Strategic citizens: Civil society as a battlespace in the era of hybrid threats', *Hybrid CoE Strategic Analysis* No. 25, November 2020.

Fiala D., Regulating foreign funding of Islam in Europe in order to prevent radicalisation and Islamophobia, Council of Europe, 17 September 2018.

Fiott, D. and Parkes, R., 'Protecting Europe – The EU's response to hybrid threats', *European Union Institute for Security Studies (EUISS) Challiot Paper* No. 151, April 2019.

Fiott D. and Theodosospoulos V., 'Sovereignity over supply?', *European Union Institute for Security Studies (EUISS)*, December 2020.

Forzieria, G. et al., 'Escalating impacts of climate extremes on critical infrastructures in Europe', *Global Environmental Change,* No. 48, April 2017, pp. 97-107.

Fouquet, H. 'China's PEACE cable in EU raises tension with the US', Bloomberg, 2021.

Germany's Presidency of the Council of the European Union, 'Strategic Compass: Developing strategic principles', August 2020.

Giannopoulos, G., Smith, H. and Theocharidou, M., The Landscape of Hybrid Threats: A conceptual model, Hybrid CoE and JRC, 2021.

Global Terrorism Database.

Government of Australia Critical Infrastructure Centre, 'CIC Compliance Strategy', 2018.

Government of Belgium Service Public Fédéral Intérieur, Loi relative à la sécurité et la protection des infrastructures critiques, *Moniteur Belge*, July 2011.

Government of Finland, Finland's Cyber security Strategy, January 2013.

Government of France Secretariat-General for National Defence and Security, 'La Sécurité des Activités d'importance Vitale', March 2016.

Government of France, The Critical Infrastructure Protection in France, January 2017.

Government of Ireland Office of Emergency Planning (OEP) and Government Information Service (GIS), Strategic Emergency Management Guideline 3 – Critical infrastructure Resilience, February 2019.

Government of the United Kingdom Cabinet Office, Public Summary of Sector Security and Resilience Plans, 2017.

Grieger, G., '5G in the EU and Chinese telecoms suppliers', European Parliamentary Research Service (EPRS), European Parliament, April 2019.

Griffin, 'Covid-19 has made Europe's technological dependence on the US clearer than ever', *Sciences Po Chair Digital, Governance and Sovereignty*, 2020.

Hallegatte, S., Rentschler, J. and Rozenberg, J., 'Lifelines: The Resilient Infrastructure Opportunity', in *Sustainable Infrastructure*, World Bank Report, 2019.

Hanneman, T. and Kratz A., 'CrossBorder Monitor (CBM). People's Republic of China. European Union Direct Investment – 4Q 2020', The Rhodium Group, February 2021.

Hopkins, V., 'Montenegro calls for EU help over $1bn Chinese highway loan', *Financial Times*, 11 April 2021.

Humphreys, B. E., Critical Infrastructure: Emerging Trends and Policy Considerations for Congress, Congressional Research Service, July 2019.

Hybrid CoE webpage, Hybrid threats as a concept. Accessed March 2021.

IAEA, IAEA Incident and trafficking Database (ITDB), 2020.

Institute for Economics & Peace, 'Global Terrorism Index', November 2020.

Lilyanova, V., Saudi Arabia in the Western Balkans, European Parliamentary Research Service (EPRS), European Parliament, November 2017.

Jie, Y. and Hakmeh, J., 'The UK's Huawei Decision: Why the West is Losing the Tech Race', Chatham House, 2020.

Juttner. A., 'Dangerous dependency on US cloud providers – The European response: Airbus 2.0?', Blog Activ.EU. March 2017.

Kalvach, Z. et al., 'Basics of soft targets protection – guidelines (2nd version)', Soft Targets Protection Institute, 2016.

Kelly, E., 'Decoding Europe's new fascination with 'tech sovereignty', *Science Business*, 2020.

Kipker. D., 'Legal Framework for Critical Infrastructures in Germany and Europe', Intrapol. 2021.

Le Corre, P., 'Chinese Investments in European Countries: Experiences and Lessons for the "Belt and Road" Initiative', in *Rethinking the Silk Road*, Meyer, M. (ed.), 2018, pp. 161-175.

Liekkilä, K., 'Finnish Approach to Critical Infrastructure Protection', National Emergency Supply Agency, 2018.

LISA Institute, Infraestructuras críticas: definición, planes, riesgos, amenazas y legislación, October 2019.

Marrone, A., and Muti, K., 'NATO's Future: Euro-Atlantic Alliance in a Peacetime War', *IAI Papers* Vol. 20 No. 28, October 2020.

Martin, H. 'Undersea Espionage: Who Owns Underwater Internet Cables?', *MC Gill International Review*, 2019.

Meridian Process webpage, accessed in February 2021.

Muti, K., 'Rischi Cbrn e Covid-19: sbagliando si impara', in *Affarinternazionali*, 13 December 2020.

NATO, NATO 2030: 'United for a New Era', NATO Reflection Group, 2020.

NATO Strategic Communication Centre of Excellence (StratCom CoE), 'Confucius Institutes', Thematic Area: GONGOs, 2019.

