EUROPEAN
COMMISSION

Brussels, 16.12.2020
SWD(2020) 358 final

COMMISSION STAFF WORKING DOCUMENT

IMPACT ASSESSMENT

Accompanying the document

Proposal for a Directive of the European Parliament and of the Council

on the resilience of critical entities

{COM(2020) 829 final} - {SEC(2020) 433 final} - {SWD(2020) 359 final}

Table of contents

Glossary

Term	*Acronym*
Artificial intelligence	AI
Computer security incident response team	CSIRT
Continuity of government	COG
Critical entity of European significance	CE-ES
Critical information infrastructure	CII
Critical infrastructure	CI
Critical infrastructure protection	CIP
Critical infrastructure resilience	CIR
Critical Infrastructure Protection Point-of-Contact	CIP PoC
Critical Infrastructure Warning Information Network	CIWIN
Digital Operational Resilience Act	DORA
European Union Agency for Cybersecurity	ENISA
European Union Programme on Prevention, Preparedness and Consequence Management of Terrorism and other Security-Related Risks	CIPS
European Critical Infrastructure	ECI
European Critical Infrastructure Protection	ECIP
European External Action Service	EEAS
European Programme for Critical Infrastructure Protection	EPCIP
European Reference Network for Critical Infrastructure Protection	ERNCIP
Extreme weather event	EWE
Foreign direct investment	FDI
Global navigation satellite systems	GNSS
Industrial control system	ICS
Information and communications	ICT

technology	
Internal Security Fund	ISF
International Standards Organisation	ISO
Multiannual Financial Framework	MFF
National critical asset	NCA
National critical infrastructure	NCI
Network and Information System	NIS
North Atlantic Treaty Organization	NATO
Operator of essential services	OES
Operator Resilience Plan	ORP
Operator Security Plan	OSP
Organisation for Economic Co-operation and Development	OECD
Personal protective equipment	PPE
Public-private partnership	PPP
Regulatory Fitness and Performance Programme	REFIT
Supervisory control and data acquisition	SCADA
Security Liaison Officer	SLO
Small- or medium-sized enterprises	SME
Treaty establishing the European Community	TEC
Treaty on European Union	TEU
Treaty on the Functioning of the European Union	TFEU
Union Civil Protection Mechanism	UCPM
United Nations International Strategy for Disaster Reduction	UNISDR
United Nations Office for Disaster Risk Reduction	UNDRR
Unmanned aircraft system	UAS

World Health Organisation	WHO

Term	***Definition***
Critical infrastructure	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[1]
European critical infrastructure	An infrastructure the disruption or destruction of which would have significant cross-border impact on at least two Member States[2]

[1] Council Directive 2008/114/EC on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection.

[2] Council Directive 2008/114/EC on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection.

1. INTRODUCTION: POLITICAL AND LEGAL CONTEXT

The livelihoods of European citizens and the health of the European economy and internal market depend on the reliable provision of different kinds of essential services, i.e. those that are essential for maintaining critical societal and economic activities. These services, vital in the best of times, are all the more crucial as Europe continues to manage the effects of and gradually recover from the ongoing Coronavirus pandemic. The provision of essential services to European citizens and businesses depends on the reliable performance of critical infrastructures (CIs). This means that the infrastructures must be **resilient**, i.e. able to resist, absorb, accommodate to and recover from incidents that have the potential to result in disruptions. In other words, they must be adequately **protected** against different risks[3] **and able to 'bounce back'** into operation in the event of disruptions that will nevertheless occur from time to time (see Annex 5).

Given the European implications of CI disruptions, the EU has taken different actions, including through the European Programme for Critical Infrastructure Protection (EPCIP)[4] and the 2008 European Critical Infrastructure (ECI) Directive[5]. The Directive, which applies only to the energy and transport sectors and focuses solely on protective measures in the face of primarily terrorist threats of a non-cyber nature, provides a procedure for designating ECIs, the disruption or destruction of which would have significant cross-border impact on at least two Member States, as well as requirements for ECI operators and the Member States that host them.[6] To date, only 94 ECIs have been designated, of which two-thirds are located in three Member States.

The scope of the EU's work on CI extends beyond the EPCIP and the ECI Directive. Since 2008, sectoral and cross-sectoral actions on *inter alia* climate proofing, civil protection, foreign direct investments (FDI) and cybersecurity (Network and Information

[3] Risk is defined as the combination of the likelihood of the occurrence of a threat or hazard and its negative consequences, which can be exacerbated by many different factors, not least the nature and character of CIs and their operations. Risk assessment, meanwhile, is a methodology by which to determine the nature and extent of risk by analysing potential hazards/threats and evaluating existing conditions of vulnerability that together could potentially disrupt operations and, thus, the services that they provide.

[4] The EPCIP sets out an overall all-hazards framework for critical infrastructure protection and, since 2013, critical infrastructure resilience in the EU. It consists of several pillars, including *inter alia*: the ECI Directive; measures to facilitate Programme implementation (e.g. CIP Points-of-Contact (CIP PoC) group, the Critical Infrastructure Warning and Information Network (CIWIN) platform); accompanying financial measures; and an EPCIP external dimension (Commission Staff Working Document on a new approach to the European Programme for Critical Infrastructure Protection. SWD(2013) 318).

[5] Council Directive 2008/114/EC on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection.

[6] The Directive requires *inter alia* that ECI operators maintain an Operator Security Plan (OSP) and designate a Security Liaison Officer (SLO). Competent authorities are subject to certain reporting requirements and must designate CIP points-of-contact.

Systems Directive[7]) have been adopted (see Annex 6). Besides implementing these and other EU legislation, Member States have continued to refine their own policies, strategies and frameworks, albeit in ways that are often divergent.[8]

Like the legislative landscape, the environment in which competent authorities and critical infrastructure operators act has changed significantly (see Annex 4). The operators face a range of risks, including cyber- and cyber-enabled attacks (addressed by the NIS Directive), natural hazards, hybrid actions, terrorism, insider incidents, epidemics, and certain kinds of accidents (such as industrial accidents). Compared to 2008 when the ECI Directive was adopted, some of these risks have gained in importance in terms of frequency and potential damage they can cause, such as extreme weather events, which are exacerbated by climate change. Other threat are of increasing concern, such as hybrid threats or the risk of insiders' infiltration, and others are unprecedented in scale, such as pandemics. In addition, the integration of technological innovations like 5G and drones has the potential to be exploited by malicious actors. Finally, CIs are increasingly interconnected and reliant upon one another (see box 2 and 3 for examples), and the disruption of an infrastructure in disparate sectors might produce cascading effects and bring disruptions to other infrastructures and sectors, including across borders.

Several proposals have been made in recent years to reform the EU's approach to critical infrastructures. For instance, the 2017 Comprehensive Assessment of EU Security Policy called for the revision of the ECI Directive.[9] In 2018, the European Parliament made a similar call, emphasising the need to achieve better alignment with the NIS Directive.[10] The following year, the Council encouraged the Commission to consult with Member States on a possible revision of the ECI Directive in light of the evolving cross-border and cross-sectoral interdependencies between CIs across Europe and in view of the uninterrupted functioning of the internal market[11]. The same year, the Commission published the findings of its own evaluation of the Directive. The evaluation found that while the Directive was successful in bringing more attention to bear on the topic, the protection- and asset-oriented nature of the Directive's provisions were only partially relevant in the face of various developments since 2008.[12]

In July 2020, the Commission adopted the EU Security Union Strategy, which acknowledged the increasing interconnection and interdependency between physical and

[7] Directive 2016/1148 concerning measures for a high common level of security of network and information systems across the Union (NIS Directive).
[8] Evaluation of Directive 2008/114 (SWD(2019) 308); Study into the potential effects of different possible measures aimed at further enhancing the protection and resilience of critical infrastructure in the EU, 2020 (hereafter referred to as the feasibility study); Good Governance for Critical Infrastructure Resilience (OECD, 2019).
[9] Comprehensive Assessment of EU Security Policy, SWD(2017) 278.
[10] Findings and recommendations of the European Parliament's Special Committee on Terrorism, 2018/2044(INI).
[11] Council Conclusions on complementary efforts to Enhance Resilience and Counter Hybrid Threats, 14972/19.
[12] SWD(2019) 308.

digital infrastructures. It underlined the need for a more coherent and consistent approach between specifically the NIS Directive and the ECI Directive to ensure the reliable provision of essential services.[13] The two instruments are therefore being reviewed in parallel. Nevertheless, given their differences (as shown in the box below), this Impact Assessment focuses on **measures to enhance critical infrastructure resilience in the face of non-cyber risks**, including natural hazards, hybrid actions, terrorism, insider incidents, epidemics, and accidents**.** Where relevant, it explores common elements with the ongoing review of the NIS Directive, including as regards the sectoral scope. The analysis in the report therefore goes beyond transport and energy sectors of the ECI Directive.

Box 1: Interplay between the NIS Directive and the ECI Directive

The NIS and ECI Directives have a similar objective aimed at ensuring the security of key actors in a number of crucial sectors, and have a similar process/logic by which Member States identify and designate those key actors that require particular guidance and oversight. At the same time, they present some differences:

Material scope and threats: while the NIS Directive is focused on the security of network and information systems against cyber threats, the ECI Directive is focused on enhancing the security of physical assets against threats such as terrorism and other intentional and unintentional man-made threats, as well as natural disasters[14].

Geographical impact: the ECI Directive is limited to those infrastructures, the destruction/disruption of which would have a significant **cross-border impact**, while the NIS Directive covers operators without explicitly requiring Member States to determine if negative cross-border effects can be anticipated in the event of a disruption.

Asset vs. services approach: while both critical (physical) infrastructures and network and information systems are by nature crucial to the provision of essential services, the ECI Directive is focused on the protection of specific assets that provide certain essential services. The NIS Directive takes a broader approach that considers essential services as a whole (some of which are provided by infrastructures designated as ECIs).

In the case of a given electricity supplier, for instance, the NIS Directive would focus on the cybersecurity of the communication networks, devices and data related to the service that the operator provides; while the ECI Directive would mainly focus on the security of specific facilities (e.g. a specific power plant, the building, surrounding perimeter, etc.) in the face of risks of non-cyber nature. In practice, this creates a situation in which actors may be designated as both ECIs and operators of essential services under the NIS Directive. This means that the network and information systems that underpin their

[13] Communication on the EU Security Union Strategy, COM(2020) 605.

[14] A possible overlap, however, arises from the fact that under the ECI Directive the ECIs should include measures on security of information systems as part of their Operator Security Plan (Annex 2 of the ECI Directive).

operations are subject to requirements per the NIS Directive. Meanwhile, the ECI Directive sets out certain requirements concerning their physical security.

Sectoral scope: while the ECI Directive is limited to energy and transport, the NIS Directive[15] applies to seven sectors: transport; energy; banking; financial market infrastructure; health; drinking water supply and distribution; and digital infrastructure.

Protection vs. resilience the ECI Directive focuses on physical protective arrangements, while the NIS Directive obligates operators to take risk management measures in relation to network and information systems to ensure the continuity of those services.

2. PROBLEM DEFINITION

2.1 What is the problem?

The findings of the 2019 evaluation of the ECI Directive and the external study to support the development of the impact assessment demonstrate that despite different measures at European and national level aimed at enhancing the resilience of CI operations in Europe, the **critical infrastructure operators are not adequately equipped to address current and future risks that may result in disruptions to the provision of essential services.** This is due to a dynamic threat landscape, deeper interdependencies and a complex operational context.

Specifically, the evaluation of the ECI Directive found that the "**evolving threat picture** involving a combination of natural and (sometimes antagonistic) man-made threats, but also the increasingly intertwined, transboundary and 'wired' nature of Europe's critical infrastructure". The evaluation highlighted that "in many instances, the **interdependencies between CIs** in different sectors are considerable, extend beyond Europe's boundaries, and need to be accounted for in addressing the security of European CI". In this increasingly complex context, **no single CI operator can reasonably be expected to independently manage and address all risks**.

The **need for resilience of critical infrastructures** is demonstrated by previous incidents (illustrated in the box below), but it is especially crucial to prevent new incidents to take place or to minimise their disruptive effect whenever these occur.

Box 2: Potential cross-sectoral/cross-border impacts of disruptions of critical infrastructures[16]

While the impact of potential CI disruptions in Europe cannot be quantified, some examples give **indications of their size and implications,** be they economic, social, or

[15] Annex III of the NIS Directive also includes Online marketplaces, Online search engines and cloud computing services as a category of providers of digital services in scope.
[16] See Annex 4 for more details.

on citizens' daily lives.

Besides cyberattacks (addressed by the NIS Directive), the main threat that CIs face include **natural hazards**, which are increasing due to climate change[17]: the damage to CIs caused by extreme climatic events could multiply by ten, up to EUR 34 billion annually[18] by the end of the century. Examples of this include the 2009 drought in France which led to a scarcity of cooling water for nuclear power stations, or the 2015 flooding in the UK that brought down a data centre of a major telecom operator[19] -the latter being an example that digital infrastructures are also vulnerable to physical threats.

Terrorist attacks, besides the loss of life, can bring critical infrastructures to a halt: after the attack in 2016, the Zaventem airport remained closed for two weeks and its capacity reduced by half in the following month – from two to one million passengers. The estimated costs for reconstructing the infrastructure amounted to 160 million EUR, while the overall impact of the attacks (including the Paris attacks the preceding year) on the economy was estimated at 2.4 billion EUR[20]. The subsequent public enquiry called for improvements as regards emergency response procedures in relation to terrorism[21].

Unintentional **accidents** and **insider threats**[22] from employees can have similar implications. The collapse in 2018 of the Genoa bridge (part of the Trans-European Transport Network) disrupted the transport flows between the port of Genoa and other major cities in Europe and caused damages amounting to 360 million EUR to some 2,000 companies and a loss of economic output in port, industrial and logistics activities of more than 100 million EUR[23]. A sabotage in 2014 caused the shutdown of a Belgian nuclear power facility for six months, making unavailable a large part of the country's electricity production capability and requiring repairs amounting to EUR 138 million[24].

Critical infrastructures are now also facing potential threats associated with **new technologies**, such as drones: the drone that disrupted London's Gatwick airport for

[17] The importance of climate resilience and adaptation to climate change has been underlined in the Communication on European Green Deal (COM (2019) 640) and the proposal for the European Climate Law (COM(2020) 80.

[18] Annual damage to Europe's CIs could increase from the current EUR 3.4 billion to EUR 34 billion by the end of the century (Report on the implementation of EU strategy on adaptation to climate change. COM(2018) 738).

[19] Datacenterdynamics.com, 2016 (link).

[20] Federation of Enterprises in Belgium, 2016 (link).

[21] La Chambre des représentants de Belgique, 2018 (link).

[22] Insiders' infiltration comprises the risk of employees misusing their access rights within an organisation, to harm and cause damage. This risk is exacerbated by the growing phenomenon of radicalisation. Even if there is no official account of how many radicalised individuals are present in the EU and posing a potential security threat, various datasets illustrate the magnitude of the problem: approximately 20,000 individuals have been reported in France; and the German security authorities have reported 11,000 Salafists, with a shift towards a more violence-prone and terrorist spectrum (2018 Report of the High-Level Commission expert group on radicalisation (link).

[23] Ilsole24ore.com, 2019 (link).

[24] The New York Times, 2016 (link).

33 hours in 2018 cost airlines an estimated EUR 55 million. The incident diverted or cancelled approximately 1,000 flights, affecting around 140,000 passengers[25].

Furthermore, due to the increasing interdependencies between CIs, disruptions in a single sector (or in some cases a single facility) can have immediate cascading effects across other sectors and across borders, **multiplying the economic and social impacts** of CI disruptions.

Only recently, the pressure on the health sector due to the COVID-19 **pandemic** resulted in measures across the EU to limit mobility. These measures impacted transport operators, directly affected other sectors such as agriculture (due to the shortage of seasonal workers) and put pressure on the electricity and Internet networks.

A number of other earlier events illustrate how disruptions to critical infrastructures can have a negative impact **across borders**. For instance, in December 2017 the explosion and fire in Austria's main **gas pipeline hub** affected the delivery of supplies to Hungary, Slovenia and Croatia, as well as to their biggest recipient, Italy. This led Italy to declare a state of emergency due to a serious energy supply problem[26]. The Italian wholesale day-ahead price surged 215 % to 75 euros per megawatt-hour, its highest recorded level.

A recent **example outside the EU**, which shows the extent of negative impacts of disruptions, is the explosion of more than 2,750 tonnes of ammonium nitrate unsafely stored at the port of Beirut in August 2020. Besides city-wide damage to housing and infrastructures estimated at between US$3.8 and US$4.6 billion[27], the explosion caused severe impacts on the health system. It also exacerbated food shortages after the main grain silos were destroyed, further undermined the confidence of citizens in the government and worsened the economic crisis.

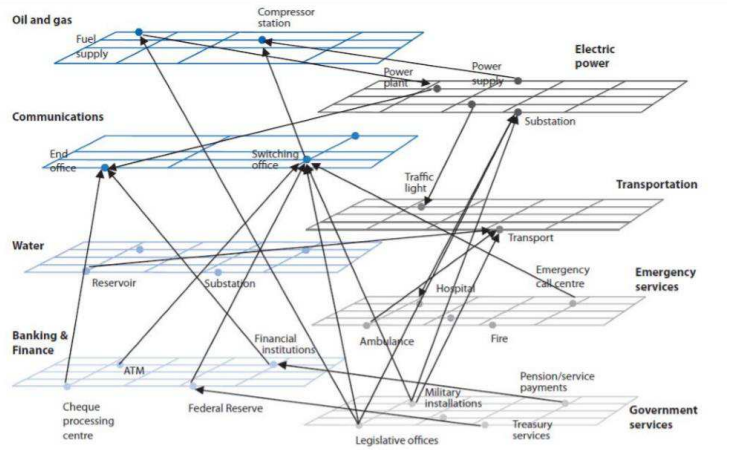
The impacts of disruptions of critical infrastructures will continue to grow due to the ever-increasing **interdependencies**, as shown in the box below.

Box 3: Increasing cross-sectoral/cross-border interdependencies[28]

Critical infrastructures in different Member States are increasingly interconnected and reliant upon one another. The more complex these interdependencies, the greater the risk for so-called cascading (or ripple) effects across sectors and Member States. The

[25] BBC, 2019 (link).
[26] Reuters, 2017 (link).
[27] World Bank, 2020 (link).
[28] See Annex 4 for more details.

illustration below shows the generic **interdependencies** that exist between different sectors, potentially involving actors in different Member States.[29] However, as with any system, the depth of interdependences between and among specific sectors will vary.



As an example, the **energy sector** enables other CIs to function, notably transport, telecommunications, healthcare or finance. The reliable delivery of electricity is also necessary for the water sector (e.g. pumping of water is entirely dependent on electricity), and vice-versa, CIs in the water sector influence the smooth functioning of the electricity sector (cooling water is necessary for the nuclear power plants).

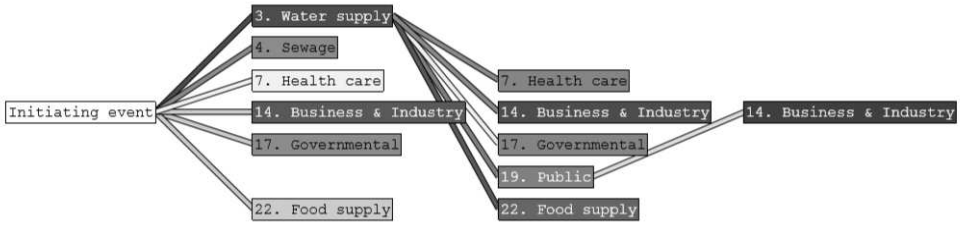
The **telecommunications sector** also has a crucial role, as most CIs (finance, electricity, health systems, transport, etc.) are dependent on communication systems for their daily operations. The aviation sector is heavily dependent on telecommunication services and the constant availability of the global navigation satellite systems like Galileo for air-traffic control and navigation. Some 90% of global data exchanges, including those related to air traffic, use a limited number of undersea cables[30]. The financial services sector is also reliant on telecommunications infrastructure (e.g. electronic payments and Automated Teller Machines), and on the Internet sector, which ultimately depends on the reliability of the electric system.

The examples below illustrate **practical, real-world implications of cross-sectoral interdependencies**.

A **storm** in October 2019 in Estonia caused a **power outage** affecting more than 10% of the country's population and leading to serious disruptions to motor fuel supply, telecommunications, drinking water and hospital operations[31]. Earlier that year, a widespread **telecommunications outage** affecting large parts of Netherlands in June

[29] National Association of Regulatory Utility Commissioners), (2005), Technical Assistance Brief on Critical Infrastructure Protection "Utility and Network Interdependencies: What State Regulators Need to Know", US, available at www.naruc.org/Publications/CIP_Interdependencies_2.pdf in OECD, 2019: 22.
[30] OECD 2019, Good Governance for Critical Infrastructure Resilience, (link).
[31] Eesti Rahvusringhääling, 2019 (link).

2019 crippled emergency services and rendered police and other government services unreachable[32]. Another example shows in a schematic fashion how a **contamination of drinking water** in Sweden in 2011 impacted across many other sectors[33]:



In addition to cross-sectoral effects, the disruptions in the **water sector** can have serious trans-boundary risk effects. This derives from the fact that drinking water supply and distribution networks rely on **water catchment areas and groundwater reservoirs** that are in the majority of cases **cross-border** in nature. Some 60% of river basins cross at least one national border, with Member States such as Belgium belonging to four international river basin districts. In other words, any incident, accidental or malicious, in one Member State that threatens to pollute or limit access to drinking water via these sources could have impacts on the distribution of water in other Member States.

Similarly, disruptions in the **health sector** pose serious cross-border and cross-sectoral risks. The transboundary effects of risks affecting the health sector have been evidenced with the **COVID-19 crisis**: the challenge of the health sector in most Member States to face the pandemic resulted in measures to limit mobility across the EU. This disrupted sectors crucial to the EU's economy such as tourism, impacted the free movement of labour (leading for example to a shortage of seasonal workers in agriculture), and negatively affected European supply chains that are crucial for the free movement of goods.

Looking in more detail at the main problem of critical infrastructure operators not being adequately equipped to address risks in this complex context: its first element relates to the fact that CI operators in many instances **do not factor in all the risks they are confronted with, and do not properly assess the scale of these risks**. This claim is supported by the OECD, which found that "owners and operators cannot address all their vulnerabilities on their own and may not have incentives to assess a complete overview of the full extent of their interdependencies".[34] As an example, a recent study demonstrated that data centre operators do not expect to be impacted by the negative effects of climate change. Some 45% of organizations surveyed acknowledged that they are not adapting to climate change impacts and some 90% did not think they needed a plan to mitigate increased risk of flooding despite being vulnerable to risks of

[32] Euronews, 2019 (link).
[33] Project on 'Modelling of dependencies and cascading effects for emergency management in crisis situations' (link).
[34] OECD, 2019, Good Governance for Critical Infrastructures Resilience (link).

inundation.[35] Similarly, a joint report by the World Health Organisation (WHO) and World Bank found that there is a global "lack of planning and readiness for a rapidly moving, lethal pandemic" with the potential to disrupt global health, social and economic systems.[36]

Secondly, **relevant CI sectors and operators are not uniformly recognised as such in all Member States**.[37] Differing understandings across the EU as to which types of infrastructures should be designated as being national critical infrastructures given their strategic importance in maintaining certain societal functions and thus subject to enhanced levels of protection leads to a situation in which a specific type of asset, e.g. a power substation, might be identified as critical in one Member State and not in another, even though they fulfil the same function, employ the same equipment/systems, and face similar risks. In the absence of some form of official recognition of being critical, CI operators are neither privy to government support aimed at promoting resilient operations, nor provided with indications as to specific risks that they might need to gear their efforts toward.

Thirdly, while risk reduction is a central element of many CI operators' work to ensure continuity of service, many are **confronted with other priorities** that might take precedence over risk mitigation activities, e.g. expanding capacity to stockpile vital supplies/components, carrying out response exercises, regular reviews of resilience plans, etc. This tendency is reflected by NATO, which acknowledges that operators may choose to "eliminate most redundancies [critical in ensuring] continuity of essential services and for use as an emergency backup in times of crises".[38]

In recognition of the fact that many operators' resilience efforts are informed by a market logic, Member States set out general requirements on **mitigation/security measures that CI operators must take**. In many cases, these are depicted in operator security plans or equivalent documents, which tend to **focus on the protection of specific critical assets**.[39] Other resilience elements, e.g. business continuity planning, recovery arrangements, are in many instances insufficiently addressed or missing.[40] The varying types of mitigation/security measures across the EU are of particular concern when pan-

[35] Datacenterknowledge.com, 2018 (link). See also Datacenterdynamics.com, 2016 (link). Survey based on responses of nearly 900 data centre operators and IT practitioners.
[36] A world at risk: Annual report on global preparedness for health emergencies. Global Preparedness Monitoring Board, 2019 (link): 28. Furthermore, the 2020 Study into the potential effects of different possible measures found that only one Member State's CIP policy takes into account pandemics as a potential threat.
[37] OECD, 2019: 46.
[38] NATO, 2020 (link).
[39] The measures detailed in OSPs can be technical (e.g. detection of potentially dangerous materials/individuals, access control) and organisational (early warning/crisis management procedures) in nature. They may also describe control/verification mechanisms; (crisis) communication strategies; and awareness-raising/training activities.
[40] For the purposes of this analysis, a business continuity plan is defined as documented information that guides an organization to respond to a disruption and resume, recover and restore the delivery of products and services consistent with its business continuity objectives.

European services such as Galileo or Eurocontrol depend on infrastructures in different Member States[41].

Finally, competent authorities seek to **incentivise operators** to engage in risk mitigation activities by rendering different forms of support, including access to privileged information (e.g. specific threat information from security services); guidance materials (e.g. handbooks, methodologies); training activities; financial support; voluntary audits/inspections to ensure that their efforts meet existing requirements; and fora aimed at facilitating network-building/cooperation at both national level and between Member States and the EU.[42] However, the extent of these incentives varies from one Member State to another, meaning that **operators do not always have access to the official support** necessary in order to ensure that their operations are resilient.[43]

In conclusion, the assessment depicts a situation in which CI operators today are not fully aware of and/or comprehend the implications of the dynamic risk landscape, and approach risk mitigation in ways that diverge between Member States and sectors. Furthermore, operators are not recognised as being critical by authorities in all Member States, which in turn provide varying degrees of official information and support tools. As a result, CI operators are not always adequately equipped to address current and future risks that may result in disruptions to the provision of essential services. Given the increasingly **interconnected nature** of services and sectors, an insufficient level of resilience on the part of one CI can have implications for other infrastructures and essential services that they provide elsewhere, including in other Member States and/or sectors, representing a risk for the integrity of the EU's internal market which depends on an uninterrupted flow of these services.

This situation, i.e. where systems are only as strong as their weakest links, has potential **consequences** not only for CI operators, but also for **governments, businesses and citizens**. In concrete terms, the citizens would be affected by disruptions as they rely on essential services in their daily lives to travel, work, or benefit from key public services such as hospitals, transport, and energy supplies. Businesses are also likely to be seriously affected, as disruptions of services such as transport or finance can negatively impact their supply chains and lead to business interruptions. As businesses in the EU are highly interconnected (both sectorally and geographically), a disruption of a single infrastructure could affect a number of associated businesses. Some of the disruptions could also have severe consequences for security (for instance following a terrorist attack

[41] The 2020 Study into the potential effects of different possible measures found that competent authorities in one Member State are not always aware of resilience measures being taken in other Member States regarding infrastructures with cross-border elements.

[42] The Study into the potential effects of different possible measures found that 43% of CIP-PoCs thought that cooperation between public and private actors at national level can be improved to a high/very high extent and 33% to a moderate extent. This opinion was supported by the operators during different consultative activities and interviews done as part of the feasibility study.

[43] For example, Member States have indicated that operators increasingly request background checks on certain staff, but that the competent authorities lack the legal basis to do so.

targeting a CI) and lead to uncertainty and undermine confidence in the responsible authorities and providers of essential services.

Box 4: Evaluation of the ECI Directive[44]

The ECI Directive, when adopted in 2008, was meant to address an inadequate level of protection of CIs with a European dimension in the energy and transport sectors. The specific objectives of the Directive were two-fold: to establish a procedure for the identification and designation of ECIs; and to establish a common approach to the assessment of the need to improve the protection of ECIs.

While the Directive generated awareness of and political momentum around the protection of critical infrastructures, the evaluation found that the Directive has been only partially effective in achieving its objectives. This is mainly due to the generality of some of its provisions and definitions that left room for different interpretations by Member States and its limited sectoral scope.

Its provisions regarding the requirement for designated operators to **assess risks**, for Member States to **designate certain infrastructures** as critical, for operators to put in place **security measures** and for Member States and the Commission to **support** them through best practices and methodologies, training and information exchange were already pointing at the existence of the problem/its main elements that are mentioned above and that still persist today.

Indeed, the Directive's narrow scope in terms of sectors, limitation to designated infrastructures with cross border impacts, the focus on protection and the voluntary character of the support measures meant that its impact remained limited. Its 2019 evaluation also found that the evolution of the context in which CIs operate means that the ECI Directive has gradually diminished in relevance. The limitations identified in the evaluation are assessed in the problem drivers' analysis in the next section.

2.2 What are the problem drivers?

This section looks at various drivers that contribute to the main problem of CI operators facing difficulties on the ground when assessing/addressing the risks they face. The drivers relate to the limitations of the existing regulatory framework[45], as part of which the authorities act and guide the operators. These problem drivers have been identified on the basis of the outcomes of the 2019 evaluation of the ECI Directive, as well as the external feasibility study that was carried out to support the development of this impact assessment. EU instruments with CI relevance and national CI policies are accounted for as appropriate.

[44] SWD(2019) 308.
[45] See Annex 6 for more details.

2.2.1 Driver 1: Risk assessment requirements are not comprehensive and do not account for complex interdependencies

One central element of ensuring CI resilience involves assessing the risks that increasingly complex and interdependent networks of CI operators face now and are likely to face in the future. In order to do so, sectoral and cross-sectoral risk assessments need to be carried out. However, as explained below, despite robust risk assessment requirements in some sectors, there are **deficiencies in the risk assessment processes**, which have the effect of rendering CI operators ill-prepared to understand and take action to mitigate the risks that they face.

At EU level, the **ECI Directive** requires Member States to carry out a threat assessment, but only within the two sectors (energy and transport) within scope, and only then in cases of ECI designation. Meanwhile, the designated operators are expected to conduct a risk analysis. However, these requirements are narrow in focus and vaguely defined, and the Directive does not stipulate which specific types of contingencies should be considered in meeting the threat assessment and risk analysis requirements.[46]

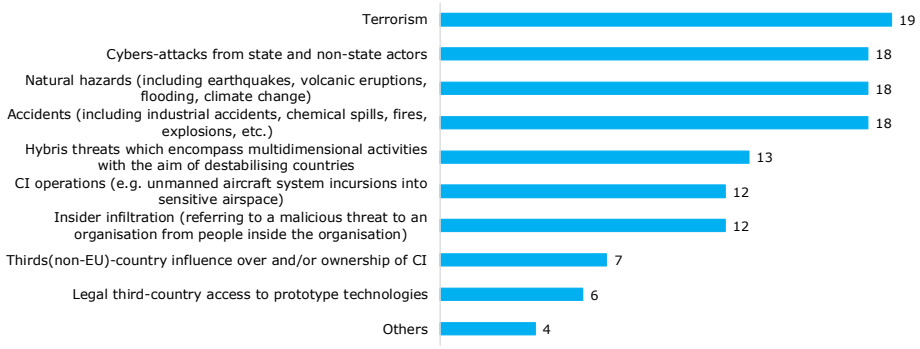
Similarly, while many relevant **sectoral and cross-sectoral EU measures** cover risk assessment practices, they do not address all relevant risks that CI operators face. Indeed, the findings of the recent feasibility study and exchanges with competent authorities suggest that the EU's approach to CI resilience neglects certain contingencies that have grown increasingly likely in recent years. These include: intentional operational disruptions (e.g. using drones); accidents (e.g. industrial accidents, chemical spills, etc.); hybrid actions; cyber incidents[47]; insider threats; and natural disasters.[48] For example, the existing aviation security regulation and current rules on security in the maritime sector focus on malicious security-related threats, but not on accidents or natural hazards.[49] Meanwhile, the Drinking Water Directive only accounts for risks associated with water contamination and industrial incidents.[50] The cross-sectoral NIS Directive stipulates that national network and information security strategies should include a risk assessment plan, and that designated computer security incident response teams (CSIRTs) carry out 'dynamic risk analyses'. The Union Civil Protection Mechanism (UCPM) contains a risk

[46] To the extent that they are referred to, it is in Recital 3 of the Directive, which makes general mention of 'man-made, technological threats and natural disasters' and specific mention of 'the threat of terrorism'.
[47] Covered under the NIS Directive.
[48] The Study into the potential effects of different possible measures found that CIP PoCs view many different risks as being dealt with inadequately (to a 'low or very low' extent): insider infiltration (35% of CIP PoCs); natural hazards (48%); accidents (57%); hybrid threats (45%); and cyberattacks (41%).
[49] Regulation 300/2008 on common rules in the field of civil aviation security; Regulation 2015/1998 laying down detailed measures for the implementation of the common basic standards on aviation security.
[50] Council Directive 98/83/EC of 3 November 1998 on the quality of water intended for human consumption.

assessment requirement, but this is primarily focused on natural and man-made disasters, including outside the EU[51].

The **approach to and scope of national-level risk assessment processes** vary as well, sometimes significantly. While threats such as terrorism, cyberattacks, natural hazards and accidents are accounted for in most Member States, others are considered in only some. These include, for instance, threats associated with new technological advances, insider threats and pandemics.

Figure 1: Threats accounted for in national risk assessments[52]



Furthermore, the risk assessment methodologies employed by Member State authorities are not always designed to allow for **the identification of interdependent relationships between operators in different sectors, including ones in other countries.** Only twelve Member States use a methodology that is geared toward the identification of interdependencies between operators in the same country. Of these, only five recognise the possibility of disruptions in one Member State having 'cascading effects' in another.[53] Studies by other international organisations, including NATO and the OECD, have come to similar conclusions. For instance, a recent OECD report suggests that two-thirds of its members have yet to adopt methodologies capable of assessing interdependencies.[54]

In large part, this situation at national level can be attributed to the nature and focus of the EU's current framework, which does not request Member States to identify and manage cross-sectoral and cross-border interdependencies in a systematic fashion. For instance, many sectoral EU-level measures do not set out requirements for Member States or operators to assess let alone address cross-sectoral interdependencies, except for

[51] The UCPM defines risk assessments as "the overall cross-sectoral process of risk identification, risk analysis, and risk evaluation undertaken at national or appropriate sub-national level". The relevant elements of the risk assessment should be provided to the Commission.
[52] Feasibility study survey of CIP PoCs. Some of the threats addressed in the survey, such as cyberattacks and third-country influence, are beyond the scope of the Impact Assessment.
[53] Study into the potential effects of different possible measures, 2020.
[54] OECD, 2019: 49.

example the Electricity Risk Preparedness Regulation[55]. For its part, the ECI Directive does not account for cross-sectoral interdependencies beyond the energy and transport sectors, this despite the fact that both are heavily reliant on other sectors, e.g. ICT and space.[56]

In conclusion, most EU and national level risk assessment requirements do not adequately account for new and emerging threats and risks. In some cases, they emphasise intentional malicious threats, like terrorism, but neglect the possibility of non-antagonistic contingencies, including natural disasters and accidents. Furthermore, current European and national-level approaches are not well equipped to identify interdependencies between stakeholders at different levels. Taken together, this situation leaves operators in different sectors in Europe without the necessary incentives, tools and/or information by which to understand the risk landscape that they face.

2.2.2 Driver 2: Diverging sectoral coverage and designation criteria

Another factor contributing to a heightened risk for disruptions to the provision of essential services relates to the fact that CI operators and/or sectors lack in some instances official status as such, meaning they are not privy to various forms of official support. This situation stems from diverging sectoral coverage and designation processes.

At **EU level**, there is no single recognised list of CI sectors. Nonetheless, different pieces of EU legislation cover **specific sectors**. For instance, the ECI Directive covers two sectors[57], while the NIS Directive covers seven.[58] The telecommunications and space sectors are covered by still other EU initiatives. Sectoral coverage at **national level**, meanwhile, varies from one Member State to another, though as the figure below demonstrates, the overwhelming majority of national approaches cover a core group of sectors (energy, transport, banking and financial market infrastructure, health, drinking water supply and distribution, digital infrastructure, and telecommunications).[59] In roughly half of the Member States, public administration and wastewater management are considered critical. Other sectors, like election infrastructure, are only covered in two Member States.

[55] Article 5(4) of Regulation (EU) 2019/941 on risk-preparedness in the electricity sector implicitly requires ENTSO-E to consider the risks of disruption of gas supply and risks stemming from malicious attacks (including cyberattacks).

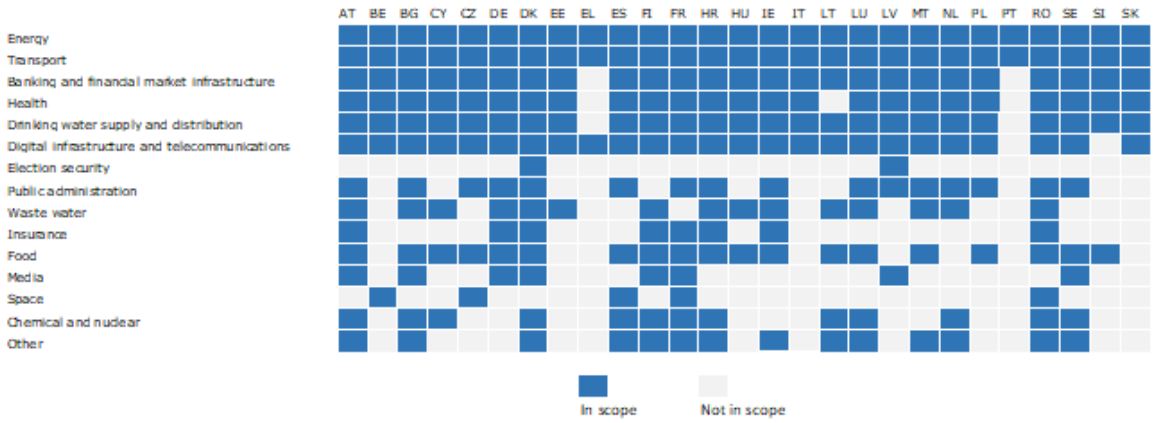
[56] SWD (2019) 308.

[57] The ECI Directive evaluation pointed to the need to review the current scope of the Directive to encompass additional sectors besides energy and transport, and to develop strategies for identifying and addressing those vulnerabilities that result from the interdependencies that exist between them.

[58] The sectors covered by the NIS Directive include transport, energy, banking, financial market infrastructures, health, drinking water supply and distribution, and digital infrastructures.

[59] The sectors mentioned are covered by all national frameworks, with the exception of a small number of Member States.

Figure 2 – Sectors covered by national critical infrastructure approaches[60]



Besides diverging sectoral coverage, there are significant differences concerning the **criteria and procedures used to identify and designate infrastructures** as critical, at both EU and national levels.

The **ECI Directive** has led to the designation of 94 ECIs, two-thirds of which are located in three Member States in Central and Eastern Europe; 16 Member States have not designated any ECI. The disproportionate representation of ECIs in certain Member States/regions can be attributed – at least partly – to the fact that **the Directive leaves Member States with significant discretion** in implementing the legislation, e.g. in setting out the thresholds to be met vis-à-vis the ECI identification/designation criteria.[61] According to feedback from Member States[62], this stems in part from the fact that some of the Directive's key terms and provisions are vaguely defined or ambiguous, but also from specific disparities in national policies/approaches. For instance, Member States employ different CI definitions[63] and criteria by which to assess CI criticality, leading to divergent assessments on the part of authorities as to what objects/services[64] are critical and, thus, worthy of particular support (and scrutiny).

Moreover, there is no obligation for Member States to communicate the ECIs identities to the Commission. This makes for a situation in which it is not possible **to know if specific CIs** (e.g. air traffic control, energy transmission, cargo shipping) **providing obvious essential services on a pan-European basis have been designated as ECIs**, or

[60] Where national measures indicated only "Energy" and/or "Water" without further specifications, the first sector has been understood as comprehensive of energy production, transmission and distribution, while the second as comprehensive of both drinking water supply and distribution and waste water.
[61] SWD(2019) 308.
[62] Feedback to 2019 ECI Directive evaluation and 2020 external feasibility study.
[63] The definitions used by most Member States associate CI with things like 'vital societal functions', 'health', 'safety', 'security', and 'economic or social well-being'(all of which are mentioned in the ECI Directive). Six Member States linked CI with economic stability as well, while another three Member States associate CI with continuity of government and/or the continued existence of the nation.
[64] While most of the Member States consider systems, services and assets as critical, others consider processes or services in their definitions of criticality.

to assess the extent to which the requirements set out in the Directive have been applied. Furthermore, it is impossible to know if different ground-based components that make up or support individual pan-European CIs (e.g. Galileo, Eurocontrol) are subject to similar security requirements in different host Member States where they are located.

Unlike the ECI Directive, which exhibits an asset- and protection-centric approach, the **NIS Directive** takes an output-oriented approach, requiring that Member States **identify operators of essential services** (OESs) based on the criticality of the services they provide, as well as more objective criteria (e.g. number of users, market share). With the exception of the Systemically Important Payments Systems Regulation,[65] no other **EU-level sectoral legislation** establishes a formal process for designating operators on the basis of their criticality.

The differences in the identification criteria and procedures of the NIS and ECI Directives result in mixed signals to competent authorities seeking to identify critical operators. This has, for instance, been recognised by several electricity operators, which have called for the distribution system operators to be considered critical per the ECI Directive[66].

Divergences in sectoral coverage and national designation approaches create uncertainty for operators as to whether their infrastructure will be considered critical or not in different Member States. Ultimately, this results in different resilience levels for similar types of infrastructure around the EU, thereby creating weaker links in those systems of operators in different critical sectors in the EU that are interdependent.

2.2.3 Driver 3: Critical Infrastructure resilience policies and approaches are divergent at different levels and between sectors

The third problem driver is that different actors and initiatives at different levels employ **divergent risk mitigation approaches**, which contribute to CI vulnerability in the EU.

The first area of divergence concerns the **extent to which the full scope of resilience activities is considered**. Historically, the focus of efforts in this policy area has been on CI *protection*, i.e. ensuring that infrastructures are shielded from threats. However, recent years have seen a shift in thinking on the part of scholars, practitioners and policymakers towards approaches that acknowledge that CIs cannot realistically be fully protected all the time against all contingencies, including low probability-high impact events. Instead,

[65] Regulation of the European Central Bank (EU) No 795/2014 of 3 July 2014 on oversight requirements for systemically important payment systems (ECB/2014/28).

[66] Feedback to the Inception Impact Assessment related to the Critical Infrastructure proposal and meeting of the Thematic Network on Critical Energy Infrastructure Protection, 26 June 2020.

the thinking is that CIs must be *resilient*, i.e. able to swiftly 'bounce back' to acceptable performance levels within an agreed-upon amount of time.[67]

Despite this shift in thinking, the notion of resilience is **not yet fully incorporated in EU and national frameworks**. While the need for resilience was reflected in the revised EPCIP approach set out in 2013,[68] the non-binding nature of subsequent actions that were taken as part of the Programme meant that it had only a limited impact in Member States. Meanwhile, the **ECI Directive** emphasises measures (e.g. an Operator Security Plan, a Security Liaison Officer, etc.) to protect specific infrastructures. This is also true for specific **EU-level sectoral initiatives**[69], many of which tend to only focus on certain resilience elements in relation to specific assets, e.g. protective measures and incident management, but not others, e.g. business continuity and recovery arrangements. Some notable exceptions include the Electricity Risk Preparedness Regulation[70] and relevant provisions of the single rulebook governing the EU's financial sector.[71] Meanwhile, the cross-sectoral NIS Directive addresses the full scope of resilience activities (protection and business continuity measures) as regards cyber risks and threats in a horizontal way.

Regardless of which elements of resilience they focus on, the various EU-level sectoral measures impose **different types of more or less rigid obligations** on Member States. While these provisions arguably reflect the specific needs of the sectors in question, they also lead to the creation of an uneven level of resilience across sectors. As an example, requirements in the aviation and maritime sectors entail very detailed protection measures, but do not address business continuity or recovery.[72] Similarly, EU-level telecommunications legislation puts in place general risk management and incident reporting requirements, but none relating to business continuity or recovery.[73] Other sectors, e.g. rail, oil, health, have very limited frameworks, focusing on information exchange, minimum stocks and cooperation among authorities, respectively. Issues related to insider threats, including personnel access to sensitive areas of CI operations (background checks), are only addressed in a few instances, e.g. EU aviation security legislation and, to a lesser extent, in the Port Security Directive.[74] Moreover, even in

[67] According to a recent OECD report, "the considerable degree of uncertainty about the intensity and the complexity of future disasters and their potential impacts on infrastructure" calls for resilience-based "approaches that prepare assets and systems with capacities to be restored and rehabilitated swiftly" (OECD, 2019: 36).

[68] Commission Staff Working Document on a new approach to the European Programme for Critical Infrastructure Protection - Making European Critical Infrastructures more secure. SWD (2013) 318.

[69] See Annex 6 for details.

[70] Regulation (EU) 2019/941 on risk-preparedness in the electricity sector.

[71] Directive 2015/2366 on payment services in the internal market; Directive 2015/2366 on payment services in the internal market; Directive 2014/65 on markets in financial instruments; Directive 2013/36 on access to the activity of credit institutions and the prudential supervision of credit institutions and investment firms; Regulation 575/2013 on prudential requirements for credit institutions and investment firms.

[72] For instance, Regulation 300/2008 lays down common rules on screening of passengers and luggage, airport and aircraft security, security controls, staff, security equipment performance and establishes a mechanism for inspections of airports, operators and entities by the Commission.

[73] Directive (EU) 2018/1972 of 11 December 2018 establishing the European Electronic Communications Code.

[74] Commission Implementing Regulation (EU) 2019/103 amending Implementing Regulation (EU) 2015/1998 as regards clarification, harmonisation and simplification as well as strengthening of certain specific aviation security

sectors where regulatory arrangements are more extensive, e.g. financial markets, there is a general lack of mechanisms geared toward providing authorities with competencies to provide support to CI operators in addressing physical threats specifically.

Meanwhile, recent studies have shown that **national CI resilience frameworks** tend to focus mostly on incident prevention and protection, and much less on incident management, business continuity, etc. Half of the Member States' CIP Points-of-Contact see a need to enhance national-level incident preparedness and consequence management capacities, for instance by setting out consequence management processes incorporating business continuity.[75] Doing so would arguably ensure a more common public-private understanding, e.g. regarding roles and responsibilities in risk mitigation.

Member States have pursued the implementation of EU legislation, including the ECI Directive and NIS Directive, in divergent ways that create potential burden for operators active in more than one Member State.[76] As an example, in addition to specific national requirements, designated ECI operators encounter divergent requirements in different Member States in meeting the obligations contained in the ECI Directive.[77] Operators may also experience potential contradictions in the respective reporting regimes set out in different pieces of EU legislation.[78]

Taken together, divergences in the approaches and requirements set out in different EU-level measures make for a complex operational environment, with operators in different sectors subject to different obligations, largely protection-oriented. The absence of clear provisions on the full spectrum of resilience at EU and, in some cases, national level makes for a situation in which operators are not incentivized by authorities to take resilience-enhancing measures, e.g. developing suitable business continuity plans.

2.2.4 Driver 4: Uneven capacities and limited exchange of information

The problem description argued that CI operators lack key means by which to detect and respond to different risks now and in the future. This situation derives from the complex regulatory framework that they are subject to, and from the fact that many operators receive limited information and support from competent authorities.

---

measures. Directive 2005/65/EC on enhancing port security. Background checks are processes to establish a person's identity; collect the person's criminal records in previous years; identify employment, education and any gaps in previous years; and may include intelligence and any other relevant information available to the competent national authorities that they consider may be relevant to the suitability of a person to work in a function.

[75] 47% of CIP PoCs according to the 2020 Study into the potential effects of different possible measures.

[76] COM(2019) 546.

[77] SWD(2019) 308: 13-14.

[78] As an example, the EU's financial single rulebook establishes oversight and reporting of financial institutions to the supervisors in their home country. However, this may be in contradiction to national CIP policies requiring that operators report incidents to competent authorities in the Member State where the infrastructure is located, and especially in cases where authorities impose confidentiality clauses on the reporting of incidents.