NEC Corporation, Commercial facilities as targets: new threats to critical infrastructures, 2016.

NIS Cooperation Group, 'Coordinated Risk Assessment of the Cybersecurity of 5G Networks', Report, October 2019.

Normark, M., 'How states use non-state actors: A modus operandi for covert state subversion and malign networks', *Strategics Analysis 1/2019*, Hybrid CoE. 2019.

OECD, Protection of 'Critical Infrastructures' and the Role of Investment Policies Relating to National Security, May 2008.

OECD, Good Governance for Critical Infrastructure Resilience, April 2019.

Parliamentary Assembly of the Council of Europe (PACE). 'Funding of the terrorist group Daesh: lessons learned'. Resolution 2211, 2018.

PEACE Cable Website, 'Peace Cable, The Carrier's Cable'. Accessed 2021.

Persi Paoli, G. et al., 'Behind the curtain – The illicit trade of firearms, explosives and ammunition on the dark web', RAND Corporation Report, 2017.

Pethő-Kiss, K. 'Countering Terrorist Acts against Christian Places of Worship', *Perspectives on Terrorism* Vol. 14 Issue 3, June 2020, pp. 74-86.

Pompes, M. A. and Tarini, G., 'Nuclear Terrorism – Threat or Not?', *AIP Conference Proceedings* No. 1898, 2017.

Ramzy, A. and Peltier, E., 'What We Know and Don't Know About the Beirut Explosions', *New York Times*, August 2020.

Reuter, M. 'Responding to the China challenge: The state of play on investment screening in Europe', *European Council on Foreign Relations*, November 2020.

Richet, X., Geographical and Strategic Factors in Chinese Foreign Direct Investment in Europe, 2017.

Rühling, T. and Seaman, J., '5G and the US-China Tech Rivalry: A Test for Europe's Future in the Digital Age', SWP Comment 2019/C 29, June 2019.

Robert Schumann Foundation, 'European Democracy, a fundamental system to be protected', European Issue n°578, November 2020.

Sabatino, E., 'Tutti gli occhi sugli Stati Uniti alla ministeriale Nato', *Affari Internazionali*, February 2021.

Sadeghi, A.-R., Wachsmann, C. and Waidner, M., 'Security and privacy challenges in industrial Internet of Things', *52nd ACM/EDAC/IEEE Design Automation Conference (DAC)*, 2015.

Sánchez Nicolás, E., 'EU five-year security plan to focus on critical infrastructure', *EUobserver*, July 2020.

Shead, L., 'Europe is focusing on 'tech sovereignty' as tensions flare between the U.S. and China', *CNBC*, 2021.

Shopov, V., 'Decade of patience: How China became a power in the Western Balkans', European Council on Foreign Relations (ECFR), February 2021.

Spacepol, 'EU foreign technologies dependency crisis: research project seeks solutions and new policies', February 2020.

Statista, 'Telecommunications equipment – statistics & facts', 2020.

The Economist Intelligence Unit, 'Politics, cyber-security, trade and the future of ICT supply chains', 2014.

Strupczewski, J., 'EU says it can't help Montenegro on China loan but can on financing', *Reuters*, 12 April 2021.

Thornton, M. et al., Non-Binding Guidelines – For Application of the Council Directive on the Identification and Designation of European Critical Infrastructure and the Assessment of the Need to Improve Their Protection, JRC Scientific and Technical Reports, 2008.

Torch Marketing and KNM Media, 'Critical Infrastructure Protection & Resilience Europe / Asia, Conference Review Discussion', 2016.

United Nations Counter-Terrorism Committee Executive Directorate (CTED), United Nations Office of Counter-Terrorism (UNOCT), and International Criminal Police Organization (Interpol), 'The Protection of Critical Infrastructures Against Terrorist Attacks: Compendium of Good Practices', October 2019.

United Nations Office for Disaster Risk Reduction (UNDRR), 'Making Critical Infrastructure Resilient: Ensuring Continuity of Service – Policy and Regulations in Europe and Central Asia', 2020.

WHO, 'WHO reports fivefold increase in cyber attacks, urges vigilance', Press Release of 23 April 2020.

Wong, B., 'China's Mask Diplomacy', *The Diplomat,* March 2020.

World Integrated Trade Solution website (WITS), 'European Union Machines; parts and accessories of automatic data processing, magnetic or optical readers, digital processing units imports by country'. 2018. 2018.

Zenelli, V., 'Mapping China's Investments in Europe, The last eight years have seen a paradigm shift in Chinese investments in Europe', *The Diplomat*, March 2019.

Zenglein. M., 'Mapping and recalibrating Europe's Economic interdependence with China', China Monitor, Merics, 2020.

Zimmer J., 'Google Owns 63,605 Miles and 8.5 % of Submarine Cables Worldwide', Broadbandnow. December 2020.

PE 653.637
EP/EXPO/INGE/FWC/2019-01/LOT4/R/02

Print ISBN 978-92-846-8183-9 | doi: 10.2861/179721 | QA-02-21-731-EN-C
PDF ISBN 978-92-846-8182-2 | doi: 10.2861/221461 | QA-02-21-731-EN-N