CI operators rely on the **availability of accurate, timely information** in order to make decisions, including ones related to risk mitigation. Without information from, for instance, security services or other operators to suggest an operator's risk exposure, it is impossible to know which mitigation measures should be taken. The recent feasibility study found that there is scope to improve information exchange and cooperation among relevant stakeholders at EU, national and operator level, in part by improving the effectiveness of existing communication channels, e.g. CIWIN, but especially **cross-border cooperation between private and public stakeholders** (e.g. a competent authority in one Member State and a private operator with headquarters in another).[79]

At national level, the depth of cooperation and information-exchange is affected by multiple factors. First of all, **resource levels** vary between authorities in different Member States, ranging from in some cases small handfuls of staff spread across multiple authorities to, in one case, a dedicated agency. Where resources are lacking, authorities may not have **an overview/oversight over relevant actions** being taken by other authorities and operators, not to mention insight into incidents. Indeed, many CIP PoCs see the need for increased monitoring and evaluation capacities at national level.[80]

Secondly, not all Member States have developed **platforms or initiatives aimed at fostering cooperation and information-exchange** between public and private actors, including ones located in other countries.[81] Even where such mechanisms exist, the scope of work and level of ambition varies. Examples include regular meetings between operators and authorities, public-private partnerships, and dedicated public-private coordination bodies.[82] However, no matter how well developed such arrangements are, cooperation is in many cases still hampered by **a lack of secure channels** (e.g. encrypted telecommunications, etc.) to exchange sensitive information, as well as by the fact that key stakeholders at the operator level sometimes lack security clearances, thus precluding security services from sharing sensitive information, e.g. on specific threats.[83]

Box 5: Critical infrastructures - an internal market perspective

As shown in boxes 2 and 3, the critical infrastructures operating in the sectors analysed in this Impact Assessment are crucial for the functioning of many other sectors of the economy, and disruptions in one such infrastructure can have significant impacts in other sectors and across borders. Besides their crucial role in underpinning the economic

[79] According to the 2020 Study into the potential effects of different possible measures, 43% of CIP-PoCs believe to a 'high/very high extent' that cooperation between public and private actors in their countries can be improved, and 33% to a 'moderate extent'. This opinion was supported by the operators during different consultative activities and interviews done as part of the feasibility study.

[80] The 2020 Study into the potential effects of different possible measures found that 34% of CIP PoCs indicated to a 'high/very high extent' that monitoring and evaluation should be improved. 43% believed this to a 'moderate extent'.

[81] OECD, 2019: 56.

[82] Study into the potential effects of different possible measures, 2020.

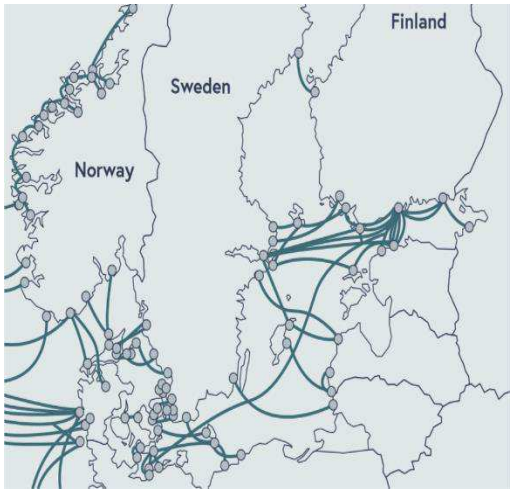
[83] OECD, 2019.

activities that compose the Internal Market and the cross-border nature of disruptions, the infrastructures that are the backbone of a number of essential services are by their nature cross-border as well.

This is the case for the European electricity grid, with one third of the EU's Member States exporting/importing more than 10% of their national generation/consumption of electricity and interconnection levels reaching up to 40% of power generation capacities in countries such as Denmark and Austria. Similarly, the European gas and oil networks span over hundreds or thousands of kilometres across all Member States in order to transport the gas and oil from the North Sea, Russia and other third countries to the consumption centres. For instance, the Druzhba pipeline carries oil from Russia directly to five Member States and branches out into numerous pipelines to deliver oil throughout Eastern Europe[84].

Transport is another clear example of an interconnected network where critical operators play an essential role in the free movement of goods and people. The Port of Rotterdam, the largest port in Europe, is the entry/exit point of 470 million metric tons of goods to and from the EU annually, reaching more than 150 European terminals through inland waterway and rail networks[85]. Air transport is also crucial for business activities and tourism: more than 500 million passengers flew between Member States in 2018, almost half of the total number of passengers travelling by air in the EU.

Telecommunications and digital services are other areas where infrastructures are to a large extent cross-border: the submarine optic fibre links the Nordic countries with major data hubs in continental Europe, channelling data and phone calls from these countries to the rest of the world86. Similarly, many digital services rely on a globally or Europe-wide scattered infrastructure: the backbone of Google services to the whole of the EU are the data centres located in Ireland, Netherlands, Finland and Belgium[87].



Optic fibre submarine cables, Source: Telegeography (2020)

[84] EP DG for Internal Policies, Gas and Oil Pipelines in Europe Briefing Note
[85] https://www.portofrotterdam.com
[86] Critical Nordic Flows Report: Collaboration between Finland, Norway and Sweden on Security of Supply and Critical Infrastructure Protection 2020
[87] https://www.copenhageneconomics.com/dyn/resources/Publication/publicationPDF/6/426/1519987830/copenhagen-economics-2018-european-data-centres.pdf

In addition to the cross-border nature of the infrastructures in the sectors considered, many of the entities operating in the sectors considered in this Impact Assessment provide services across the Internal Market. For example, the gas transmission operator Fluxis operates more than 8,000 km of pipelines across six Member States and two third countries[88], while in the water sector companies like the Suez Group provide drinking water services across several Member States including France, Spain, Italy, Czech Republic, Slovenia and Croatia[89]. Euronext, the largest stock exchange in Europe, operates markets in Amsterdam, Brussels, Dublin, Lisbon and Paris, as well as London and Oslo[90.] The global navigation services provided by Galileo through infrastructures across several Member States is available and used by cars, mobile phones, trains, ships and aircraft across the EU.

The fact that in many cases the potential operators of critical infrastructures are multinational companies adds up to the problems identified in section 2. **Companies operating in more than one Member State** will be subject to diverging obligations and thus suffer an **additional administrative burden** when operating infrastructures across borders, e.g. different certification requirements, duplication of reporting obligations, etc. The difficulties for multinational companies facing different requirements in each Member State has been pointed out by competent authorities and businesses alike as part of the consultation conducted to carry out the 2020 feasibility study. The additional effort required to ensure compliance with different national frameworks is an obstacle for companies to operate in other Member States.

Furthermore, the differences in terms of designation, requirements, support and oversight can also create distortions in the Internal Market since it creates an **uneven level playing field** among business depending on the Member State where they operate.

The absence of common criteria and processes for designating critical infrastructures implies that the same type of infrastructure may be designated as critical in one Member State but not in another. This creates a competitive disadvantage for companies from Member States with a broader sectoral scope and a more ambitious designation approach. These companies are subject to national requirements that their counterparts in other Member States do not have to comply with.

The differences in requirements and oversight on critical infrastructures also results in distortions to competition. The majority of Member States (18) have some form of national legislation related to critical infrastructure resilience. Others approach this matter through non-legislative means. Generally speaking, these approaches can be categorised into three categories: stringent, hybrid, and soft.

[88] https://www.fluxys.com/en/company/fluxys-group/about-fluxys
[89] https://www.suez.com/-/media/suez-global/files/publication-docs/pdf-francais/finance/suez-deu-2019-fr.pdf
[90] Euronext

Critical infrastructure in Member States that impose **stringent obligations** on operators are subject to specific risk assessment, risk management and reporting obligations, including the development of plans subject to official scrutiny by competent authorities at regular intervals. Critical infrastructure operators in those Member States may be obliged to carry out additional security investments if authorities consider it necessary. The critical infrastructure policies in those Member States that apply **hybrid approaches** involve a combination of limited obligations on operators and voluntary measures. In some cases these limited obligations are not subject to a sanctioning regime and thus not enforceable, its compliance based on the willingness of operators to cooperate. Those Member States promote the resilience of critical entities through dialogue mechanisms such as public-private partnerships where authorities and operators work together on a voluntary basis to identify risks and promote the adoption of resilience measures. Finally, the Member States having taken a **soft approach** to the resilience of critical infrastructures rely on operators voluntarily self-identifying themselves as being critical, a self-assessment of risks by those operators, and voluntary cooperation through public-private networks.

While these differences reflect the policy choices of different Member States as to how to approach critical infrastructure policies, this results in a competitive disadvantage for similar entities depending on the Member States where they operate. For example, designated operators in those Member States where authorities systematically review their security plans have a higher administrative burden than in those where this is not the case, and may be required to carry out additional investments. The divergences in national frameworks also create a disadvantage in relation to the support that critical operators receive, as pointed out by stakeholders from the electricity distribution or air traffic control in different Member States, which have called for their recognition as critical infrastructure operators in order to obtain such support[91].

In conclusion, in addition to the uneven level of resilience of critical infrastructures in different Member States that may result in disruptions to the provision of essential services across the EU, such disparities between national rules cause substantial distortions of competition within the Internal Market. This problem is likely to increase in the coming years given that some Member States (IT, BE) have indicated their intention to review their national CI frameworks. Without a minimum level of harmonisation, the current national divergences and resulting obstacles to the Internal Market are foreseen to continue and even increase in the future.

2.2.5 How will the problem evolve?

The problem drivers above show the extent to which the context in which CIs are operated has changed significantly since the ECI Directive was adopted. The outlook for

[91] Feedback to the Inception Impact Assessment and bilateral discussions with operators.

all of these drivers indicates that the problem set will become more acute in the future. Indeed, the already challenging **threat picture of today** is likely to worsen.

Climate change and more frequent **extreme weather events** are also likely to continue and worsen, even in best-case scenarios where drastic remedial action is taken. Critical infrastructures will likely struggle to withstand at least some of these events, especially where they are aging and/or subject to insufficient maintenance. The outlook for the **global security environment** is also negative.[92] The risk that **hostile actors**, both nation state and terrorist, would seek to impede CI operations in the EU seems likely to increase, either as a means to affect decision-making or to cause actual harm.[93]

The EU has already responded to the impact of the **evolving geopolitical context** on CIs with a mechanism to assess the desirability of critical processes being controlled by or vulnerable to influence by **third countries**.[94] This will affect decision-making on the ownership of critical service operators and the relationships they have with other entities. Equally, there is growing concern about the sourcing and vulnerability of CI components, a trend that suggests that **supply chain security** will receive additional attention.

Meanwhile, **technology** will continue to evolve and become more complex. This will be driven by industry needs to increase efficiency, reduce environmental impact, and lower costs in the wake of the economic slowdown precipitated by the Coronavirus pandemic. Within individual entities and infrastructures, the trend towards increased digitalisation appears likely to continue, meaning that operational and information technologies will become increasingly intertwined. This will include the integration of emerging technologies like **5G infrastructure**[95] into critical networks. The 5G (which relies on physical infrastructures) will become the backbone of many IT applications, including in critical sectors such as energy, transport, banking, and health, as well as industrial control systems that contain sensitive information and support safety systems. As many critical services will depend on 5G, ensuring the security of these networks is a strategic goal[96].

Furthermore, the transition to a more **green economy** will deliver fundamental change to the nature of CI systems. In the energy sector, for instance, the transition will lead to more complex networks, but also the potential for new vulnerabilities.

Finally, in response to current and future challenges, the **regulatory and legislative environment** will continue to evolve both at sectoral level and through overarching

[92] Global Trends to 2030 – Challenges and Choices for Europe. EUISS, 2019 (link). 2020 Strategic Foresight Report: Charting the Course Towards a More Resilient Europe. European Commission, 2020 (link).
[93] Joint Communication to the European Parliament and the Council on the Joint Framework on countering hybrid threats: A European Union response. JOIN/2016/018.
[94] Regulation (EU) 2019/452 establishing a framework for the screening of foreign direct investments into the Union.
[95] The process put in place by the Commission's 2019 Recommendation on the Cybersecurity of 5G networks has led to Member State action on the measures set out in a 5G toolbox, as reflected in the report on the implementation of the Toolbox adopted in July 2020.
[96] COM(2019) 552.

thematic policy responses.[97] Member States will likely update their national legislation and, absent an EU framework, this would occur in an uncoordinated and uneven manner, leading to greater fragmentation and a more uneven playing field.

3. WHY SHOULD THE EU ACT?

3.1 Legal basis

Where EU action is legislative in nature, the choice of legal basis must rest on objective factors amenable to judicial review, and in particular the proposal's primary objective and scope. Given the problem that is addressed here and the solutions proposed, Article 114 TFEU is the most appropriate legal basis for an EU intervention.

The ECI Directive relies on Article 308 of the Treaty establishing the European Community as its legal basis. This provision has since been replaced by Article 352 TFEU, which can only be the legal basis for an initiative if the Treaties have not provided the necessary powers otherwise.

In order to use this legal basis, other legal bases would therefore have to be excluded first. In the field of critical infrastructure resilience, the legal basis could be found either in Article 114 TFEU (approximation of laws for the improvement of the internal market) or in Article 196 TFEU (civil protection).

Article 196 TFEU only allows the legislator to take action with regard to the activities of civil protection authorities aimed at the prevention and protection against disasters. While there is certainly a link between civil protection and the resilience of operators of critical infrastructure, the focus of the two policy areas is different. On the one hand, civil protection deals with prevention, preparedness and response to disasters affecting primarily people but also the environment and property at large. While the service provision by operators of critical infrastructure themselves can be impacted by a disaster that requires a response by civil protection authorities, the resilience policy in this regard can and should cover additional types of incidents and areas where civil protection authorities have only a limited role.

On the other hand, policy on the resilience of operators of critical infrastructure and the essential services thus provided encompasses the range of actions required by authorities and operators to ensure that the operators are able to resist, absorb, accommodate to and recover from incidents that have the potential to result in significant functional disruptions. In meeting these aims, different public authorities (sometimes the same as for civil protections, but in other cases including the representatives of ministries of interior or sectoral ministries) provide support to and cooperate with operators. For this

[97] The Commission announced in the EU Security Union Strategy (COM(2020) 605) *inter alia* initiatives on the operational resilience in the financial sector and the protection and cybersecurity of critical energy infrastructures.

reason, Article 196 TFEU would not be suited to impose obligations on operators, which are ultimately the actors responsible for implementing resilience-enhancing measures.

Furthermore, the overall aim of said policy is to secure the continuous supply of services essential to the wellbeing of the EU citizens and the EU economy, and to improve the functioning of the internal market and the stability of the provision of vital societal functions and economic activities. The disparities resulting from uneven situations across the Member States in terms of resilience obligations constitute a barrier to the internal market and justify EU action.

In the sectors considered in this Impact Assessment, critical operators perform their activities within networks spanning across several Member States. Many of the operators of critical infrastructures have assets and deliver essential services across the internal market. The different regimes in each Member State and the variety of requirements applicable across the EU are raising challenges for operators that conduct business throughout the EU, which have to comply with different requirements depending on the Member State. Furthermore, differences in national frameworks also create situations of unfair advantage and distorted competition between operators active in Member States with more comprehensive rules and those that perform their activities under more limited and lenient legal frameworks. Given that the rules differ or are not applied in the same way across the EU, and in view of the aforementioned interdependencies and actual and potential cross-border economic activities of relevant operators, there is not a sufficient level playing field for those operators.

Given the crucial role that the operators play for the functioning of the internal market, Article 114 TFEU would be the most appropriate legal basis.

Moreover, the EU legislator has already used Article 114 TFEU in the context of the NIS Directive, which harmonises rules related to measures aimed at achieving a high common level of security of network and information systems within the Union and the provision of related essential services so as to improve the functioning of the internal market. The current NIS Directive and the options explored in this Impact Assessment have common objectives and have a similar scope, the main difference being in relation to the threats and the objects to be protected. While the NIS Directive addresses the security of the network and information systems (software and hardware) of the operators of essential services against cyber-threats, the options presented in section 5 aim at ensuring the resilience of those operators against all other threats that can affect their physical infrastructure, processes and personnel. Given the similarities in objectives and scope, it is appropriate to apply the same legal basis used in the NIS Directive.

3.2 Subsidiarity: Necessity of EU action

According to the principle of subsidiarity laid down in Article 5(3) of the Treaty on European Union, action at EU level should be taken only when the aims envisaged

cannot be achieved sufficiently by Member States alone and can therefore, by reason of the scale or effects of the proposed action, be better achieved by the EU.

EU intervention in the area of resilience of operators of CIs is justified from a subsidiarity perspective due to the cross-border nature of the services provided by those operators and the internal market objective pursued, as well as the connections between nodes within a network of infrastructures in a given sector and the dependencies of CIs from other essential services.

On the one hand, many CIs located in one Member State, such as data centres or ground infrastructures for satellite navigation, provide services in several other Member States or across the EU. Therefore, the disruption of one single facility could have an impact on users and activities across borders. On the other hand, given that CI networks are composed of mutually dependent hubs, the failure of one infrastructure could disrupt the normal functioning of others within the same sector. For instance, the interruption of operations at one airport or control centre could affect air traffic across Europe and beyond.

Moreover, given the increasingly dense linkages between sectors, cascading effects originating from a single disruption are likely to have cross-border consequences, e.g. where a power outage in one Member State disrupts hospital operations in another. The recent feasibility study shows that many Member State and industry stakeholders see the need for a more common and coordinated approach in this area in view of the evolving interdependencies between service provision using CIs in different sectors. At the same time, some of the most severe incidents affecting operators of certain CIs, such as accidents in nuclear or chemical facilities, could have a cross-border impact well beyond their users and affect negatively, for instance, the environment or citizens' health in more than one Member State.

The options explored in this Impact Assessment strike a balance between the need to ensure a harmonised approach and reinforce resilience of critical infrastructures on the one hand and subsidiarity considerations on the other hand. Therefore, a framework has been devised containing certain minimum standards and requirements leaving a margin of appreciation to Member States and operators concerned. The framework will structure and harmonise the activities of authorities in identifying the services and operators that are to be considered as essential respectively critical, whilst leaving a degree of flexibility to take account of national specificities, including in terms of risks. It will also provide a framework for operators to take the necessary and most adequate measures to address the risks they face, without being overly prescriptive.

3.3 Subsidiarity: Added value of EU action

An intervention at the level of the EU in this policy area is justified due to the common nature of risks that operators of CIs in the EU face and the transnational character of essential services that risk being affected in case of disruption and that could not effectively be dealt with by national action alone. It would also contribute to a more level

playing field in the internal market. Regardless of where in the EU they are located, electricity production facilities, transport hubs or telecommunications networks all face risks that are similar in their essential characteristics. A coherent approach to manage and address these risks that brings together knowledge and expertise from across the EU would optimise the response of operators and authorities everywhere in the EU.

Furthermore, as noted above, the provision of essential services depends on an increasingly interlinked network of assets and systems operating across different Member States. However, a network is only as strong as its weakest link. In other words, vulnerabilities in one Member State have the potential to affect negatively services provided by even the most resilient operators of CIs elsewhere in the EU. Common EU action is necessary to ensure that operators can provide their services without undue restrictions and take appropriate measures to ensure that their operations are resilient in the face of disruptions, thereby harmonising and, for some, raising the proverbial bar.

Finally, an EU intervention would prompt closer alignment of the policies on the resilience of operators of CIs between Member States, which would serve to ensure that operators receive a minimum level of guidance, support and information and are subject to common obligations aimed at enhancing resilience. This, in turn, would contribute to a more level playing field in the internal market and facilitate operators' cross-border activities.

Therefore, comprehensive action at EU level would produce greater benefits compared to action taken solely at the Member State level; the challenge is simply far too large for countries to handle in isolation.

4. OBJECTIVES: WHAT IS TO BE ACHIEVED?

4.1 General objective

The general objective of the initiative is to ensure the continuous provision of essential services in the internal market by enhancing the resilience of critical infrastructure operators in the Member States.

4.2 Specific objectives

Each specific objective (SO) corresponds to one of the problem drivers:

- SO 1: Ensure higher level of understanding of risks and interdependencies, as well as the means to address them;
- SO 2: Ensure that all relevant entities in all key sectors are identified as critical by Member States authorities;
- SO 3: Ensure that the full spectrum of resilience activities is included in public policies and operational practice;

- SO 4: Strengthen capacities and improve cooperation and communication between stakeholders.

As this is a REFIT initiative, simplification potential for companies and public authorities is explored as part of each objective, and in the policy options described below.

5. WHAT ARE THE AVAILABLE POLICY OPTIONS?

5.1 What is the baseline from which options are assessed?

The baseline scenario entails no change over the current situation, i.e. the existing EU framework for CI resilience would remain in place without significant changes.

Here, the existing provisions contained in the **ECI Directive** would continue to apply to cross-border infrastructures in the transport and energy sectors designated as ECIs. However, the application of the Directive would continue to diverge considerably from one Member State to another due to, among other things, the vague articulation of key provisions. As a result, Member States would continue to pursue **heterogeneous approaches to the ECI identification/designation process**, and thus a comparatively small number of Member States would continue to host the vast majority of ECIs. It is conceivable that the total number of ECIs would continue to increase slowly on a year-on-year basis in keeping with the trend in recent years (no reported designations in 2017, +3 in 2018, +1 in 2019). In every instance, ECI operators would continue to be expected to meet a narrow set of obligations focused on asset protection.

In terms of other **relevant legislation at EU level**, the baseline scenario anticipates the revision of the NIS Directive and the adoption of the Digital Operational Resilience Act (DORA),[98] changes which are likely to enhance further the resilience of network and information systems, in particular in the financial sector given the detailed requirements contained in the latter. Besides these initiatives, no other significant changes over the status quo would be made at EU level.[99]

Meanwhile, the proposed Disaster Resilience Goals as part of a revised Union Civil Protection Mechanism (UCPM)[100] could have an indirect impact on the current state-of-play as regards CI resilience, but especially in Member States where this policy area is managed by civil protection authorities.

---

[98] COM(2020) 959. Proposal for a Regulation of the European Parliament and the Council on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014 and (EU) No 909/2014. The Act would contribute to an improved ICT risk management by financial entities, increase supervisors' awareness of cyber risks and incidents, and mitigate risks stemming from financial entities' dependence on third-party ICT service providers.

[99] The exception is an upcoming initiative to enhance the resilience of the European energy system, which would *inter alia* address issues related to the financing of specific security measures by energy operators.

[100] Disaster Resilience Goals are defined in the Commission's Proposal for a Decision of the European Parliament and of the Council amending Decision No 1313/2013/EU on a Union Civil Protection Mechanism (COM(2020) 220). Negotiations on the proposal are ongoing.

At national level, the baseline scenario assumes that **divergences in national CI resilience frameworks** would persist, meaning there would be continued differences between Member States regarding sectoral coverage, support arrangements, and designation criteria. As a result, many CI operators would not be designated as critical at national level, and thus would not benefit from access to specific forms of information and support necessary to address adequately their risk exposure. Meanwhile, operators designated as critical would continue to be subject to diverging national requirements across Europe. It could be envisaged that at least some Member States would seek to put more emphasis on CI resilience and the provision of essential services at national level, given the persisting attention to these issues in different fora, including other international organisations, including NATO, which has set out seven baseline requirements for the purpose of boosting resilience through civil preparedness.

But overall, **the capacity of operators to address risk would remain largely unchanged**, meaning that there will be no significant improvements to the resilience of CI operators. This is even when assuming continued engagement in various network and capacity building fora, including the European Reference Network for Critical Infrastructure Protection (ERNCIP)[101] and other EU-funded networks/projects.

While their risk management capacity might remain largely unchanged, **operators' risk exposure would increase**, given a shifting threat landscape, technological advances, increasingly complex networks and deeper interdependencies. In such an environment, operators would continue to struggle to adequately assess their actual risk exposure and then take timely and appropriate measures in response.

In conclusion, the baseline scenario is unlikely to create conditions that lead to any significant further enhancements to the CI resilience in the years to come.

5.2 Description of the policy options

5.2.1 Policy Option 1: Non-legislative measures at EU level to encourage more common approaches and information-sharing

This option envisages the retention of the existing ECI Directive, accompanied by a set of voluntary measures within the context of the existing EPCIP programme.

First of all, the Commission would produce regular **threat updates/reports** (both general and tailored to specific risks or sectors) based on inputs from the Joint Research Centre (JRC) and Member States. These would be available to authorities (and operators depending on the information's sensitivity), and would support their risk assessments.

[101] https://erncip-project.jrc.ec.europa.eu/

These reports could be developed through a **structured dialogue**[102] between **Member States and the Commission** that would complement existing forms of exchange, e.g. CIP PoC meetings or sectoral fora and committees. Where appropriate, these might involve **subject-matter experts and operators**, and could address different topics, including: methodologies to assess risks and interdependencies; identification of critical sectors and assets; security (physical/personnel) measures, including specific/state-of-the-art solutions; business continuity management policies and practice; incident reporting criteria and methodology; and the facilitation of public-private cooperation.

Through the structured dialogue, Member States and operators would be able to share knowledge, facilitating **more common approaches** in national policies and practice regarding the **assessment of risks and interdependencies, and the definition of critical sectors and focus on resilience**. On the basis of these exchanges, the Commission would develop guidelines to support the work of authorities and operators.

Furthermore, the Commission would work to improve the functionality of its CIWIN platform, which enables **communication and information-sharing** both between the Commission and Member States, and between stakeholders at national level, including operators. Using CIWIN and the structured dialogue, the Commission would also provide a better overview of relevant activities, including EU-funded projects.

Stakeholders' views: A limited number of Member States expressed their preference for this voluntary measures option. They thought that the role of the EU should be to complement national critical infrastructure policies with measures such as exchange of best practices and methodologies. Similarly, a small number of operators[103] found that the existing measures are sufficient, and preferred the voluntary option. Other operators did not consider this option as a 'stand-alone' one, but rather found that the soft measures should complement the regulatory policy options.

5.2.2 Policy Option 2: Revised selection criteria and requirements for operators of European Critical Infrastructures (ECIs)

This option envisages a new ECI Directive in line with the recommendations of the 2019 evaluation. Rather than focus on asset protection in the energy and transport sectors, the revised approach would focus on ensuring **the resilience of ECIs in the sectors currently covered by the NIS Directive**.[104] In practice, the new Directive would entail changes to the existing cross-border ECI designation process, as well as new requirements on Member States and operators. The broader sectoral scope, coupled with the revised criteria, would **increase the number of ECIs designated** by Member States.

[102] The exchanges could also take form of seminars or workshops.
[103] Some of the operators providing feedback to the Inception Impact Assessment.
[104] The seven sectors currently covered by the NIS Directive include: transport; energy; banking; financial market infrastructures; health; drinking water supply and distribution; and digital infrastructure.

In order to clarify **the ECI identification/designation process**, the new Directive would refine the existing criteria and add new ones, e.g. the interdependency with other sectors, the number of users.[105] Member States would report to the Commission concerning the application of the revised criteria, including justification as to why certain infrastructures were not designated (without disclosing their identities). In the interest of ensuring a more aligned approach across Member States, the Commission would review each report together with Member State authorities, meeting in a small-group classified setting.

Compared to the limited risk assessment provisions of the existing Directive, the new Directive would require Member States to carry out regular **national risk assessments** relevant for designated ECIs, taking into account similar requirements in other EU legislation.[106] This, in turn, would be the basis for more thorough **risk and interdependency assessments by individual ECI operators** supported by authorities in the host Member States, as well as authorities and relevant operators in other concerned Member States. In order to ensure that necessary information is available to support this work, the Directive would include provisions aimed at facilitating the **sharing of sensitive data** (e.g. threat information or commercially sensitive information) between authorities and operators, including ones located in other Member States, thereby improving levels of **cooperation and communication** between relevant stakeholders.

In order to **enhance resilience**, ECI operators would have to ensure that their security plans contain provisions on risk reduction and preparedness, incident management, but also business continuity and recovery arrangements. This **operator resilience plan (ORP)** would also need to include arrangements for employee security management - such as on access control, access rights (including to particularly sensitive information) and categories of personnel exercising critical functions including the possibility for background checks. Member States would need to ensure that background checks of personnel exercising critical functions can be carried out upon request of an operator.

Member States would also retain an **oversight role** over designated ECIs on their territory to ensure that each operator's ORP reflects all new requirements. Member States and operators alike would be encouraged to engage in **cross-border exchanges** with authorities and operators in other potentially impacted Member States, e.g. in conducting risk assessments or in developing individual ORPs.

In order to support the implementation of the Directive, competent authorities would be required to ensure **appropriate competencies and capacities** for different capacity

[105] Article 2 of the ECI Directive sets out several cross-cutting criteria, namely: casualties; economic effects; and public effects. The 2019 ECI Directive evaluation (SWD(2019) 308) found that the cross-cutting criteria are interpreted and implemented in many different ways across Member States.

[106] For instance, the UCPM requires that civil protection authorities carry out regularly risk assessments focused on natural and man-made disasters within and outside the EU. Meanwhile, the Electricity Risk Preparedness Regulation requires National electricity crisis scenarios related to national risk preparedness plans. For other examples of EU legislation containing risk assessments, see Annex 6.

building activities (e.g. trainings, exercises) on topics such as risk assessment, business continuity planning, personnel security management, etc. The Commission in turn would be required to provide different forms of support, e.g. trainings, EU-wide exercises, etc., to authorities and designated ECI operators.[107]

To the extent that the requirements envisaged in the new ECI Directive are already provided for in existing sectoral legislation, those existing provisions should apply if they contain requirements that are at least equivalent in effect to the obligations under the envisaged new legislation.

Stakeholders' views: Only one Member State preferred keeping the focus on European Critical Infrastructures in their current form. Other Member States were in favour of changing their concept to cover infrastructures with real pan-European dimension. The operators' positions were mixed between this option and option 3 – with many of them indicating the two options as a possible way forward.

5.2.3 Policy Option 3: New requirements on critical entities

This option entails the replacement of the existing ECI Directive with an **overarching cross-sectoral framework** to enhance the resilience of **critical entities** delivering essential services in a number of sectors through infrastructures located in each Member State. This option would set out harmonised **minimum requirements** for Member States and critical entities identified under the new framework.

The **sectoral scope** would be enlarged beyond transport and energy, to include banking; financial market infrastructures; health; drinking water; waste water; digital infrastructure (including telecommunications); public administration; and space.

The larger sectoral scope is justified, as it would largely reflect the sectors that a majority of **Member States consider as critical** under their national critical infrastructure frameworks (as shown in Figure 2) and it would therefore ensure the alignment of all Member States within the sectoral scope.

It will also bring **coherence with the NIS Directive sectors**[108] (current ones and those that will feature in the future NIS Directive in the category of essential sectors). The NIS Directive already demonstrated that there was a need to ensure the security of network and information systems used by operators for the provision of services that are essential for the maintenance of critical societal or economic activities against cyber threats. These operators should therefore also be secure and resilient against a range of non-cyber risks.

[107] Currently, Article 8 of the ECI Directive stipulates that the Commission will provide different types of support for ECIs, including 'available best practices and methodologies as well as support training and the exchange of information on new technical developments related to critical infrastructure protection'.

[108] The seven sectors currently covered by the current NIS Directive include: transport; energy; banking; financial market infrastructures; health; drinking water supply and distribution; and digital infrastructure. The essential sectors that will be covered in the revised NIS Directive should in addition include the telecommunications, public administration and waste water sectors.

In addition, including the telecommunications and space sectors would ensure that these two sectors, which are important vectors for daily operations of many other sectors (as shown in box 3), are resilient. In both sectors, the operators rely on physical assets requiring protection against non-cyber risks (such as 5G towers or ground stations and centres of space systems). As to the space sector, a number of Member States advocated for its inclusion in the scope, notably given its particular European dimension[109].

The larger sectoral scope will also respond to the **finding of the evaluation** of the ECI Directive, which concluded that its limited sectoral scope does not allow taking into account the increased interdependencies that exist with other sectors. The new sectoral coverage will ensure that authorities and operators adequately address the risks arising from the dependencies between sectors.

Other factors that supported the selection of the sectors included stakeholders' views reflected in the results of different consultation activities; the level of importance for society of sectors as revealed by a major crisis such as COVID-19 and the interdependency among sectors.

More specifically **on substance of the option:**

Member States would be obligated to develop a **national CI resilience strategy**[110] for at least the sectors within the scope of the legislation. The strategy would set out objectives and measures aimed at enhancing the resilience of critical entities. The legislation would require Member States to carry out **national cross-sectoral risk assessments,** taking into account similar requirements in other EU legislation. In carrying out the risk assessment, Member States would have to identify the risks arising from interdependencies between sectors and operators, including cross-border interdependencies.

On the basis of the outcomes of the risk assessment, Member States would be required to use **common criteria** set out in the new legislation (similar to those depicted in Option 2) to identify critical entities. The criteria included in the legislative instrument would be determined taking into account the criteria more commonly used by Member States in designating national critical infrastructures as well as the criteria currently used in the ECI Directive as well as those contained in the NIS Directive. These criteria would be aimed at ensuring that Member States, taking into account national specificities, identify in a consistent manner across the EU those entities operating infrastructures in their territory to deliver essential services that could be significantly disrupted by an incident, thus reducing the current discrepancies between Member States. The criteria would also provide Member States with guidance to determine what level of disruption would justify the identification of a given entity as critical. This risk-based identification process based on common

[109] Space sector (Galileo) was retained as one of the four critical infrastructures of European dimension (together with Eurocontrol, the electricity transmission grid and the gas transmission network) as part of the 2013 EPCIP voluntary pilot exercise aimed at optimising their protection and resilience (SWD(2013) 318).

[110] The NIS Directive requires the articulation of a national strategy on security of network and information systems. Member States could use the existing processes, and complement it with elements related to CI resilience.

criteria would ensure that authorities adequately identify those entities that are vulnerable to incidents that could create a significant disruption in the provision of essential services.

As a basis to identify critical entities, the legislative framework explored in this option would provide with a list of the types of entities to be considered for the identification process. The type of entities would vary depending on the sector and sub-sector: suppliers, producers, and distribution and transmission system operators for electricity, infrastructure managers and railway undertakings for the rail sector. On the basis of this list, and taking into account the risk-based approach identification process based on common criteria, the number of critical entities is estimated at 5,000 operators across the EU, approximately.

All **critical entities** would be obligated to regularly carry out **risk assessments** of their own, looking at the risks to delivering the service they provide rather than only to the (physical) infrastructure that underpins that service. These risk assessment would have to cover a minimum number of elements, including the vulnerability of their supply chains in case of disruptions and the risks from potential disruptions in other services on which the operator is dependent. This analysis of interdependencies by the operator would include cross-border spill-overs of security threats. Critical entities would receive the relevant elements of the national risk assessment in order to facilitate the assessment of the risks and interdependencies they are confronted with. Critical entities would be required to maintain **operator resilience plans** (or equivalent documents). Operator resilience plans should contain provisions on risk reduction and preparedness, incident management, business continuity and recovery arrangements, as well as arrangements as depicted in Option 2 for employee security management. Critical entities would determine the detailed resilience measures needed under the relevant requirements, taking into account the specificities of their operations and on the basis of the risk assessments, therefore ensuring that the measures are commensurate to the risks they face.

Unlike in Option 2, the plans would be focused on ensuring the resilience of services and not individual infrastructures. As an example, a critical entity providing drinking water services would be required to identify risks and prescribe measures from an overarching services perspective, rather than on the basis of what is required to protect individual elements of the operator's network, e.g. individual water treatment/purification facilities. Critical entities would also be required to engage in staff education and training on the measures contained in the plans.

Member States would exercise **oversight** over operators insofar as they would be allowed to request – where relevant and necessary – specific information from operators about their assessment of risks and interdependencies, the ORPs and other obligations, and to issue orders to operators. Such orders would, where appropriate, be provided on the basis of a dialogue between the authorities and the operator and, in any event, the authority would only be able to require measures which are proportionate to the capacity of the operators and commensurate to the risks they face. As in Option 2, competent

authorities would also be responsible for ensuring that background checks on critical personnel can be carried out upon request of an operator.

In order to promote close sectoral and cross-sectoral coordination, including during incidents, Member States would be required to establish **cooperation structures** involving competent authorities and operators, both of whom would in turn designate **points of contact**. Furthermore, the new legislative instrument would require competent authorities to ensure that appropriate resources and competencies are allocated to **oversee and support resilience-building efforts** on the part of critical entities.

For its part, the Commission would **support the implementation of the legislation** by setting up **a dedicated knowledge hub** within the Commission.[111] This hub could offer, for instance, assistance in relation to the following: facilitating a common approach to assessing risks relating to cross-border and cross-sectoral interdependencies; guidance materials; trainings; supporting organisation of exercises and stress tests; or exchange of knowledge and best practices with experts. The Commission and the hub more specifically would also support efforts to **share information** both in relation to the legislation itself and more generally as well, e.g. in the context of the external dimension involving neighbouring countries and strategic partners. Furthermore, the Commission could explore the feasibility of setting up a secure communication platform or reinforcing existing ones to facilitate information-exchange between Member States.

The hub's activities would complement those of **a Commission expert group** replacing the existing CIP PoC group. The expert group would also allow for coordination with other relevant EU-level groups and in particular with the NIS cooperation group.[112] The group would act as a forum to advise the Commission and to facilitate cooperation, including between Member States, by promoting the exchange of and best practice, including on the identification of critical entities, sharing of information on national strategies, or collecting information relating to risks and incidents, among other tasks. This would add to other provisions to ensure coordination among Member States, such as a requirement for Member States to consult each other where an entity would be identified as critical by more than one Member State, with a view to reduce the burden on the critical entity.

The definition of ECIs would be changed as compared with the current ECI Directive, focusing exclusively on core infrastructures of particular European significance.[113] The

[111] The hub would need to account for the work of existing Commission centres, including the Emergency Response Coordination Centre (ERCC) and the Disaster Risk Knowledge Management Centre (DRKMC), co-organised by DG ECHO and the JRC.

[112] Other examples include the Electricity Coordination Group, the Gas Coordination Group, the Oil Coordination Group; AVSEC, RAILSEC, MARSEC in the transport area; the Civil Protection Committee, the Seveso Committee, the Health Security Committee, etc.

[113] Candidates for classification as European Critical Infrastructures could be put forward by the Commission and agreed with the Member States. Some examples of arguably core European infrastructures include

new legislation would establish a process to identify **critical entities of particular European significance** (CE-ES), i.e. those which provide services across a large number of Member States (e.g. air traffic management, space-based navigation and timing services meeting the criteria), and thus establish an EU approach in order to ensure their resilience. The identification of critical entities of particular European significance would be done on the basis of the number of Member States to or in which the operator provides its services.

Operators identified as critical entities of particular European significance would be subject to the same requirements as critical operators (regarding the risk assessments and operators resilience plans) and the oversight and enforcement of compliance would remain under the responsibility of the Member State that identified them as critical. It would be up to the Member States where the infrastructure underpinning the essential service is located to require the operators to draw up the operator resilience plans. The difference would be that all Member States would be made aware of the measures taken to ensure the resilience of the operator. Those Member States would inform other Member States and the Commission about their oversight activities for an exchange of views.

Furthermore, these critical entities of particular European significance could receive additional guidance about the resilience measures through advisory mission organised at EU level, without prejudice to the Member States responsibility to ensure oversight and enforcement. The knowledge hub within the Commission could organise a pool of **European Resilience Advisors** from the Member States, which would be tasked with providing advisory support to the entities concerned in meeting the requirements stipulated in the legislation.

On a voluntary basis, Member States could also request that European Resilience Advisors provide support to other critical entities besides those of European significance.

As regards the **setup of this option**, it would consist of a **general framework** (Directive) setting out harmonised **minimum requirements** for Member States and critical operators. To the extent that the baseline requirements envisaged in the new legislation are already provided for in **existing EU sectoral legislation**, those existing provisions should apply if they contain requirements which are at least equivalent in effect to the obligations under the envisaged legislation. In some instances, critical entities might need to complement the measures already in place with additional elements. For instance, when the sectoral legislation only addresses in an equivalent manner intentional threats or requires protection measures, the identified operators would have to address other types of threats in accordance with the requirements of the new directive.

EUROCONTROL, certain components of the EU Space Programme (Galileo, Copernicus etc.), and energy and transport networks.

The minimum baseline requirements would be, where necessary, subsequently complemented by **more tailored obligations** to reflect thematic specificities (for instance on risk assessment processes or employee security requirements) or covering aspects specific to a certain sector, and without obligation to amend existing EU sectoral legislative instruments. The more tailored obligations could be adopted by delegated/implementing acts, as appropriate, or by legislative measures.

The general framework could also establish provisions to ensure that the relevant authorities notify incidents to other relevant authorities. The overall approach would thus aim to ensure coherence with existing sectoral obligations under EU law, so as to avoid excessive burden or duplication.

Stakeholders' views: This option focused on the shift from protection of assets to resilience of essential services provided by critical entities was considered as the preferred option by the majority of Member States that provided input[114]*. Member States considered that the best way to achieve a more common approach to resilience would be by establishing minimum criteria (for different obligations and the identification process), which would leave room for flexibility for national specificities. Member States were supportive to expanding the scope beyond transport and energy sectors (to current NIS sectors or beyond). The views of operators as regards the sectors diverged, ranging from no additional sectors to a more ambitious sectoral scope. Several operators considered that requirements under the existing sectoral legislation should be taken into account.*

5.2.4 Policy Option 4: New requirements on critical entities and a reinforced role for the EU

This option includes all elements outlined in Option 3. In addition, this option proposes a more substantial role for the Commission in identifying critical entities as well as either the creation of a dedicated EU Agency responsible for CI resilience in support of Member States and operators or to task existing EU Agency, such as Europol, with this responsibility. The Agency would assume the roles and responsibilities assigned to the dedicated knowledge hub proposed in Option 3.

As regards the **identification of critical entities**, the legislation would provide clear sector and country-specific thresholds for each of the criteria used to identify operators providing essential services. On the basis of these thresholds, Member States would be required to provide the Commission with an initial list of identified operators and relevant accompanying data, which would be assessed jointly by the Commission, the EU Agency, and competent Member State authorities for the purposes of identifying

[114] Representing the balance between the size and geographical position of Member States, as well as the maturity of CI policies in place.

those operators as critical. The identification arrangements would be established in the legislation. Just as in Option 3, identified critical entities would be required to develop an **operator resilience plan** and meet other specific requirements. The Commission and the EU Agency would develop **binding sector-specific risk assessment and interdependency identification methodologies** for use by competent authorities and critical entities in the different sectors within the scope of the legislation.

Per this option, the **oversight role** exercised by competent national authorities over critical entities would be **supported by the EU Agency**, which would be tasked with carrying out regular on-site inspections of sites/facilities owned or operated by critical entities, including those of European significance (described in more detail in Option 3). As part of its **capacity building** mission, the Agency would also provide advice and assess individual operator plans upon request. Furthermore, the Agency would be charged with organising regular trainings and EU-level exercises as part of a multi-year EU-wide capacity building programme, which would be developed in close coordination with other relevant EU Agencies. Finally, the Agency would be in charge of organising the pool of European Resilience Advisers envisaged in Option 3. The procedure for their deployment would be aligned with relevant procedures contained within the EU Civil Protection Mechanism.[115]

As in Option 3, the new legislation would be coherent with and complement the existing EU sectoral obligations.

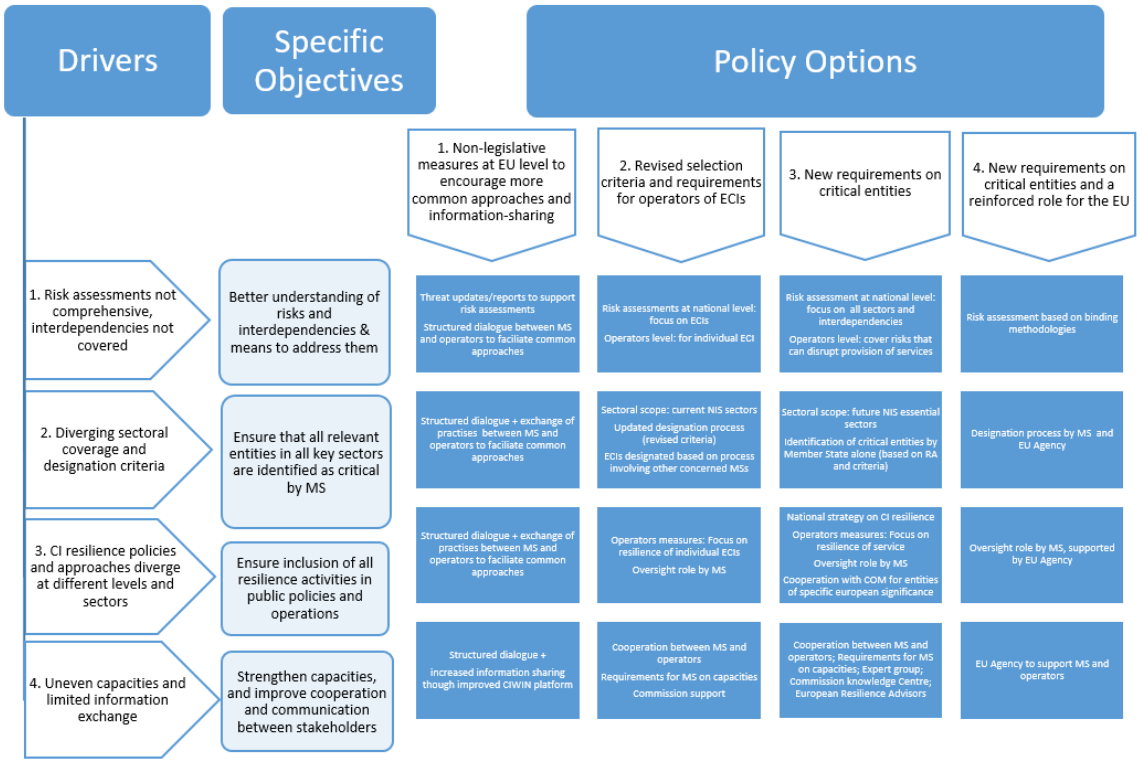
Stakeholders' views: This option was the least favoured by the Member States and the operators, as they considered it as too intrusive, 'one size fits' all approach not leaving room for sectoral specificities.

The figure below presents the intervention logic and summarises the four policy options considered and their links with the problem drivers and specific objectives[116]:

Figure 3 – Intervention logic

[115] Article 6 of Decision No 1313/2013/EU regarding voluntary peer reviews.

[116] Option 4 contains all elements of option 3. The figure only refers to key elements in addition to Option 3. Table in Annex 7 provides more detailed overview of policy options and their links with problem drivers and objectives.



Box 6: Relationship between the legislative options and sectoral legislation

The legislative options contemplated in this Impact Assessment aim at putting in place a **comprehensive cross-sectoral framework** complementing the existing sectoral legislation, which is not always exhaustive in terms of risks, focus and types of measures. For example, existing rules in sectors such as aviation or water transport focus on protection against man-made intentional threats, but not on accidents or natural events, while water legislation is limited to risks associated with water contamination and industrial incidents. The large majority of EU regulations relevant for critical infrastructures do not require the assessment of cross-border or cross-sectoral interdependencies.

As regards the measures established by sectoral instruments, in most cases these are focused on protective measures and incident management, but do not address other resilience measures such as business continuity and recovery arrangements. Other sectors, such as rail, oil or health, do not count with a framework setting out security measures in a comprehensive manner.

The legislative options foresee a cross-sectoral framework setting out a **process to identify and prioritise** those operators which are most crucial for the delivery of essential services and which thus require specific support, guidance and oversight from a security perspective. This **targeted approach** is a key feature of Critical Infrastructure policies, which therefore **complements the sectoral regulations** that, except for one specific case, apply to all entities in the sector irrespective of their importance.

The initiative resulting from this Impact Assessment will include a *lex specialis* clause,

building on the *lex specialis* clause in the current NIS Directive. When sectoral legislation establishes requirements on operators which are at least equivalent to the ones foreseen in the general framework on critical infrastructures, operators will be subject to the sectoral legislation and the corresponding obligations arising from the new initiative would not apply. This could be possible, for example, for the financial sector, which counts with a robust set of regulations for different sub-sectors requiring financial operators to manage operational risks in a comprehensive manner.

Whenever the sectoral legislation is not comprehensive in terms of setting out requirements that are at least equivalent to all those applicable under the new instrument, the requirements of the new instrument would also apply. Consequently, operators identified as critical entity would have to apply the obligations established in the upcoming initiative in addition to the obligations from the sectoral legislation. When doing so, operators would nonetheless be able to use elements arising from the sectoral legislation. For example, all airports are required to assess the risks of intentional man-made threats and to take security measures accordingly; those airports identified as critical entities would have to additionally assess the natural and unintentional risks and incorporate in their protection plans additional measures related to business continuity.

The introduction of a *lex specialis* clause and the fact that the upcoming initiative builds on existing sectoral legislation with complementary objectives means that there are no risks of overlaps and unclear requirements for operators and enforcement bodies. Moreover, current policies on resilience of operators in Member States already contemplate a strong involvement of sectoral bodies at national level. These authorities play an important role in the identification of critical entities in their respective sectors, and in relation to the security measures to be applied in every area and the oversight of the critical entities in the sector for which those bodies are responsible.

5.3 Options discarded at an early stage

One option that was considered as part of this Impact Assessment was to address the resilience of critical (physical) infrastructures and network and information systems underpinning essential services in a **single legislative framework**.

As explained in box 1, the current and future NIS Directive and the upcoming initiative on critical infrastructures have complementary objectives and have a similar scope. Nevertheless, they differ in relation to the threats and the objects to be protected. Both initiatives aim at reinforcing the level of resilience of vital economic operators, one addressing the cybersecurity of the network and information systems (software and hardware) against cyber-threats, the other addressing all other threats that can affect the physical infrastructure, processes or personnel of vital economic operators.

While the non-cyber risks considered in this Impact Assessment have evolved over time, the number of cyberattacks has grown constantly over the years[117] and does not only affect critical infrastructure operators, but a wide range of companies fulfilling important functions for the economy and society. To address a cyber-threat, which potentially materialises every day, both public authorities and companies have developed cybersecurity strategies, which – even if sometimes part of broader security policies – set out distinct arrangements specifically needed to address cyber-threats. According to Eurostat, in 2019, one in eight businesses was affected by cyberattacks, and 93% of EU enterprises with 10 or more persons employed used at least one ICT security measure[118]. As the number of cyberattacks will continue to rise, the **cybersecurity** considerations will require an EU intervention that is much broader in scope and content of measures. As outlined in the preferred policy option for the new NIS, the selected approach involves **uniform security requirements and incident reporting obligations applicable to a large number of sectors and entities** (based on fixed criteria such as the company's size[119], absence or limited availability of alternative service providers and potential impact of disruption on public safety and health).

Such an approach would be **disproportionate for critical infrastructure resilience** policy, where it is necessary to pursue a **risk-based approach** that identifies critical infrastructures/services in sectors where a disruption would have a significant negative impact on economy, citizens' daily life and security. In the area of critical infrastructures, Member States need to keep a possibility to decide, **based on an assessment of risks**, which selected entities they consider as critical and requiring particular attention in terms of increased resilience efforts (decision considered by Member States as their national prerogative, related to wider national security aspects). The option of a single legislative framework was therefore discarded.

5.4 Synergies with the revision of the NIS Directive

The previous section clarified why a single legislative framework to address the resilience of both critical (physical) infrastructures and network and information systems was not considered as feasible.

Nevertheless, there is a clear link between the two initiatives, and therefore room for synergies on a number of points:

In terms of scope, the upcoming initiative on critical infrastructures will cover the operators that Member States will identify as critical entities. In practice, because of the risk-based identification process, the number of identified critical entities would be lower

[117] A study of the Commission's Joint Research Centre *(Cybersecurity – Our Digital Anchor, a European perspective,* published in July 2020, page 7.)
[118] Eurostat press release (link).
[119] Medium or large size enterprises.

than the number of companies in scope of the new NIS. This would be a proportionate approach, taking into account the relatively lower frequency of physical incidents compared to cyberattacks.

For the identified critical entities, the revised CI framework will include requirements to ensure their resilience against a range of non-cyber threats. However, infrastructures are also exposed to cyber threats – there were almost 450 cybersecurity incidents in 2019 involving European critical infrastructures in sectors such as health, finance and energy[120]. It is therefore necessary to ensure that critical entities are also resilient against cyber-risks, given that their operations rely, among other things, on ICT systems. The cybersecurity element of critical entities identified by Member States in revised CI framework will be covered by the obligations in the revised NIS Directive, which will have a provision including critical CI entities in its scope. All critical entities under the new CI framework will therefore be covered by the new NIS Directive. This will ensure a **comprehensive, 'all hazards' approach towards the resilience of critical operators.**

The complementarity between the two initiatives would also be ensured by an **alignment in terms of sectors**, as explained in section 5.3 (all sectors under the new CI framework would be in scope of the new NIS essential sectors),

Moreover, the initiative will include provisions for **cooperation between competent authorities** under both Directives. This will be done via regular meetings, exchanges and information sharing between the Commission expert group on resilience of CIs and the NIS cooperation group. The new initiative will also foresee more detailed provisions on information exchange on incident notification and enforcement activities. The timelines of different obligations (such as MS national strategies on resilience of CIs and cybersecurity strategy and their updates) will also be streamlined between the two initiatives.

6. WHAT ARE THE IMPACTS OF THE POLICY OPTIONS?

6.1 Economic impacts

All the options would positively contribute to varying degrees to the reliable functioning of the **internal market** when compared to the baseline scenario. For instance, the measures would all reinforce the capacity of operators to ensure the resilience of CIs underpinning essential services in the face of current and future risks. By doing so, the number of disruptions to essential services and their negative consequences would be reduced. The effect of this would be that the provision of essential services across the EU would be more reliable over the medium to long term.

[120] A study of the Commission's Joint Research Centre *(Cybersecurity – Our Digital Anchor, a European perspective,* published in July 2020, page 7). As framed by the World Economic Forum, 'cyberattacks on critical infrastructure have become the new normal across sectors such as energy, healthcare, and transportation' (WEF, The Global Risks Report 2020).

According to the World Bank, as companies "rely on infrastructure services to operate effectively and compete internationally, […] disruptions and lack of reliability have significant adverse impacts on the performance of firms".[121] Indeed, arguably every sector relies on services rendered by electricity providers, while the retail sector would come to a standstill without reliable logistical services underpinned by transport infrastructure. Given the key role of essential services such as these for business activities, actors in all sectors of the economy would be expected to benefit from enhanced resilience, including small-, medium- and large-scale enterprises.

Besides the effect on business, efforts to ensure the uninterrupted delivery of essential services would increase economic stability and further improve the attractiveness of the European market to investors. The measures in different options could be expected to reduce the likelihood that business interests come to view certain Member States as being more prone to disruptions than others, which would in turn disadvantage certain companies in 'more vulnerable' Member States and benefit those in 'less vulnerable' ones. Furthermore, these measures would ensure that operators, regardless of where they operate, receive more consistent support and guidance from authorities. Taken together, these effects would contribute to a more even playing field in the internal market.

While each option would have a generally positive impact on the economy, specific options would entail different positive but also negative impacts on **critical infrastructure operators**. On the one hand, operators would benefit from greater government support to ensure enhanced levels of operational resilience, and, thus, greater overall reliability of service provision. This, in turn, would increase consumer confidence in both operators and the government authorities charged with overseeing them.

On the other hand, the measures under consideration, and in particular those involving legislation, would entail certain compliance costs, especially on the part of operators that had not previously made any particular investments in, for instance, various resilience-building measures (such as the development of preparedness, incident response, business continuity and recovery arrangements, etc). The total amount of investments needed would vary from company to company, depending on the size, the sectors, the type of infrastructures they operate, the risks they face and the security measures they have in place already. Operators who have already taken such measures would be likely to experience minimal added burden over the status quo.

Any additional costs incurred by operators could potentially be felt by **consumers**, for instance, where operators were to pass these on in the form of increased tariffs, fees, etc. However, these costs would be accompanied by the provision of more resilient and, thus, more reliable services. In regulated sectors such as energy transmission, the allocation of

[121] Hallegatte, S; J. Rentschler, and J. Rozenberg. Lifelines : The Resilient Infrastructure Opportunity. World Bank, 2019 (link).

those costs among public and private actors would require more transparency for the costs of protecting CI in the tariff structures.[122]

The **number of companies** that would bear the costs associated with different measures would vary by option[123]. For instance, the impacts of Option 2 would only directly affect designated ECI operators (estimated at approximately 1,200), while Option 3 and Option 4 would concern a larger number of companies identified as critical operators (estimated at approximately 5,000 operators in Option 3, and 6,000 in Option 4).[124] Given the sensitivities related to the identities of critical infrastructures/operators, and lack of information shared by the Member States, the estimates for option 2 were done on the basis of designations according to the ECI Directive. The estimates for options 3 and 4 were done on the basis of the number of OES identified according to the NIS Directive, and have been confirmed through estimates based on the numbers of national critical infrastructures communicated by some Member States as part of the feasibility study, which led to similar results.

Ultimately, Member States will also take into account the outcomes of national risk assessments to identify critical operators.

Among those operators affected by the various options, the number of **small- or medium-sized enterprises (SMEs)** is expected to be small. While in sectors such as transport, energy or water, CI operators are usually sizable enterprises with thousands of employees, they may be smaller elsewhere. For instance, it is conceivable that in the digital infrastructures or space services sectors, SMEs provide some specific highly technical or specialised services. However, SMEs in this position are arguably incentivized to ensure a high level of resilience on their own and/or are subject to specific

[122] The Commission is currently preparing an initiative for enhancing the resilience of the European energy system against physical, cyber or hybrid threats, which, among other issues considers ensuring a level playing field for energy operators with regard to the financing of specific security measures.

[123] For Options 1 and 2, the impacts on national infrastructures not designated as ECIs would be indirect, given that the exchange of best practices and new policy towards ECIs could potentially contribute to some alignment of national CI resilience policies in terms of sectors and objects/services considered to be critical.

[124] The estimations about the number of identified operators are informed expert-based assumptions carried out on the basis of the information available at the time of writing this Impact Assessment.

The estimation of ECIs designated in Option 2 takes as a departing point the Member States that have until now designated more than five ECIs. It considers factors such as their population and geographical characteristics, and assumes that the improved designation criteria would trigger Member States not having made any designation so far, to achieve more ECIs designations in their territory under the new Directive. It also takes into account the enlarged sectoral scope, while considering that the infrastructures in some of the additional sectors are likely to have a smaller cross-border dimension compared to those in transport and energy.

The estimation of critical entities is based on the report on the implementation of the NIS Directive (COM(2019) 546). It is based on the assumption that all Member States would achieve a similar number of identified operators as those Member States that have so far identified a relatively high number of operators of essential services under NIS in relation to their population –excluding extreme cases. The approximate figures were developed by selecting a sample of Member States with different sizes and geographical balance, and extrapolating the average number of identified operators of those countries to the EU-27. In Option 4, the number is expected to be higher because of clear thresholds for identification criteria and coordination efforts of the Commission/Agency in the identification process.

national- and/or EU-level requirements, thus reducing the additional costs associated with these options. It is worth noting that particularly large-scale operators may outsource certain tasks to SMEs, e.g. maintenance services or more qualified technical support competencies. However, the burden on these SMEs is anticipated to be small, as the obligations under each option target operators and not supporting actors such as these.

Finally, every option would likely entail some administrative and budgetary burden on **competent Member State authorities**. Per Option 1, authorities might expend considerable resources in the context of the **structured dialogue** and other related work streams. Those Member States that make changes to their approaches at national level as a result of the structured dialogue would also incur additional costs.

In the case of Option 2, the costs would increase for those Member States not yet carrying out **national risk assessments for ECIs**, and with regard to the anticipated **designation** of additional ECIs in more sectors. These costs would stem largely from the organisation of consultations with candidate ECI operators and competent authorities in other Member States and targeted capacity building activities, as well as reporting by Member States on the application of designation criteria.

The **identification-related costs** associated with Option 3 are expected to be lower than in Option 2. This is due to the fact that Member States would not be obligated to engage in dialogue with other Member States, and that the identification process established under the NIS Directive could be used as a starting point to identify critical entities. On the other hand, the need to set up **public-private cooperation structures** where they do not already exist and to provide additional support to operators in fulfilling the obligations of the legislation would entail certain costs. These could be partially alleviated by the activities of the Commission's knowledge hub. Similarly, the expected higher costs related to the identification process of Option 4 (due to additional coordination efforts with the Commission) could be compensated by the support of the EU Agency.

Generally speaking, the options are expected to have varying degrees of positive impacts on the economy depending on the extent/depth of each intervention. While authorities, operators and consumers could be expected to bear some additional costs in each case, especially where the legislative options are concerned, these would be outweighed by the fact that the provision of essential services is made more reliable. The costs would be limited for those Member States and operators already fulfilling equivalent requirements stemming from the existing sectoral legislation at EU level.

6.2 Social impacts

The social impacts of the options at both societal and individual level are anticipated to be most tangible as regards security, public safety, quality of life, and health.

Seen from a societal standpoint, the proposed options aim to ensure more coordinated cross-border and cross-sectoral responses to the challenges posed by a rapidly changing operational landscape. For instance, the implementation of additional resilience-building measures at operator level would ensure more effective mitigation of current and future risks, many of which, like climate-induced hazards and accidents, were not adequately accounted for when the ECI Directive was adopted, and which might otherwise risk falling outside the narrow bounds of existing operational security arrangements.

Assuming these resilience-building measures lead to fewer disruptions, we can anticipate safer working conditions for CI staff, as well as positive economic, quality of life and health impacts on a more strategic level. Indeed, the World Bank suggests that "the well-being and livelihoods of households depend so critically on the availability of quality infrastructure services".[125] By this logic, the more reliable the provision of essential societal services, the greater the likelihood for positive economic, social, educational, professional and recreational benefits in citizens' lives.

While every option analysed would have a positive social impact when compared to the baseline scenario, those that involve a comparatively large number of operators and that strengthen the role of authorities, e.g. to provide guidance, exercise oversight, are expected to be particularly beneficial. These include Option 3 and Option 4. For their part, Option 1 and Option 2 would lead to smaller improvements to resilience, given that they provide fewer incentives to a smaller number of operators to take relevant measures.

6.3 Environmental impacts

Every option is intended to reduce the likelihood of disruptions to essential services provided by CIs. Depending on the circumstances, such disruptions can lead to fires, spills, leaks, etc. that have serious environmental effects that can threaten air and (drinking) water quality, and, by extension, biodiversity, flora, fauna and landscape. Furthermore, while certain CI operations are associated with different detrimental environmental effects (e.g. poor air quality, climate change, etc.), activities associated with the management of disruptive events, such as a sudden shutdown or start-up of operations, may too have environmental impacts, since they constitute an inefficient use of resources and threaten efforts toward more sustainable consumption and production.

The sharing of best practices envisaged in Option 1 would, to some extent, contribute to reducing the risk of disruptions affecting the environment. However, more significant positive impacts are expected from the legislative options, where the capacity of authorities and of a larger number of operators to respond to disruptions (including those with environmental implications) would be enhanced in a more structured fashion.

[125] Hallegatte, S; J. Rentschler, and J. Rozenberg. Lifelines : The Resilient Infrastructure Opportunity. World Bank, 2019 (link).

6.4 Impact on fundamental rights

Every option is intended to enhance the resilience of CI operators that underpin the provision of essential services, whilst eliminating regulatory obstacles to their ability to provide their services across the Union. This would reduce the risk for disruptions at both societal and individual levels, and contribute positively to higher level of public security whilst also positively affecting the freedom of operators to conduct business, as well as many other economic operators reliant on the provision of esesntial services, ultimately benefitting consumers. The operator resilience plans envisaged in Options 2, 3 and 4, respectively, would include arrangements to ensure effective employee security management, which may include the processing of personal data in the interest of, for instance, establishing access controls and determining access rights for specific categories of personnel exercising critical functions or with access to particularly sensitive information. The envisaged legislation would only spell out general principles in relation to employee security management. The processing of personal data by individual operators would be governed by the General Data Protection Regulation.[126]

7. HOW DO THE OPTIONS COMPARE?

7.1 Effectiveness

Objective 1: Ensure higher level of understanding of risks and interdependencies, as well as the means to address them

All options will contribute to increasing the capacity of authorities to assess risks and interdependencies and inform operators about them, enhancing in turn their understanding of the risk landscape. The effectiveness of the specific measures contained in **Option 1** (e.g. threat updates/reports, the exchange of information as part of the structured dialogue) would depend on Member States' willingness to participate and share effectively outcomes with operators. **Option 2** would be very effective in increasing ECI operators' ability to understand risks and interdependencies, as they would benefit from the national risk assessment and receive targeted support from authorities in carrying out their own. Other operators (not designated as ECIs) could also benefit, if Member States decided to use a similar approach to support national critical infrastructures.

Option 3 and Option 4 would be more effective than Option 2, insofar as the obligations would be directly applicable to a larger number of operators, irrespective of the extent to which their operations are cross-border in nature. Given that the national risk assessment would be broader in scope, covering more sectors and operators, and the risk assessment

[126] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

requirements at operator level better articulated, Option 3 would effectively ensure a clearer understanding of the risks. **Option 4** would be still more effective – in addition to the measures of Option 3, the methodologies developed by the Commission/EU Agency would ensure a consistent approach across Member States and operators.

Objective 2: Ensure that all relevant entities in all key sectors are identified as critical by Member States

Option 1 would have limited effectiveness, given that it would be difficult for authorities involved in the structured dialogue to translate the exchange of best practices into changes of national policy over the medium term. Meanwhile, **Option 2** would bring greater alignment of national-level policies by enlarging the sectoral scope and refining the cross-cutting criteria for designating ECIs. In practice, Member States would designate more ECIs in a larger set of sectors and in a more coherent manner, ensuring that a higher proportion of critical assets obtain such a status and the government guidance and support associated with it. While this impact would be direct on ECIs, a spill-over effect could be expected in national designation policies.

As with the previous objective, **Option 3 and Option 4** would be more effective than Option 2, as the clearer identification process and broader sectoral coverage would concern a larger number of operators, going beyond the ECIs. This would mean that there would be greater consistency with regard to the sectors and assets/services that the Member States would identify as critical, and more clarity for the operators as to whether a given infrastructure will be considered as critical across the countries and sectors. In **Option 4**, the involvement of the EU Agency in the identification process together with the Member States could lead to further alignment of the identification of critical entities.

Objective 3: Ensure that the full spectrum of resilience activities is included in public policies and operational practice

In **Option 1**, the participation of the authorities in the structured dialogue discussions related to business continuity management policies would lead to a limited shift towards resilience as compared to the baseline scenario. While the exchange of best practices would help in obtaining a more common understanding of the measures necessary to ensure the resilience of essential services, the non-binding nature of the dialogue would mean that there would still be considerable gaps in the CI approaches followed by different Member States. The outcome of the exchange of best practices is more likely to be translated into national policies in Member States where thinking on resilience is already enshrined in legislation, as opposed to Member States where this concept is not yet fully considered and prioritised.

In **Options 2, 3 and 4**, the provisions requesting the operators to include business continuity arrangements in their resilience plans and the requirements on Member States to provide guidance and oversight to operators would ensure that the concept of resilience is effectively mainstreamed and operationalised in Member States' policies and

operators' measures. The effectiveness of **Option 2** would mainly relate to the increased resilience of a specific set of ECIs –although a spill-over effect could be expected for national CIs, since some Member States would adapt their approaches to the latter as well. In **Options 3 and 4**, this would be the case for a larger number of operators, who would be expected to focus on ensuring the resilience of the services that they provide, rather than solely the protection of individual physical assets that their operations consist of. The requirement in Options 3 and 4 for the Member States to develop a national strategy on resilience in all relevant sectors, would increase their effectiveness as compared to Option 2, as it would ensure a greater focus on resilience in CI policies.

Objective 4: Strengthen capacities and improve cooperation and communication between stakeholders

Like for the previous objectives, the extent to which the good practices on public-private cooperation shared in **Option 1** would be replicated across the EU would depend on the willingness of Member States to introduce them at national level, especially if these required changes to legislation or additional resources. The effectiveness of Option 1 in respect of cooperation between stakeholders would thus be limited, although it would be compensated to some extent by the upgraded functionalities of the CIWIN platform.

The provisions considered in the remaining options aimed at facilitating the sharing of sensitive data and the requirement to ensure additional competencies and capacities would be considerably more effective in reinforcing the capacities of and cooperation among stakeholders than Option 1. Given that **Options 3 and 4** would have a larger scope than **Option 2** and would bring more structured support from the EU to authorities and operators, they would be significantly more effective. This applies in particular to Option 4 due to the higher budgetary and organisational capabilities of a dedicated Agency compared to a smaller structure (the knowledge hub) within the Commission.

7.2 Efficiency

The assessment of efficiency is qualitative[127], given the difficulty to obtain quantitative data from Member States and operators because of the sensitive nature of this policy area. As an example, the identities of specific ECIs are not known, as it is considered as sensitive information by Member States. Similarly, operators are not willing to share data that could also in addition be commercially sensitive.

Box 7: Estimation of costs and benefits – main assumptions

[127] Annex 3 includes indicative estimates for the preferred option, on the basis of limited information provided by some Member States. The difficulty to obtain the data was already faced during the evaluation of the ECI Directive, because of the sensitivity concerns.

The **benefits have been assessed in a qualitative way**, since some of them are per definition intangible, such as the increased reliability of services improving the functioning of the Internal Market or the reinforced security benefits. Compliance cost reductions have also been assessed from a qualitative perspective since they will depend on the actual implementation of the initiative by Member States and their current practices, which vary across Member States.

The **costs on administrations** have been estimated considering that for Member States, costs will vary depending on the current status of their national CI frameworks: some will only have to introduce adjustments in their national strategy and risk assessment while others will require more efforts in order to comply with the new obligations. The specific costs for each obligation have been **estimated for the preferred option**, and are summarised in Annex 3. The estimates were obtained through an informed assumption, on the basis of experiences with similar exercises (preparation of strategies, performance of risk assessments, etc.) and the tasks that each obligation would involve.

The **costs on operators** are also established through an informed assumption, considering the tasks for each obligation. The number of critical operators that will have to comply with the requirements (explained in economic impacts section 6.1) was estimated on the basis of the identification of operators of essential services under the current NIS Directive, and has been confirmed through estimates based on the numbers of national CIs communicated by some Member States.

While the options come at varying costs for operators and Member States, their benefits are also proportionate, i.e. the higher the costs, the greater the benefits. Overall, all the options can be considered efficient insofar as the costs incurred under each option are balanced compared to the benefits to be expected in improving the resilience of essential services and the good functioning of the internal market. Serious incidents affecting CIs are high-impact low-frequency events. They are by their nature unpredictable but when they occur, the costs can be significant. In considering the relative efficiency of the options, the investments in improving resilience elaborated under all options would likely appear marginal compared to the cost of a major disruption.

Option 1 would bring both direct and indirect costs for Member States and operators. The **direct costs** would relate to the contribution of Member States and selected operators/experts to activities within the structured dialogue, in terms of providing input and information. The Commission would bear the organisational costs, the coordination of inputs and development of the resulting guidelines and reports. The improvement of CIWIN's functionalities would imply a moderate cost for the Commission as well.

The **indirect costs** would depend on the extent to which Member States take up the outcomes of the exchanges. Some of the elements addressed in the structured dialogue, such as the risk assessment methodologies and incident reporting criteria and methodologies would not imply many additional costs, since they would be easily

incorporated into existing practices. Other elements could result in relatively higher costs for a limited number of Member States that would decide to step up their public-private cooperation mechanisms or that would shift towards a more resilience-oriented policy. In this case, some operators would incur new costs resulting from the new obligations imposed on them, e.g. business continuity requirements.

While the **costs of this option would be smaller** than for the remaining options, the **benefits would be more limited** because of the voluntary nature of the measures. While the activities related to risks and interdependency assessments and cooperation practices would lead, in the medium to long term, to better guidance from authorities to CI operators, the gaps that would remain in terms of sectors and assets/services considered as critical would reduce the overall efficiency of the option.

Given that **Option 2** would only lead to improved resilience of a limited number of operators – those owning/managing an ECI – the significant administrative burden of adapting the existing **designation process** (in terms of new legislation, thresholds and processes) in 27 Member States means that this option would be **less efficient** than the other options. An aspect that makes Option 2 particularly inefficient is the burden associated with the bilateral and/or multilateral discussions between the host Member State and the affected ones in order to designate an ECI. This would be an additional process on top of the one to designate national CIs, leading to additional administrative costs for authorities. On the contrary, in **Options 3 and 4** focused on identifying critical entities, Member States would be able to use as a basis the identification process set up for the current NIS Directive (which is in many cases aligned with the national identification process). Member States would therefore benefit from reduced compliance costs for the identification. At the same time, while the involvement of the Agency and the Commission in the identification process as per Option 4 would ensure that a relatively larger number of operators would be identified as critical, a double level of identification could lead to a duplication of efforts.

Given that some substantive **obligations for Member States** in Option 2 are similar to those in Options 3 and 4 (national risk assessment, capacity building, information exchange and cooperation), the efficiency in terms of Member States' actions would be higher in those options where a larger number of operators benefit from the efforts of Member States. As regards the oversight costs, they would be higher in Option 2 for the majority of Member States, as they would have to assess and validate the resilience plans of all designated ECIs[128]. In Options 3 and 4, Member States would not be compelled to scrutinize all resilience plans – given the larger number of identified operators – but would rather be empowered to do so when necessary. Such an approach would be more efficient as it would allow authorities to prioritize the operators needing further scrutiny.

[128] In a limited number of Member States, authorities already assess and validate operator security plans and measures.

The substantive **requirements on operators** are also similar in Options 2, 3 and 4, the difference being in the number of operators affected and the engagement with authorities as regards oversight. Therefore, while the burden on individual operators would be similar, the total costs on all operators combined are expected to be higher in Option 3, and especially Option 4, as they would cover a larger number of entities. At the same time, the benefits would also be commensurate to the costs: the increased reliability of more operators improves the resilience of CI networks across the EU.

In Options 2, 3 and 4, operators would have to carry out risk assessments and to develop or upgrade their current security plans, especially to include business continuity arrangements in the cases where these are not yet considered. The administrative burden for individual designated operators would be greater in Option 2, as all of them would have to discuss their plans with the respective authorities. Although this would ensure that they have more appropriate measures in place, it may in some cases also imply greater investments in security measures. Option 4 would entail an additional burden on some critical entities; given the efforts on which they would incur in order to facilitate the on-site inspections by the EU Agency.

Some operators would also incur bigger security expenses in **Options 3 and 4**, although only those operators where the authorities consider that there is a need to verify the operators' plans and, if necessary, amend them and take corresponding measures. In these two options, the majority of operators would not be subject to such detailed controls. Nevertheless, the mere requirement for the operators to carry out the risk assessments and develop resilience plans would contribute to a greater security culture and awareness among management and would provide arguments for security departments in the allocation of resources in respect of other priorities.

The burden borne by the operators deriving from additional security measures and by the authorities in terms of additional support to operators would be partly alleviated by the Commission's **capacity building and support activities**, such as trainings, exercises, and guidelines. In Option 2, this would be channelled via ad-hoc initiatives through, for instance, EU funded projects or the activities of the Joint Research Centre. The efficiency of this option will be lower, as it will be more burdensome to organise (e.g. calls for proposals) and it will be more difficult to capitalise on the output of these activities after the conclusion of the projects. The organisation, coordination of activities and optimisation of results would be the main added value of the knowledge hub, which would be an efficient platform to ensure a smooth set-up, overview and dissemination of EU-projects, accumulating expertise over time that would prove beneficial to stakeholders. The Agency as per Option 4 would also be a useful instrument to carry out these capacity building activities, as well as to support Member States in the identification and oversight of operators. However, it would come at a significant cost for the EU budget. This, together with the risk of duplicating efforts in relation to the

identification of critical entities and the additional burden on operators related to EU inspections, suggest that Option 4 is overall less efficient as compared to Option 3.

7.3 Coherence

The different options would be coherent with the overall objective of improving the good functioning of the internal market and building an area of freedom, security and justice. The measures envisaged contribute to one of the four main strategic priorities of the **Security Union Strategy** aimed at achieving a future-proof security environment[129]. Furthermore, reinforcing the resilience of CIs providing essential services would be in line with the objective of the Next Generation EU fund aimed at supporting not only the recovery but also the resilience of the economies of the Member States[130].

All the options complement the different **sectoral initiatives** that aim at improving the resilience of operators providing services essential for society. While generally, these sectoral instruments establish requirements applicable to all types of operators, the options assessed in this Impact Assessment target those operators which play a crucial role in delivering those services and thus require special support and guidance.

While Options 1 and 2 are consistent to a large extent with national frameworks, their focus on assets would maintain the discrepancy with the services-oriented approach of the NIS Directive. In the case of Option 1, this discrepancy would be higher, as the ECI Directive would remain unchanged, and focused on protection and limited to two sectors.

With the reinforced focus on resilience, all options would be in line with the proposal for a revised Union Civil Protection Mechanism and its resilience goals, and, in particular, Options 3 and 4, since they would incorporate the resilience approach in the legislative instrument. These two options would also ensure an alignment with the focus on ensuring the provision of services under the current and future NIS Directive. They would also be coherent with different sectoral legislation insofar as the latter would take precedence whenever the existing rules and requirements for operators in that sector would be equivalent or even go beyond the proposed measures. Whenever that was not the case, the measures under these options would not replace the sectoral legislation, but only complement it. For example, identified operators covered by existing EU legislation focused on a limited set of risks or establishing only protection measures would have to ensure, that they address additional risks or take measures towards resilience.

7.4 Proportionality

While some of the proposed measures in the legislative options may have negative impacts on operators, particularly in relation to the expected costs of additional security

[129] COM(2020) 605.
[130] Conclusions of the Special meeting of the European Council (17, 18, 19, 20 and 21 July 2020) (link).

measures, these impacts would not be disproportionate insofar as they would be limited to those operators with insufficient measures as regards the security of their infrastructures and services. The costs on operators that the different options would entail are justified in light of the negative consequences of the disruption of services, which are essential for the normal functioning of the society and the economy.

Similarly, the administrative burden on Member States' authorities of the different options would not be disproportionate, given that they would contribute to improve their existing CI resilience policies. Moreover, it is assumed that in many instances, the measures put forward would only update or complement the already existing processes.

The costs of setting a new Agency as per Option 4 would not be negligible but would also pay off in the medium term, given the reinforced effectiveness of EU actions to improve the resilience of essential services. At the same time, the binding methodologies would not allow for adapting to specificities of different Member States, and the prominent role of the Commission and the EU Agency in identifying operators and in exercising oversight through on-site inspections would interfere in an excessive manner with the primary responsibility of Member States in security. Therefore, Option 4, despite being slightly more effective than Option 3, would go beyond of what is necessary to achieve the objectives.

The table below summarises the assessment of different policy options, in relation to the baseline scenario.

Option	Effectiveness vis-à-vis objectives				Efficiency	Coherence	Proportionality
	SO 1	SO 2	SO 3	SO 4			
1	+	≈/+	≈/+	≈/+	++	≈	+++
2	++	+	++	++	≈/+	+	+++
3	+++	+++	++++	+++	++++	++++	+++
4	+++	++++	++++	++++	++	++++	---

8. PREFERRED OPTION

8.1 Presentation of the preferred option

This Impact Assessment report has proposed a number of options, each addressing the problem drivers with increasing levels of requirements.

Option 1 would address the problem and the reasons behind it to a limited extent. While the structured dialogue would require relatively low costs for all stakeholders, it would not lead to meaningful results in the medium term, given the voluntary nature of integrating those changes into national frameworks or translating the outcomes to the current practices of authorities and operators. While it would be proportionate, it would not improve the coherence of the ECI Directive with the existing EU framework, and in particular with the services-oriented approach of the NIS Directive.

This would also be the case to some extent in Option 2: despite the new focus on resilience, maintaining a designation process focused on assets with cross-border impacts would not follow the focus on services of the NIS Directive. Despite its increased effectiveness as compared to option 1, it would mainly enhance the resilience of a limited set of CIs, leaving a substantial gap that would only be addressed to the extent that Member States replicate the existing measures and tools in relation to national CIs. Furthermore, this option would not be much more efficient as regards the current situation, since the efforts by Member States would not benefit all relevant operators, as compared to Options 3 and 4.

Precisely the difference in the number of operators identified under each option is the main factor behind the different economic and social benefits. Given that overall the legislative measures aimed at improving the resilience of the essential services provided by CI operators would bring positive social effects and create positive economic impacts both to society as a whole and to affected operators – despite the increased costs on them – Options 3 and 4 would be more effective than Option 2. Under these options, the operators would be expected to focus on ensuring the resilience of the services that they provide, rather than solely on the protection of individual physical assets that their operations consist of. Options 3 and 4 would also ensure greater coherence with the NIS Directive by adopting a services approach, as well as with other CI-relevant legislation by complementing those instruments that do not provide for sufficient tools in terms of risk assessment, resilience measures or support from public authorities.

The key difference between Options 3 and 4 is the proportionality of the measures proposed. While Option 4 would be slightly more effective than Option 3, the former be less efficient since it would be more costly, bring duplication of efforts and additional burden for operators. Moreover, it would be disproportionate with regard to the involvement of the Commission in the identification process and to the lack of flexibility to reflect national specificities. Option 3 would be in this sense more appropriate, not only for the higher efficiency as compared to option 4, but also because it would provide Member States with a framework that increases consistency in national approaches while leaving the necessary flexibility to address the specific risks and interests of each Member State.

Given the different economic and social impacts of the various options and considering their value in terms of effectiveness, efficiency and proportionality, the preferred option to ensure a high level of resilience of essential services provided by CIs is **Option 3**. While Options 1 and 2 would not deliver the changes needed to address the problem, Option 3 would result in a more comprehensive CI resilience framework that also aligns with and accounts for existing EU measures in related fields. Option 3 is also more efficient than the other options and more proportionate than option 4, and appears politically feasible as it aligns with the statements of the Council and Parliament on potential EU action on CI resilience. This option – with a general framework setting out

minimum requirements and the possibility to complement them as necessary with more tailored obligations on a thematic or sectoral basis – would ensure flexibility and offer a **future-proof framework** that would allow critical entities to respond to different risks now and in the future. In essence, this option would ensure that critical entities are adequately equipped to address current and future risks that may result in disruptions to the provision of essential services, addressing the problem in a cost-efficient manner.

In practice, the **complementarity** will be ensured **between the new general framework** in Option 3 **and the existing sectoral frameworks**. Whenever an operator is identified as critical entity, the entity would be required to assess all risks to their services and to set up resilience measures to ensure the continuity of those services. Whenever the identified entities are already fulfilling those obligations due to requirements from other instruments, they would not have to take further measures. Whenever their assessments/measures would not be as comprehensive because the relevant sectoral legislation is limited to some hazards (e.g. intentional threats), to specific assets or to some type of measures (e.g. protection), the identified entities would have to ensure that their risk assessments cover additional risks (e.g. unintentional threats) to extend their approach (looking at the whole service rather than at the specific asset) and to also set up business continuity measures. A similar logic will apply to the obligations for Member States authorities.

Under this preferred option, critical entities would be more resilient to potential incidents, their operations being more reliable and their services provided in a continuous fashion, thus benefitting from a better, more resilient servicing of customers. Therefore, citizens and businesses would benefit from the greater reliability in the provision of essential services, from electricity to drinking water. This would be a relevant contribution to the good functioning of the internal market. Public authorities, on their part, would benefit from the stability derived from the smooth functioning of key economic activities and the constant provision of essential services to their citizens.

Main costs and benefits of the preferred option are presented in Annex 3, including the underlying assumptions used for the estimates of costs.

It is assumed that **Member States** will have to incur one-off costs when adopting for the first time the national strategy on resilience of CIs and carrying out the risk assessment according to the new requirements. It is assumed that for some Member States, this will only require small adjustments to the existing practices, while for others, more important efforts will be required. Recurring costs would be incurred every 3 years on average, when the strategy and risk assessment would be updated. Similar assumptions apply to costs related to the identification of critical entities. Member States would also incur recurrent costs related to oversight of critical entities. It is assumed that every year, only a part of critical entities would be subject to scrutiny.

As regards the **operators**, the preferred option estimates that up to 5,000 critical entities could be concerned. This assumption is based on the number of operators identified

according to the NIS Directive, and on number of national critical infrastructures communicated by some Member States. Ultimately, Member States will also take into account the outcomes of national risk assessments to identify critical operators.

The estimated costs incurred by critical entities summarised in Annex 3 focus on the administrative costs and compliance of operators with the direct obligations. They do not estimate the additional investments that operators would carry out as a result of their resilience plans, as such investments would vary from company to company (depending on the size, the sectors, the risks they face, the measures they have in place already). In terms of recurrent administrative costs for businesses, these would relate to providing information to authorities in the context of oversight activities, and as part of the identification process (every three years on average).

8.2 REFIT (simplification and improved efficiency)

Per the Commission's Regulatory Fitness and Performance Programme (REFIT), all initiatives aimed at changing existing EU legislation should aim to simplify and deliver stated policy objectives more efficiently (i.e. by reducing unnecessary regulatory costs). The analysis of impacts suggests that the preferred option is anticipated to reduce the overall burden on Member States.

First of all, closer alignment with the services oriented approach of the NIS Directive are likely to lead to reduced compliance costs. For instance, the burdensome cross-border ECI designation process would be replaced with requirements to identify critical entities delivering essential services. Member States would be able to use as a basis the identification process set up for the current NIS Directive (which is in many cases aligned with the national identification process). This would reduce the burden on Member States.

While additional requirements would be imposed on individual operators, e.g. the development of operational resilience plans, the assumption is that, in most cases, a significant number of operators already have some form of security planning and thus would not incur any significant additional burden.

Moreover, the risk-based procedure for the identification of critical entities will ensure a targeted approach, so that the obligations are only imposed on operators considered as critical. Besides, the risk-based approach according to which the critical entities would decide on the resilience measures on the basis of specificities of their operations and of risk assessment, would mean that security investments will remain targeted and commensurate to the risks of every individual operator. (An in-depth analysis of anticipated one-off and recurring costs is provided in Annex III.)

It follows that the implementation of additional measures aimed at improving the resilience of CI operators would lead to a reduction in the overall number of disruptive events affecting negatively the provision of essential services to national and European markets. Ensuring more reliable provision of such services would have a positive impact on the overall health of the European economy, given the extent to which such services underpin essentially all business activities in the Union. In other words, the initiative would bring about an improved functioning of the internal market.

9 HOW WILL ACTUAL IMPACTS BE MONITORED AND EVALUATED?

The Commission should review the implementation of any (legislative or non-legislative) proposals on the resilience of CIs providing essential services with regard to the achievement of policy objectives identified in this Impact Assessment. A commitment to evaluating the impacts of a legislative act, if proposed, should be included in the draft text. This evaluation should be engaged 4 years after the deadline for implementation of the legislative act to ensure that there is a sufficiently long period to evaluate the effects of the initiative after it has been fully implemented across all Member States. It may include a public consultation and/or survey stakeholders to review the effect of the potential legislative act on the different categories of stakeholders.

In addition to that formal evaluation, the Commission will remain in close contact with the Member States and with the relevant stakeholders to monitor the effects of the new legislative act. The Commission Expert group that would replace the existing CIP PoC group, would be the most appropriate forum to exchange information with the Member States and to gather first-hand information and qualitative evidence on the activities to promote the resilience of CI operators delivering essential services. Qualitative evidence provided by competent authorities can be a cost effective yet informative way to illustrate the gaps that a possible legislative instrument would aim to cover. The Commission could also collect qualitative evidence from operators through workshops with EU and national associations as well as individual CI operators.

The Commission should also submit a report assessing the extent to which the Member States have taken the necessary measures in order to comply with the legislative act, 2 years after the deadline to implement it.

The table below summarizes the indicators proposed to monitor the achievement of policy objectives identified in this Impact Assessment. The specific objectives are the same ones as those proposed in section 4, whereas the operational objectives are linked to the preferred option described in section 8.

SPECIFIC OBJECTIVES	OPERATIONAL OBJECTIVES	INDICATORS	COLLECTION STRATEGY
Ensure higher level of	Increase the capacity of	Number of national and	Data reported to the

SPECIFIC OBJECTIVES	OPERATIONAL OBJECTIVES	INDICATORS	COLLECTION STRATEGY
understanding of risks and interdependencies, as well as the means to address them	Member States to perform a comprehensive assessment of CI risks and interdependencies.	sectoral risk assessments performed and types of risks and interdependencies covered.	Commission by Member State authorities. Discussions at the Commission Expert group.
	Increase the capacity of critical entities to assess the risks and interdependencies affecting their CI operations.	Number of risk assessments performed by operators and types of risks and interdependencies covered.	Workshops with operators.
Ensure that all relevant entities in all key sectors are identified as critical	Ensure a comprehensive sectoral scope of national CI resilience policies.	Number of essential services identified by Member States in each of the sectors.	Data reported to the Commission by Member State authorities.
	Ensure an appropriate level of identification of critical entities.	Number of critical entities identified by Member States in each of the sectors, on the basis of their criticality and identification criteria.	Data reported to the Commission by Member State authorities.
Ensure that the full spectrum of resilience activities is included in public policies and operational practice	Ensure that Member States mainstream resilience in their national policies.	Number of Member States having adopted a national strategy on resilience.	Data reported to the Commission by Member State authorities.
	Ensure that operators' security plans contain measures to ensure their resilience.	Number of resilience plans scrutinised by the authorities.	Data reported to the Commission by Member State authorities.
		Proportion of operators having incorporated resilience in their security culture.	Workshops with operators.
		Number of resilience plans assessed by European Resilience Advisors.	Reporting from European Resilience Advisors.
Strengthen capacities and improve cooperation and communication between stakeholders	Reinforce capacities of Member States authorities.	Capacity building activities involving Member States.	Report of activities of the Knowledge hub.
	Reinforce cooperation between public and private stakeholders and among operators.	Number of cooperation initiatives set up at national level and covering all relevant stakeholders.	Discussions at the Commission Expert Group.

ANNEX 1: PROCEDURAL INFORMATION

Lead DG, Decide Planning/CWP references

The lead DG is the Directorate-General for Migration and Home Affairs (DG HOME). The agenda planning reference is PLAN/2019/5448.

Organisation and timing

The Commission Work Programme for 2020 announced, under the heading "Promoting our European Way of Life - Fostering Europe's security", a legislative proposal for "additional measures for Critical Infrastructure Protection".

The Inception Impact Assessment was published on 19 June 2020.

The Inter-service Steering Group was set up by the Secretariat-General to assist in the preparation of the initiative. The representatives of the following Directorates General participated in the ISSG work: Legal Service, CNECT, JRC, TAXUD, DIGIT, CERT-EU, GROW, FISMA, SANTE, MARE, DEFIS, MOVE, ENER, ECHO, EEAS, NEAR, AGRI, BUDG, REFORM, ENV, TRADE, ESTAT, HR, JUST, CLIMA.

The last meeting of the Inter-Service Steering Group took place on 30 September 2020.

Consultation of the RSB

On 20 October 2020, the Directorate-General for Migration and Home Affairs submitted the draft Impact Assessment to the Regulatory Scrutiny Board, which examined the draft Impact Assessment on 18 November 2020. The Board issued a positive opinion with reservations. The comments made by the Board were addressed in the revised report. A succinct presentation of how the main finding of the Board were reflected in the revised report is presented below.

(1) The report does not sufficiently explain the risks related to critical infrastructure and the cross-border dimension: the revised report clarifies that the primary focus of the ECI Directive is on terrorist threats of a non-cyber nature, and the focus of the initiative on non-cyber risks. The cross-sectoral and cross-border interdependencies have been further exemplified, including in relation to the proposed legal basis.

(2) The report lacks a clear description of the link between this initiative and the NIS revision. It does not provide a clear justification for expanding the sectoral scope of the ECI and aligning it with that of the NIS Directive: the link with NIS revision has been clarified, and synergies explained (including the sectoral scope, entities in scope and cooperation mechanisms).

(3) The report is unclear on how it relates to sectoral legislation. It does not sufficiently address the risk of unclear requirements for operators and enforcement bodies: the

revised report clarifies the links with sectoral legislation It explains that the use of a *lex specialis* clause and the fact that the upcoming initiative builds on existing sectoral legislation with complementary objectives means that there are no risks of overlaps and unclear requirements for operators and enforcement bodies.

(4) The report is not clear about the criteria Member States will have to apply for the designation of European critical infrastructures. It does not explain their role in a) factoring in interdependencies and cross-border risks, b) in ensuring proportionality, while c) promoting greater coherence in the designation process across the EU: the revised report clarifies in the options section the criteria for identifying critical operators, and explains how national specificities would be taken into account using a risk-based identification process. The options description also clarifies the compliance oversight responsibility.

(5) The report does not sufficiently explain how the preferred option would lead to better national responses to cross-border risks. It remains unclear why this is a proportionate measure in view of the problems identified: the revised report clarifies how cooperation and coordination between the Member States would be facilitated cooperation between Member States; and explains better the choice of the preferred option and number of companies that are likely to be covered this option.

Evidence, sources and quality

As detailed in Annex 2, the Impact Assessment is based on a number of consultation activities that have taken place in recent years, both in the context of different studies launched by the Commission (e.g. the ECI Directive evaluation finalised in 2019, the 2020 feasibility study) and that have been carried out by the Commission independently. These consultations have been broad-based, targeting competent authorities in the Member States, CI operators and the European associations that represent their interests, academia, think tanks and members of the public (via a public consultation that was carried out to support the ECI Directive evaluation). However, taking into account the technicalities and specificities of the subject, the Commission has focused primarily on targeted consultations in preparing the Impact Assessment.

Some more recent examples of consultation include the collection of feedback on the Inception Impact Assessment, which sought views from all interested parties via the Commission's 'Have your say' portal, targeted stakeholder consultations with competent Member State authorities, CI operators, European industry associations and the members of the European Reference Network for Critical Infrastructure Protection (ERNCIP) using a combination of online surveys, questionnaires, virtual 'field visits' involving authorities and operators in ten Member States, consultative seminars, and bilateral exchanges as appropriate.

Taken together, the recent studies and consultations carried out by external consultants and the Commission independently have generated a substantial amount of data. However, given the sensitive nature of this policy area (as an example, the identities of specific ECIs are not known, as this information is considered as sensitive by Member States) and operators' reluctance to share information with potential market competition implications, much of this data is of a general, non-granular nature, but especially with regard to questions of costs/burdens. For this reason, the Impact Assessment relies on a qualitative methodology capable of accommodating quantitative measures and reflecting quantitative estimates from other sources. The cost estimates that are provided in the Impact Assessment are based on a combination of factors, including representative data on costs provided by certain Member States and operators.

ANNEX 2: STAKEHOLDER CONSULTATION

This annex provides a synopsis report of all stakeholder consultation activities undertaken in the context of this Impact Assessment.

2.1 Consultation strategy

The Commission has consulted broadly on aspects related to CI resilience in an EU context. The overall aim of the consultation activities was to collect relevant input from a wide range of stakeholders at both national and EU level to enable the preparation of an initiative on CI resilience. The consultations sought to collect inputs pertaining to:

- The effectiveness, efficiency, relevance, coherence and EU added value of the existing framework for CI protection;
- Problems related to the existing framework that stakeholders consider should be addressed in the initiative; and,
- Possible options to tackle the identified problems as well as their anticipated impact.

In preparing the initiative, including the Impact Assessment and draft proposal, Commission services carried out an initial mapping of **primary stakeholders**, which include: (i) competent Member States authorities; (ii) CI operators in different sectors; (iii) European industry associations and other industry stakeholders; (iv) subject-matter experts; (v) international organisations; (vi) academia and think-tank representatives; and (vii) members from the public, albeit to a limited extent.

Over the course of the consultation process, Commission services used a variety of **methods and forms of consultation**. These included:

- An opportunity for all interested parties to provide feedback on the Inception Impact Assessment via the Commission's 'Have your say' platform;
- A consultative seminar with competent Member State authorities, complemented by a targeted questionnaire that was circulated afterward;
- A consultative seminar with operators of critical infrastructures and accompanying targeted questionnaire; and,
- Numerous bilateral exchanges with Member States and operators.

Moreover, a series of **consultation activities** were carried out **as part of the feasibility study** that supported the development of this Impact Assessment. This study, which sought to explore 'the potential effects of different possible measures aimed at further enhancing the resilience of critical infrastructure in the EU', was commissioned by the Commission's Directorate-General for Migration and Home Affairs (DG HOME) and conducted by an external contractor. Besides a substantial desk research component, the study involved multiple consultation opportunities, including: an online survey targeting competent Member State authorities; a written questionnaire targeting competent

authorities and CI operators; structured interviews with all primary stakeholder categories (with the exception of members of the public); and virtual 'field visits' involving interviews with competent authorities and operators in a total of 10 Member States.

These consultation activities and brief summary of the outcomes are summarised in the next section. It should be noted that due to circumstances related to the Coronavirus pandemic, e.g. travel restrictions, limits on physical meetings, but also the fact that many stakeholders had a significant role to play in managing the crisis, the **format of some of the in-person consultation activities planned as part of the study and independently by the Commission had to be carried out using alternative means**, e.g. video teleconferencing, bilateral phone interviews, written questionnaires, etc.

All **feedback** received through the targeted consultations organised by Commission services was processed manually. This was feasible given the overall number of inputs that were received. The assessment of replies involved reading each consultation response in full and documenting viewpoints, including any issues and concerns that were raised. This feedback was then used as appropriate in conducting the Impact Assessment.

Given the particularly technical nature of the subject matter, Commission services chose to prioritise the collection of viewpoints from particularly relevant stakeholder groups. As such, **no public consultation was conducted** specifically for this Impact Assessment. This decision was made in light of the technical nature of the topic, meaning that members of the general public would be unlikely to see themselves being directly concerned by the issues addressed in the context of the consultations, e.g. specific measures on the part of competent authorities and operators. Furthermore, specific information depicting how critical infrastructures are protected or are resilient (e.g. security plans, continuity arrangements, etc.) are rarely if ever publicly available information. Without access to such information, it was assumed that individual citizens lacked the information necessary with which to contribute in a constructive way to any public consultation.

That being said, a twelve-week public consultation to support the evaluation of the ECI Directive was launched in November 2018 and concluded in February 2019. The public consultation yielded a total of 69 replies, only 20% of which were submitted by individuals (summarised in the Staff Working Document on the outcomes of the evaluation[131]). Similarly, only two individuals (out of a total of 37 contributors) provided feedback on the Inception Impact Assessment for this initiative (for more information see section 2.5 below). The limited participation of the public in consultations such as these

[131] SWD(2019) 308.

suggests a relatively limited public interest in this topic (which, again, may stem from its inherently technical nature). Nevertheless, all views expressed in the context of these earlier consultations have been accounted for in preparing this Impact Assessment.

2.2 Consultation activities and results

2.2.1 Consultation of competent Member State authorities via online survey

As part of the aforementioned external feasibility study, an online survey addressed to the Member States' Critical Infrastructure Protection Points-of-Contact (CIP PoCs) was administered using eSurvey tool provided by the contractor. The survey was conducted over the course of four weeks in January-February 2020. The **objective** of the survey was to generate an overview of the different approaches to CI resilience in the Member States and to identify potential areas for improvement. More specifically, the questions contained in the survey focused on:

- Current measures and initiatives related to CI resilience;
- The process for the identification and prioritisation of CI;
- Current and possible future threats to and vulnerabilities of CI;
- Threat assessment and risk assessment processes;
- Risk management, preparedness and consequence management processes;
- Processes for monitoring and evaluating relevant measures; and,
- The stakeholders involved in relevant processes, but also the nature/extent of public-private cooperation;

The survey was also an opportunity for the CIP PoCs and other competent authorities that chose to respond to the survey to provide their views as to the challenges/deficiencies that they see at national and/or EU level, and the need for further EU action.

Feedback received

A total of 24 Member States[132] responded to the questionnaire. The consultation revealed a number of key challenges, namely that: (i) threats are not sufficiently analysed and addressed; (ii) there is an insufficient emphasis on resilience and consequence management; (iii) stakeholders experience certain administrative and financial burdens and uncertainty from diverging obligations; (iv) there is insufficient cooperation and communication between stakeholders; (v) there are inadequate capacities and capabilities at authority and operator level to respond to disruptions effectively.

[132] AT, BE, BG, CZ, DE, DK, EE, EL, ES, FI, FR, HR, HU, IT, LT, LU, LV, NL, PL, PT, RO, SI, SE, SK.

2.2.2 Targeted written consultation of Member States and CI operators

As a follow-up to the online survey that was carried out in early 2020, the external contractor responsible for the feasibility study carried out in March-April 2020 a written consultation of both competent authorities and CI operators using a short, targeted questionnaire. These consultations replaced the consultative workshops with competent Member States authorities and CI operators that were originally planned for the end of March 2020.

The decision to replace the workshops with the written consultations was precipitated by developments related to COVID-19. The option of a short, targeted questionnaire was seen to provide stakeholders, many of whom were involved in managing the crisis, with maximum flexibility in being consulted. The contractor organised a brief virtual introduction to the questionnaire at the outset of the consultation period.

Even with the new format, the **objective** of the consultation remained the same, namely to collect information that would be useful in:

- Further articulating the baseline situation;
- Gaining a better understanding as to the relevance of the identified problems for different types of stakeholders; and,
- Identifying possible measures to address them and improve the EU approach to CI resilience.

Feedback received

A total of 12 Member States[133], 11 national CI operators and six European CI associations (from energy, transport, health, water, banking, financial services) provided responses to the questionnaire. The contributions broadly confirmed the problems/drivers identified in the survey of the Member States' CIP PoCs. The stakeholders' responses to the question focused on possible future measures were taken into account when drawing up an initial list of potential policy options/measures to enhance CI resilience.

2.2.3 In-depth interviews (virtual 'field visits')

Having carried out the online survey and targeted written consultations, the external contractor responsible for the feasibility study then conducted virtual 'field visits' in 10 Member States[134] in May-June 2020. Each 'field visit' involved in-depth interviews with, typically, two national competent authorities and three CI operators. These replaced the in-person field visits that were originally envisioned as part of the study.

[133] AT, DK, EL, ES, FR, HR, IT, LT, PL, PT, SE, SI.
[134] DE, EE, HR, IT, MT, NL, PL, PT, RO, SE.

The case study countries were selected on the basis of the following criteria: (i) size; (ii) geographical location; (iii) level of maturity of CI resilience framework before the ECI Directive; (iv) sectoral scope of the CI resilience framework; (v) exposure to natural and man-made risks; (vi) level of cybersecurity commitment of the Member State; (vii) the fact that Member States were not already the subject of a case study in the context of ECI Directive evaluation.

The **objective** of the field visit component of the study was to collect additional insights into possible policy measures over those already received through other consultation activities, and their anticipated implications at Member State and operator level.

Feedback received

A total of 42 stakeholders participated in the ten field visits, including 18 competent authorities and 24 operators (from energy, transport, health, water, telecommunications sectors). In preparation for each interview, every stakeholder received from the contractor a description of one specific problem along with its associated drivers and a preliminary list of potentially relevant policy measures (of different levels of ambition). The interviews served as an opportunity for stakeholders to provide feedback on these measures, but also to assess their likely impacts. These in-depth discussions allowed the contractor to 'fine-tune' its list of possible measures, which were then subject to further consultation with all relevant stakeholders, this time organised by the Commission (see below).

2.2.4 Consultative workshops

Working partially on the basis of the interim conclusions of the external contractor, the Commission services organised two additional consultation opportunities for competent authorities and CI operators, namely back-to-back virtual **consultative workshops with Member States representatives** on 29 June 2020 and with **CI operators and industry associations** on 30 June 2020. These workshops aimed to collect feedback on the policy options and measures that had been identified during previous stages of the consultations, and notably during the virtual field visits in the selected 10 Member States.

Feedback received

A total of 20 Member States[135] and 40 CI operators and industry associations (from energy, transport, health, water, financial markets, banking, digital and telecommunications sectors) participated in the two workshops. In anticipation of each workshop, participants were provided with a discussion paper that served to summarize the outcomes of the consultation activities to date as part of the feasibility study. For

[135] BE, CZ, DK, EE, ES, FI, FR, HU, LT, MT, NL, PL, PT, SE, SI, SK.

instance, the discussion paper provided an overview of the main problems/drivers and possible policy options and measures that had been identified by the external contractor. The outcomes of the workshops can be summarized as follows:

- The majority of both Member States and operators that provided feedback during the workshops highlighted the need for a more common approach across the EU with regard to **threat/risk assessments** using common definitions and methodologies in the interest of enhancing their comparability. They expressed the view that cross-sectoral **interdependencies** are currently not accounted for sufficiently, something that the then still-ongoing COVID-19 crisis amply demonstrated.
- There was overall agreement among competent authorities and operators concerning the need to ensure the **resilience** (including business continuity) **of essential service providers**, thereby moving away from the current protection-oriented approach. Some Member States nevertheless indicated their reluctance to regulate national critical infrastructures at EU level, especially if detailed requirements were to be imposed on national CIs.
- There was considerable support amongst Member States to expand the **sectoral scope** of the EU's approach in order to cover at least the seven sectors currently subject to regulation through the NIS Directive. Certain Member States suggested including the public administration and food sectors as well. Meanwhile, operators in specific sectors (water and health), appeared less supportive to an expansion of sectoral coverage.
- Several operators (e.g. in the water, energy and banking sectors) considered that sectoral legislation already provides for some common requirements (e.g. on risk assessments, security plans) and that any additional EU-level action would need to take this into account.
- A number of operators and industry associations highlighted the burden created by diverging national regimes, and in particular the reporting obligations imposed by different national authorities.
- Both MS and operators were in favor of **enhanced cooperation** between authorities and operators operating in different sectors. According to some MS, the CIP PoC group should play a crucial role in this at strategic level.
- Many Member States considered that the EU could support more **operational cooperation** by organising EU-level exercises and stress-tests of public and private capabilities, developing common training curricula and threat-identification tools, facilitating the exchange of best practices, etc. Many participants supported the idea of setting up a dedicated knowledge center within the Commission. Finally, several MS saw a need to better use and/or reinforce existing tools such as the CIP PoC group and CIWIN platform.
- A number of operators argued that the current range of support activities offered by the Commission's Joint Research Center (JRC) should continue.

Additional feedback from Member States

As a follow-up to the consultative workshop, 11 Member States provided additional written feedback, and several Member States provided input in bilateral conversations. This is summarised below:

- MS considered that the preferred means to achieve a **more common approach of assessment of risks/threats** is via the establishing of minimum criteria or methodologies (thereby allowing room for flexibility in approaches at national level) and enhanced cooperation. Many Member States expressed the need to carry out joint EU-level analyses, one of them pertaining specifically to pan-European services such as Galileo.
- As regards **interdependencies**, most Member States highlighted the need to assess interdependencies at every level (e.g. operator, national, EU). In the last case, at EU level, the respondents suggested that the JRC should have a role to play.
- Similarly, in order to achieve a shift in approach towards **resilience**, guidelines and/or definitions of baseline resilience criteria enabling national-level flexibility were suggested by most of the respondents. More prescriptive measures enjoyed less support. Furthermore, most responding Member States (9 out of 11) agreed that it would be useful to develop a **national resilience strategy** (where they do not already exist).
- As for the question of **sectoral coverage**, the written feedback saw some Member States propose that additional sectors besides those covered by the NIS Directive could be within the scope of any new initiative. Examples included agriculture, public safety, law enforcement, defense, and space. On the other hand, one Member State explicitly argued for excluding space.
- The majority of respondents voiced a clear interest as regards the need for measures to enhance the resilience of **pan-European services** such as Galileo and Eurocontrol (with one Member State also proposing the gas and electricity transmission networks for consideration).
- A clear majority of responding Member States (8 out of 11) were in favor of establishing baseline criteria to support the **designation of CIs providing essential services**. Meanwhile, certain Member States pointed out that the designation process is a national responsibility, and indicated that it is already largely in line with the NIS approach and sectors.
- Concerning the **synergies** between existing instruments, a number of Member States considered that moving towards an essential services approach would help to better ensure synergies, not least with the NIS Directive. Others pointed to the fact that synergies already exist at national level regarding the ECI Directive and NIS Directive, respectively, and that any further alignment of the two would not imply much additional burden.

- Most Member States supported the idea of creating a dedicated knowledge center within the Commission.

2.2.5 Inception Impact Assessment

The Inception Impact Assessment[136] was published for feedback by all interested parties on the Commission's 'Have your say' portal. Respondents were invited to provide online comments and, where appropriate, submit short position papers to provide more background to their views. The consultation period was seven weeks, starting on 19 June 2020. The feedback period was longer than what is usually applied by the Commission, due to the fact that no public consultation to support the development of the initiative was organised. It also reflected the rules set out in the adjusted 2020 Commission Work Programme.

Feedback received

A total of 37 contributions representing the entire stakeholder spectrum[137] were submitted over the seven-week feedback period. Of these, 28 were provided by **companies/business organisations**[138] and **business associations**[139] representing a range of sectors, including, most commonly, energy (electricity, gas, nuclear), followed by the digital (including cybersecurity), telecommunications, water, transport and chemical industry sectors.

Overall, these contributions suggested that the existing EU framework for CI resilience should be reviewed in light of increasing interdependencies, evolving risks, and cross-border challenges. Many contributions called for consistency between the reviews of the ECI Directive and the NIS Directive, respectively.

As regards questions of **sectoral scope**, views diverged. Where some stakeholders did not see the need to include any new sectors, others identified individual sectors like the information and digital infrastructures sector, and still others proposed considering all the sectors covered by the NIS Directive. The views on **policy options** also varied: with a clear preference for either the option that would clarify the provisions of the existing ECI Directive (Option 2 in the Impact Assessment), and for the option that would shift the focus towards the critical entities (Option 3). In any case, the stakeholders considered

[136] The Inception Impact Assessment and received feedback is available here.
[137] One association submitted the same input twice. It is counted only as one submission in the total of 37 replies. The contributions were registered from the Member States France, Norway, Belgium, Germany, Spain, Luxemburg, Spain, Italy, Ireland, Finland, Greece, Hungary, Italy, Portugal, and Sweden.
[138] FR, BE, ES, DE, HU, IT.
[139] DE, BE, FI.

that various 'soft' measures that encourage/facilitate cooperation (including between public and private entities), information-sharing, the exchange of good practice, and trainings should complement regulatory ones. Some stakeholders flagged the importance of accounting for the provisions contained in existing sectoral legislation, and favoured purely voluntary measures.

More specific suggestions were expressed by some of the sectoral representatives. For instance, one suggestion was that the electricity Distribution System Operators (DSO) in the *energy sector* should be considered to be CI, while another was for specifically the *nuclear sector* to be included in the CI protection approach. Other ideas included that the *water sector* be part of the assessment of cross-border interdependencies, and that the *cybersecurity industry* be considered a vital sector.

A limited number of contributions were received from **public authorities**[140]. These included: a local administration (calling for the need to consider digital infrastructures and water sector as critical); a national CIP PoC; and a CI operator (presumably designated as an ECI under the ECI Directive) expressing a preference for the combination of voluntary measures and new requirements focused on essential services.

Moreover, a number of **EU-funded projects Horizon 2020**[141] related to CI resilience against cyber, physical and hybrid threats in areas such as energy, maritime logistics, water infrastructures, first responders and financial services submitted their feedback (13 contributions). While the projects provided more general comments acknowledging the gaps in terms of risk assessment and addressing interdependencies, they also provided more technical input, proposing specific methodologies or technological solutions to be integrated into the new CI resilience framework. These more technical comments were disregarded insofar the proposal is technology-agnostic.

Other views were expressed by a **non-governmental organisation**[142] arguing that the ultra-high frequency (UHF)-band (terrestrial transmission frequency range) is a CI that need to be secured, while two **EU citizens**[143] argued for the importance of ensuring the protection of CIs against both physical and cyber threats.

[140] FR, BE, SE.
[141] Projects from PT, GR, FI, NO, FR, IT, and ES.
[142] LU.
[143] IE and IT.

2.2.6 Additional feedback

Meeting with Member State CIP PoCs

In September 2020, the Commission organised a meeting with the Member State CIP PoCs. Representatives for 24 Member States participated[144]. The **objective** of the meeting was to seek the views of Member States on specific elements of policy options assessed as part of the Impact Assessment.

A limited number of Member States intervened, typically to express their general support for a number of key aspects included in the regulatory policy options, notably:

- Additional opportunities for Member States to exercise oversight over operators (including their respective operator resilience plans);
- Putting in place arrangements to identify cross-border interdependencies and critical entities of European significance;
- Expanding the sectoral scope of the existing CI resilience legislation; and,
- Including the possibility for background checks of personnel exercising critical functions in more CI sectors (beyond aviation).

Member States also supported an approach bringing physical security and cybersecurity closer together.

Consultation of experts via ERNCIP network

The Commission services also sought views on different policy options from the various CI experts who are members of the European Reference Network for Critical Infrastructure Protection (ERNCIP). The written consultation was concluded on 1 October 2020. On the basis of the feedback that was received (three replies in total), ERNCIP members expressed a general preference for measures aimed at developing guidelines, strengthening relationships, promoting knowledge-sharing, establishing working groups, ensuring better coordination, and developing funding tools. There was a clear preference for non-binding measures accounting for sectoral differences.

2.3 Stakeholder participation

Stakeholders consulted included:

- EU institutions and agencies;
- international organisations;
- CIP PoCs in Member States;
- other authorities in the Member States;

[144] AT, BE, BG, CZ, DE, DK, EE, EL, ES, FI, FR, HR, HU, IT, LT, LU, LV, MT, NL, PL, PT, RO, SE, and SI.

- private entities (operators of CIs, business associations)
- academia / research entities /experts.

The feedback on the Inception Impact Assessment also included a limited number of responses from members of the public, and from a non-governmental organisation. This allowed collecting input from a wide variety of stakeholders, with different views and perspectives on the subject matter.

ANNEX 3: WHO IS AFFECTED AND HOW?

3.1 Practical implications of the initiative

The key obligations that will have to be fulfilled by Member States, entities and the European Commission are summarised below:

National authorities

- Develop/maintain national resilience strategies which should identify strategic objectives and set out appropriate policy and regulatory measures with a view to achieving a high level of CI resilience;
- Carry out regular risk assessments at national level encompassing, at a minimum, in the energy, transport, banking, financial market infrastructures, health, drinking water, waste water, digital infrastructure (including telecommunications), public administration, and space sectors;
- Develop/maintain procedures for identification of critical entities;
- Identify critical entities/update the list of critical entities in different sectors on a regular basis;
- Maintain oversight over the compliance of critical entities with standing requirements/obligations;
- Designate a single point-of-contact at national level responsible for CI resilience in order to facilitate cross-border cooperation;
- Develop/maintain national sectoral and cross-sectoral coordination/cooperation structures involving relevant public and private stakeholders;
- Develop/maintain national CI resilience competencies tasked with providing practical support to relevant public and private stakeholders, including operators;
- Regular reporting to the Commission on implementation;
- Participation in the identification, guidance and oversight of critical entities of European significance.

Critical entities

- Carry out regular risk assessments that can feed into other risk assessment processes, including ones at national level;
- Maintain an Operator Resilience Plan or equivalent, including provisions on risk reduction and preparedness, incident management and recovery. The Resilience plan[145] should describe arrangements concerning:
    - General preparedness measures;
    - Physical security, accounting for both traditional and emerging threats;
    - Employee security management; and

[145] The elements related to cybersecurity would be covered as part of the NIS Directive.

    - Business continuity plans.
- Designate a single point-of-contact for protection/resilience matters, linking the operator with other stakeholders, including MS competent authorities and other CI operators;
- Engage in capacity building activities, including staff education and training/awareness-raising; and
- Report incidents.

European Commission

- Set up of the Knowledge hub;
- Development of guidance materials, organisation of capacity building activities, conduct of risk assessments - as part of the Knowledge hub activities;
- Set up the process and participate in the identification, guidance and oversight of critical entities of European significance; and
- Organisation and coordination of Resilience advisory teams.

3.2 Summary of costs and benefits

The tables below summarise the costs and benefits for the preferred option, with respect to the baseline situation. Given the limitations created by the lack of available data, the tables have been filled to the extent possible:

I. Overview of Benefits (total for all provisions) – Preferred option (Policy Option 3)		
Description	***Amount***	***Comments***
Direct benefits		
Compliance cost reductions		Member States will benefit from reduced compliance costs since the burdensome designation process of ECIs would be replaced by a process aligned to the largest extent possible with the one set up for the NIS Directive (which in many cases is aligned with the national designation process).
Improved functioning of the internal market		The improved resilience of CI operators would reduce the number of disruptive events affecting essential services, making more stable and reliable the provision of those services to their customers, both citizens and companies. This would have an overall positive impact on the economy, given the key role of such services for all types of business activities, which would benefit from the uninterrupted provision of essential services, from electricity to drinking water.
Reinforced security		The increased protection and improved capacity of reaction of operators would reduce the number of incidents, and decrease the impact of current and anticipated future threats (such as terrorism or natural events). This would positively affect the security interests of Member States and reinforce the security of the society as a whole. Public authorities would therefore benefit from the stability derived from the smooth functioning of key economic activities and the constant provision of essential services to their citizens.

II. Overview of costs – Preferred option (Policy Option 3)[146]						
Measures	*Administrations*		*Businesses (critical entities)*		*Citizens/ Consumers*	
	One-off	*Recurrent*	*One-off*	*Recurrent*	*One-off*	*Recurrent*
Member States national strategy on resilience	Member States adopting 1st national strategy according to new requirements. In many instances, this will mean complementing already existing strategies with resilience elements and/or enlarging its sectoral coverage, meaning that some Member States will only have to adjust their existing strategies. ***EUR 1 million / EUR 1.25 million***	Member States updating their national strategies (every 3 years on average) ***EUR 0.65 million / EUR 0.80 million every three years***	None	None	None	None
Member States national risk assessments (incl. interdependencies)	Member States carrying out 1st national risk assessment (RA) according to new requirements. In many instances, this will mean adapting existing RA practices to include interdependencies as well as more sectors, meaning introducing adjustments to existing RA practices. ***EUR 2.9 million / EUR 3.3 million***	Member States updating national risk assessment (every 3 years on average) ***EUR 2 million / EUR 2.25 million***	Possible contribution of selected operators to national risk assessment (1st risk assessment according to new requirements). This will depend on whether MS will want to involve the operators. ***EUR 2.9 million / EUR 3.2 million*** (5 operators per sector per Member State)	Possible contribution of selected operators to national risk assessment (updates, every 3 years on average) ***EUR 1.8 million / EUR 2 million***	None	None
Identification process of critical entities	Member States identifying critical entities. This would involve collecting sector-specific information on operators to verify if thresholds in new legislative instrument are fulfilled, and nominating operators. The costs would be	Member States updating the identification of critical entities (every 3 years on average) ***EUR 0.4 million / EUR 0.5 million***	Participation in the designation process (consultation with MS) ***EUR 3.75 million / EUR 9 million*** [entities concerned: potentially 5.000 operators in 27 MS]	Reporting back to authorities if criteria for qualifying as critical operator of essential services is still fulfilled (every 3 years on average) ***EUR 1.9 million / EUR 3.2 million*** [entities concerned: potentially 5000	None	None

[146] Because of the sensitive nature of this policy area, it was difficult to obtain quantitative data from Member States and operators. These estimates have been made on the basis of the considerations outlined in the Impact Assessment and of partial estimates shared by some Member States. The costs in the table are aggregated for all Member States and all potentially concerned operators. The estimates consider that for 7 Member States, only some adjustments to existing national strategies/risk assessment practices are needed, and that for 20 Member States, additional efforts will be required. For identification process, the estimates are based on the assumption that 12 Member States already largely rely on the identification process established for the NIS Directive when identifying national CIs.

II. Overview of costs – Preferred option (Policy Option 3)[146]						
Measures	*Administrations*		*Businesses (critical entities)*		*Citizens/ Consumers*	
	One-off	*Recurrent*	*One-off*	*Recurrent*	*One-off*	*Recurrent*
	lower for those MS already using NIS identification process. ***EUR 0.75 million / EUR 1 million***			operators in 27 MS]		
Member States oversight of critical entities		When relevant and necessary, MS could request information from operators, and issue instructions. It is assumed that every year, only a part of identified operators would be asked to provide information on their resilience plans. It is also assumed that only a part of those providing information would be subject to detailed scrutiny/instructions by MS authority. ***EUR 3.2 million / EUR 3.5 million***		Operators providing information on their resilience plans to authorities. ***EUR 2.25 million / EUR 3.6 million*** [entities concerned: potentially 25% of 5000 operators in 27 MS per year asked to provide information on resilience plans. Of those, a small part would be asked for in-depth scrutiny]	None	None
Operators Resilience Plans and risk assessments		*[costs related to oversight - see above]*	Operators adopting 1st resilience plan and carrying out the risk assessment according to new requirements. In many instances, this will mean updating the existing security plans (to include business continuity and recovery measures and employee security management) and adjusting existing RA methodology. ***EUR 98 million / EUR 117 million***	Regular updates of Operators resilience plans and risk assessments ***EUR 37.5 million / EUR 72 million*** *[costs related to oversight - see above]*	[indirect transfer on consumer prices]	
Cooperation structures (incl. information exchange) and capacity support of authorities to operators	Member States setting up sectoral and cross-sectoral cooperation structures and providing support to operators. In many instances, this would entail adjusting existing mechanisms. ***EUR 3.6 million / EUR 4.2 million***	Member States running cooperation structures and providing support to operators. ***EUR 2.9 million / EUR 2.1 million***		Operators participating in cooperation structures ***EUR 4.5 million / EUR 7.2 million***	None	None
Identification, oversight and support to critical entities of	<u>European Commission:</u> - setting up process and participation in	<u>European Commission:</u> - participation in additional	*[Obligations of* critical entities of European significance *are the same as for* critical	*[Obligations of* critical entities of European significance *are the same as for* critical	None	None

II. Overview of costs – Preferred option (Policy Option 3)[146]						
Measures	*Administrations*		*Businesses (critical entities)*		*Citizens/ Consumers*	
	One-off	*Recurrent*	*One-off*	*Recurrent*	*One-off*	*Recurrent*
European significance	identification of critical entities of European significance with MS - organisation of Resilience advisory teams ***EUR 0.12 million / EUR 0.16 million*** Member States: - participation in identification of CE-ES with COM (identification of potential candidates, collecting/assessing information on potential CE-ES) ***EUR 0.5 million / EUR 0.7 million***	identifications (if new candidates for critical entities of European significance are identified); - guidance and oversight of identified CE-ES (together with MS) - day-to-day coordination of Resilience advisory teams ***EUR 0.21 million / EUR 0.27 million*** Member States: - participation in additional identifications (if new CE-ES candidates are identified); - guidance and oversight of identified CE-ES (together with the Commission) - Resilience advisors (support to critical entities, assessment of security measures in place) ***EUR 0.85 million / 1 million***	entities - *see above]*	entities - *see above]*		
Capacity building – EU knowledge hub	European Commission: Initial set-up of organisation ***EUR 0.16 million / EUR 0.21 million*** Member States: Provision of initial strategic direction to the knowledge hub at the inception phase ***EUR 0.4 million / EUR 0.5 million***	European Commission: Development of guidance materials, organisation of capacity building activities, conduct of risk assessments, etc. ***EUR 0.5 million / EUR 0.7 million*** Member States: Voluntary participation in capacity building activities, risk assessments, etc. ***EUR 0.8 million / EUR 1 million***	None	Voluntary participation in capacity building activities (assuming about one tenth of identified operators would participate annually) ***EUR 1.5 million / EUR 2.7 million***	None	None

ANNEX 4: A DYNAMIC, OPERATIONAL CONTEXT FOR CI OPERATORS

Chapter 2 of the Impact Assessment argues that the problem to be addressed is that CI operators are not adequately equipped to address different types of disruptions to the provision of essential services now and which are anticipated in the future. In this annex, the intention is to describe the challenges inherent in the dynamic operational environment in which CI operators find themselves in now and in the years to come.

An evolving threat spectrum

Since the EPCIP was adopted in 2006, the threat picture facing critical infrastructures in Europe has changed in significant ways that pose new challenges to not least operators. The recent feasibility study highlighted a number of threats that competent authorities, operators and other stakeholders have identified as being of particular concern. One such threat is **cyberattacks**[147] orchestrated by many different actors targeting systems, networks, but also individual computer devices. Such incidents continue to be of considerable concern to stakeholders, especially where they disrupt, directly or indirectly, critical infrastructure operations, many of which are heavily reliant on digital infrastructure.[148] According to the European Union Agency for Cybersecurity (ENISA), the incidents of cyberattacks in Europe is on the rise, and many of these have a significant impact on both CI operations and their ability to deliver essential services.[149]

Meanwhile, the challenges posed by **natural hazards**, including ones like extreme weather events (EWEs), exacerbated by climate change, continue to grow, with certain sectors like energy, transport, ICT and water supply and distribution being particularly susceptible.[150] Such hazards, many of which are closely interrelated, include windstorms, storm surges, riverine and flash floods, sea level rise, forest and brush fires, heat waves, droughts and seismic events resulting in earthquakes and tsunamis, for instance. Further afield, space weather events, including solar storms, are also of concern. The 2009 heatwave and drought in France exemplifies how individual hazards can have far-reaching implications across multiple sectors. In this case, a scarcity of cooling water for nuclear power stations led to a decrease in energy production across the country, which in turn had ripple effects across other sectors.[151] Besides having operational consequences, such events also have significant economic implications for governments, operators and citizens. For instance, according to one estimate, the damage to critical

[147] Addressed by the NIS Directive.
[148] Study into the potential effects of different possible measures, 2020.
[149] ENISA Threat Landscape Report 2018 (link)
[150] Study into the potential effects of different possible measures, 2020.
[151] Linnerud, K., T.K. Midesa, and G.S. Eskeland. "The Impact of Climate Change on Nuclear Power Supply." *The Energy Journal*. 2011 (32.1). See also Operating Experience with Nuclear Power Stations in Member States in 2003. IAEA, 2004.

infrastructures in Europe could total as much as EUR 34 billion on a per annum basis by the end of the century.[152]

Meanwhile, **terrorist acts** carried out by a range of groups, including jihadist, right- and left-wing extremist organisations, but also lone actors continues to pose a serious threat to critical infrastructure operations in many different sectors.[153] While elements of the transport sector are by their nature particularly vulnerable to attacks,[154] reports suggest that other sectors are increasingly at risk. These include, for instance, the energy, water supply and distribution, chemical manufacturing, and telecommunications sectors.[155] In the last instance, for example, telecommunications operators in Europe and globally continue to see attacks on mobile infrastructure, which have been blamed by certain groups for the spread of the current Coronavirus.[156] However, besides terrorism, critical infrastructure operators must confront **other forms of criminality** that are just as or potentially even more disruptive than terrorism, including (cyber-)ransom attempts,[157] theft of essential components (e.g. copper wiring necessary for energy and transport operations), espionage, sabotage, etc. While such incidents certainly involve lone individuals and organised criminal networks, they can also be state-sponsored.

Operators must also contend with the risk for **insider threats**, which involve the exploitation of privileged access to sensitive information and/or facilities by staff for what are in most cases malicious ends. Insider threats can take many forms, including, for instance, the theft of sensitive information, the implantation of harmful code into ICT systems, or sabotage, which in 2014 led to the shutdown of a Belgian nuclear power facility.[158] Events showing the persistent risk of insider threats have taken place in the last few years both inside the EU[159] and in third countries[160]. This problem is clearly recognised by many Member State authorities and points to, among other things, the

[152] COM(2018) 738: 2, based on Forzieri et al. "Escalating impacts of climate extremes on critical infrastructures in Europe." *Global Environmental Change*. 2018 (48): 97-107. See also OECD, 2019: 19.

[153] EU Terrorism Situation & Trend Report (TE-SAT). Europol, 2020 (link); Open Source Report: Terrorist threats on critical infrastructures. EUINTCEN, April 2020.

[154] Hedel, et al. "Assessment of the European Programme for Critical Infrastructure Protection in the surface transport sector." *International Journal of Critical Infrastructures* 2018 (14.4): 311-335.

[155] OECD, 2019.

[156] Politico.eu, 2020 (link).

[157] INTERPOL, 2020 (link). See also OECD, 2019: 29.

[158] Abele-Wigert, I. and Dunn, M. International CIIP Handbook 2006: An Inventory of 20 National and 6 International Critical Information Infrastructure Protection Policies, Zurich: Center for Security Studies, ETH, 2006 (1).

[159] For instance, in 2018, at least four investigations were underway in different EU Member States involving radicalised individuals with links to terrorist organisations working at different airports. The following year, two investigations were launched involving radicalised railway employees arrested on terrorism charges. The same year, law enforcement authorities arrested a radicalised teacher for providing material support to ISIS, but also sensitive school security procedures to ISIS handlers. Elsewhere, a civilian employee at police headquarters in Paris attacked and killed four police officers.

[160] In December 2019, a radicalised Saudi air force officer undergoing training at a US military base with ties to Al-Qaeda on the Arabian Peninsula (AQAP) killed three US service members. Earlier, in February 2016, two airport workers allegedly helped facilitate the placement of an explosive device on a commercial aircraft departing out of Somalia's Mogadishu airport. In 2015, a Russian railway employee confessed to plotting an attack on a commuter train.

need for adequate vetting procedures and internal risk reduction measures (e.g. restricting the use of personal computer devices on internal networks).[161]

The ongoing Coronavirus pandemic points to the potential that **pandemics and other public health emergencies** have to disrupt and/or entail heavy strains on critical infrastructure operations in many different sectors, including, obviously, public health, as well as transport, energy, food supply, and telecommunications all of which have come into increasing demand while at the same time facing continued risk of workplace absenteeism among critical staff. Furthermore, events such as these, which create pressing global needs for specific kinds of materials, such as personal protective equipment (PPE) and medical supplies, point to the need for established and effective coordination mechanisms across sectors and countries.

Operators must also contend with the eventuality for **accidents** (e.g. fires, spills, structural collapse, workplace incidents caused by any number of factors (e.g. insufficient maintenance/upkeep, negligence, sheer bad luck, etc.).[162] Such accidents, many of which may initially appear minor, have the potential to lead to sustained shutdowns affecting operations on a system-wide basis, for instance where supply chains are concerned. Furthermore, they can also pose a serious risk to life where dangerous, potentially volatile materials are involved, as the August 2020 Beirut harbour explosions demonstrate. The likelihood for accidents, but also the disruptive effects of other types of incidents, including natural and man-made antagonistic ones, may be exacerbated where aging infrastructure is involved.[163]

Recent years have seen an increase in **hybrid actions** on the part of state and non-state actors, defined by the Commission and European External Action Service as the mixture of coercive and subversive activity, conventional and unconventional methods (i.e. diplomatic, military, economic, technological), which can be used in a coordinated manner by state or non-state actors to achieve specific objectives while remaining below the threshold of formally declared warfare.[164] In some cases, these actions seek to disrupt critical infrastructure operations, either by instigating incidents (e.g. cyberattacks, terrorist attacks) or, more typically, exploiting existing ones (e.g. a pandemic) in ways that threaten the provision of essential services and, in the process, undermine public trust and confidence in key societal actors, functions and/or institutions.[165] The extent to which hybrid threats are recognised by Member States has grown considerably since the

[161] Study into the potential effects of different possible measures, 2020. See also Gouglidis, et al. Threat awareness for critical infrastructures resilience. 8th International Workshop on Resilient Networks Design and Modelling (RNDM), 2016, and Bunn, M., and S. Sagan. Insider Threats. New York: Cornell, 2016.
[162] Study into the potential effects of different possible measures, 2020: 26.
[163] OECD, 2019: 13.
[164] JOIN/2016/018.
[165] Hybrid Threats and Vulnerabilities of Modern Critical Infrastructure – Weapons of Mass Disturbance. Hybrid Centre of Excellence, 2019.

mid-2000s.[166] This growing awareness could be attributed to real-world events, including ones in the Ukraine starting in 2014. These events demonstrated that a combination of physical attacks (sabotage) and cyberattacks on infrastructures coupled with a concerted, large-scale disinformation campaign could cause serious damage to the economy and undermine political stability.[167]

Technological innovations

Critical infrastructures, not least critical information infrastructures (CIIs) are today reliant on many different advanced technologies to function. Fast-paced **technological innovations**, many of which (e.g. 5G, artificial intelligence (AI) and machine learning, unmanned vehicles, including cars and drones, etc.) hold forth the promise of even greater efficiencies by achieving improved connectivity, remote monitoring, scalability, reliability, and cost reductions in the years to come. However, the push for smarter infrastructures and smarter cities tied together through an Internet of Things (IoT) also has risk implications that need to be accounted for.[168] The first type of risk is for unintentional disruptions caused by the introduction of new, potentially incompatible technologies into existing systems, such as industrial control systems (ICS), including Supervisory Control and Data Acquisition (SCADA) systems. A second is where such systems, which could potentially be non-European in origin, exacerbate existing or create new vulnerabilities that can be exploited by antagonists, i.e. they increase the infrastructure's 'target surface'. One such example pertains to the use of GNSS systems in not least the energy, transport, telecommunications and banking sectors for position/location data and timing/synchronisation services. However, as essential as they are, recent episodes have shown that they can be disrupted through radio frequency interference (RFI), prompting serious disruptions.[169] Still another type of risk is where malicious – in many cases non-attributable – actors exploit these and other new technologies to target operations from the outside, one obvious example being the routine, potentially dangerous and economically costly disruption of flight operations at major European airports using drones.[170] The challenge for Member States and operators is to keep pace with ongoing technological advances, understand how they might alter the risk profile of critical infrastructures, and then develop appropriate security solutions in response.

Increasingly complex, but also fragmented networks

[166] Study into the potential effects of different possible measures, 2020.
[167] JOIN/2016/018.
[168] Fiott, D. and R. Parkes. Protecting Europe – The EU's response to hybrid threats. European Union Institute for Security Studies, 2019 (151); Simon, T. Critical Infrastructure and the Internet of Things. Global Commission on Internet Governance, 2017 (46).
[169] Wildemeersch, M. and J. Fortuny-Guasch, Radio Frequency Interference Impact Assessment on Global Navigation Satellite Systems. Joint Research Centre, 2010.
[170] Study into the potential effects of different possible measures, 2020. See also Associated Press, 2020 (link); The Independent, 2020 (link).

Be it within and between individual critical infrastructure sectors, networks have grown increasingly complex, but also more fragmented since the start of the new century. This is due to two closely interrelated trends: the one towards the increased **privatisation** of the provision of essential services and the other towards **globalisation**. In the first case, the move toward a more liberal economic order starting in the 1980s and intensifying in the decade that followed saw many critical infrastructure operations handed off to private entities.[171] These, in turn, would come to rely on subcontractors to support their operations.[172] This makes today for a more complex and in many cases diffuse management/oversight regime in the Member States that is potentially less redundant and resilient than previously. The privatisation of European critical infrastructures has enabled foreign non-European entities to become involved in and, in some cases, exert varying degrees of control over the same. Such involvement can take many forms, ranging from involvement in research and innovation cooperation to venture capital funding to the supply of critical materials, components and systems, services, including maintenance services, and/or expertise to outright ownership and operational control over day-to-day operations.[173] The effect of this is to reduce European control over infrastructures situated in and essential to Europe, but also potentially to allow third countries to exert political influence in Europe.[174] It is clear that Europe's strategic autonomy is a matter of concern for Member States[175] and is something that has been addressed by the European Commission, not least through the adoption of the Foreign Directive Investment (FDI) Regulation.[176]

Growing interdependencies

From a strictly operational standpoint, critical infrastructures, both in Europe and further afield, are increasingly interconnected and reliant upon one another. The more complex these interdependencies, the more infrastructure in disparate (and at first glance seemingly peripheral) sectors might be considered critical. In such an instance, the risk for so-called cascading (or ripple) effects across sectors and Member States is real. Recent examples from within Europe abound. For example, in early 2019, a widespread

[171] The GFCE-MERIDIAN Good Practice Guide on Critical Information Infrastructure Protection for governmental policy-makers. GFCE and Meridian, 2017; Newlove-Eriksson, et al. The Invisible Hand? Critical Information Infrastructures, Commercialisation and National Security, *The International Spectator*. 2018 (53:2): 124-140.

[172] For a concrete example of where outsourcing creates specific security vulnerabilities, see Newlove-Eriksson, et al., 2018.

[173] Fiott and Parkes, 2019; Finon, D. and C. Locatelli. "Russian and European gas interdependence - Can market forces balance out geopolitics?" Laboratoire d'Economie de la Production et de l'Intégration Internationale. 2007: 1-36; RWR Advisory Group. A Transactional Risk Profile of Huawei. 2018; EPRS. 5G in the EU and Chinese telecoms suppliers. 2019; Study into the potential effects of different possible measures, 2020.

[174] Korteweg, R. "Energy as a tool of foreign policy of authoritarian states, in particular Russia". European Parliament, 2018; Holz, et al. European Natural Gas Infrastructure: The role of Gazprom in European natural gas supplies. DIW Berlin, 2014.

[175] Study into the potential effects of different possible measures, 2020.

[176] Fiott and Parkes, 2019; Regulation 2019/452 establishing a framework for the screening of foreign direct investments into the Union; Report on the implementation of the 2016 Joint Framework on countering hybrid threats and the 2018 Joint Communication on increasing resilience and bolstering capabilities to address hybrid threats. Joint Staff Working Document, SWD(2019) 200.

telecommunications outage affecting large parts of the Netherlands crippled emergency services and rendered police and other government services unreachable.[177] In October of the same year, a power outage in Estonia led to serious disruptions to motor fuel supply, telecommunications, drinking water and hospital operations.[178] Still later the same year, a fault in the Malta-Sicily interconnector resulted in a sustained power outage on Malta, which took several months to finally resolve.[179] Finally, the ongoing Coronavirus pandemic illustrates the extent to which a pandemic can have immediate and lasting ripple effects across many different sectors in Europe and the world, not least transport, telecommunications, and food supply.[180]

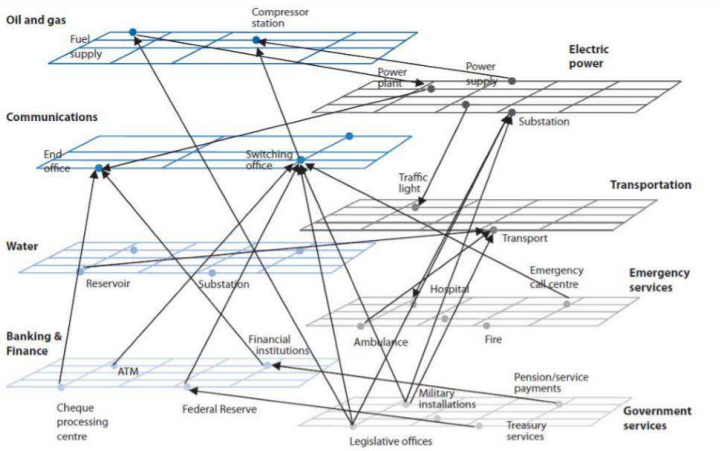
However, a number of longstanding strategic trends – digitalisation, privatisation, globalisation – serve to make the situation even more complex. For instance, a single ICT provider might support key operators in multiple sectors in many different Member State; a transport operator might rely on ten sub-contractors, some based in other Member States, to operate a facility; a power plant might be owned by a concern based in a third country. In other words, critical infrastructures are increasingly bound up together in a web of public and private connections across Member States, but also with third countries around the world.[181] Crucially, the recent feasibility study suggests that interdependencies such as these are often not mapped in the Member States nor considered in the context of national risk assessments. This implies that the potential adverse impacts of cascading effects over sectoral and national borders are in many cases likely to go unanticipated.

[177] CNN.com, 2019 (link).
[178] Eesti Rahvusringhääling, 2019 (link).
[179] Times of Malta, 2019 (link). See also Plietzch, et al. "Local vs global redundancy – trade-offs between resilience against cascading failures and frequency stability". *The European Physical Journal*. 2016 (225): 551–68.
[180] Revamping Crisis Resilience and Security in the Post-Pandemic World. Royal United Services Institute and the Swedish Civil Contingencies Agency (MSB), 2020 (link).
[181] De Bruijne, M. and M. Van Eeten, M. "Systems that Should Have Failed: Critical Infrastructure Protection in an Institutionally Fragmented Environment". *Journal of Contingencies and Crisis Management*. 2007 (15.1): 18-19.

ANNEX 5: MOVING FROM THREAT PROTECTION TO RISK-BASED RESILIENCE

Whereas historically the focus of efforts to ensure robust critical infrastructure operations has been on, as the name implies, critical infrastructure *protection* – preventing disruptions (largely caused by outside forces) from happening in the first place – the focus of the options put forward in the context of the Impact Assessment is instead on critical infrastructure *resilience*, i.e. the ability for critical infrastructures to resist, absorb, accommodate to and recover from incidents and/or conditions that have the potential to result in significant functional disruptions. In other words, the notion of resilience includes but is hardly limited to the task of preventing infrastructure operations from being disrupted.

This shift from protection to resilience is something that has been underway for some time, and is manifested to different extents in the thinking and approaches of different EU initiatives, Member States, operators and scholars. When compared to protection, resilience arguably constitutes a more realistic view on the limits of control in a modern world bound together by dense networks of systems and sectors subject to considerable uncertainty thanks to a dynamic operational environment. In this deeply interconnected world, disruptions in one sector may be felt, potentially severely, in others. Here, recognising the risk for and implications of so-called cascading effects within and across sectors is essential. The illustration below shows the generic interdependencies between utilities and networks in a given system. The implications in the event of cascading effects from one sector to another in such a system are obvious.

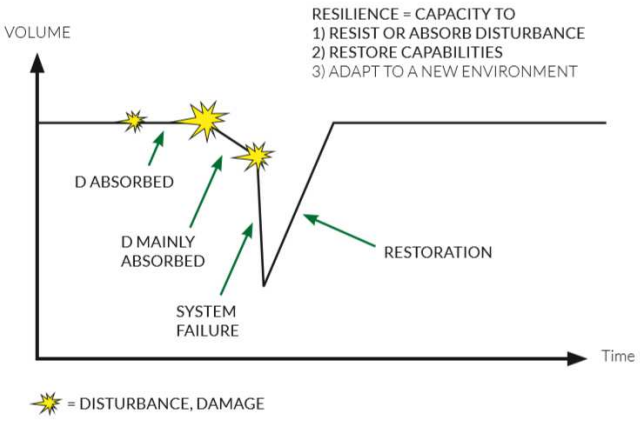


Source: National Association of Regulatory Utility Commissioners[182]

Whereas the notion of protection assumes that (all) disruptions can be prevented, resilience is arguably more reflective of the reality (that this will not always be possible),

[182] National Association of Regulatory Utility Commissioners), (2005), Technical Assistance Brief on Critical Infrastructure Protection "Utility and Network Interdependencies: What State Regulators Need to Know", US, available at www.naruc.org/Publications/CIP_Interdependencies_2.pdf in OECD, 2019: 22.

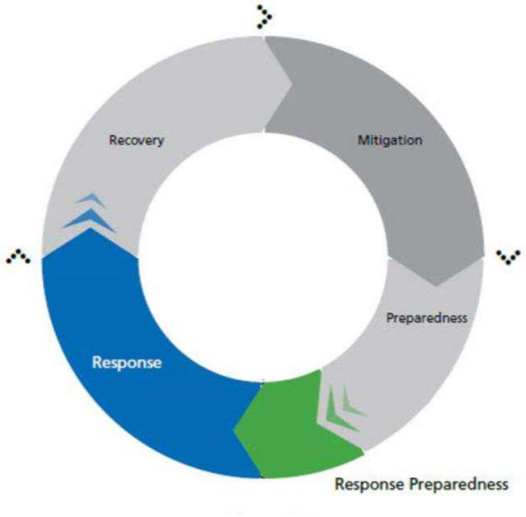
but also connotes a greater degree of proactivity. From the perspective of the proponents of resilience, most, but not all, disruptions can be avoided. Where they are not, arrangements are needed to ensure that infrastructures are able to absorb, accommodate to, and recover from them. The illustration below illustrates this point:



Source: Linkov, 2019[183]

Resilience also entails recognising that the post-disruption environment may not be identical to the one that existed previously. This points to the fact that critical infrastructure resilience should be approached in the same way that disaster responses (depicted below) typically are, namely in cyclical fashion – in responding to disruptions, organisations and individuals (hopefully) learn to prepare better for the next event. In other words, effective critical infrastructure resilience involves measures before, during and after a disruption.

[183] Linkov, Igor; Trump, Benjamin: The Science and Practice of Resilience. Washington 2019 (Springer) Nemr, Christina and Gangware, William: Weapons of Mass-Distraction - Foreign State-Sponsored Disinformation in the Digital Age. 2019 Park Advisors.



Source: Humanitarianresponse.info[184]

Furthermore, the approach being put forward here is one that is all-hazards, meaning that it accounts for the totality of a dangerous phenomenon, substance, human activity or conditions that may cause loss of life, injury or other health impacts, property damage, loss of livelihoods and services, social and economic disruption, or environment damage that CI operations are potentially threatened by. It follows then that it is threat-agnostic and thus, future-proofed, meaning it should be equally relevant now and in fifty years' time.

Finally, it is one that is squarely focused on *risk*, defined as the combination of the likelihood of the occurrence of a *threat* or *hazard*[185] and its negative consequences, which can be ameliorated or exacerbated by many different factors, not least the nature and character of critical infrastructures and their operations, which, when taken together, create a certain degree of *vulnerability*.[186] In order to gauge the risk profile of a given infrastructure or system of infrastructures, authorities and operators employ risk assessment methodologies. By way of analysing potential threats and hazards and inherent vulnerabilities, it is possible to gauge overall risk and, on this basis, prescribe appropriate improvements in response where necessary.[187]

---

[184] https://www.humanitarianresponse.info/sites/www.humanitarianresponse.info/files/documents/files/Pacific_EPREP_2013.pdf

[185] The term hazard, which is sometimes used interchangeably with threat, connotes a dangerous phenomenon, substance, human activity or conditions that may cause loss of life, injury or other health impacts, property damage, loss of livelihoods and services, social and economic disruption, or environment damage, according to the United Nations International Strategy for Disaster Reduction (UNISDR) (now the UN Office for Disaster Risk Reduction (UNDRR)) (https://www.unisdr.org/files/7817_UNISDRTerminologyEnglish.pdf).

[186] According to COM (2006) 787, a vulnerability is a characteristic of an element of the CI's design, implementation, or operation that renders it susceptible to disruption or destruction by a threat and includes dependencies on other types of infrastructure.

[187] United Nations International Strategy for Disaster Reduction (UNISDR) (now the UN Office for Disaster Risk Reduction (UNDRR)) (https://www.unisdr.org/files/7817_UNISDRTerminologyEnglish.pdf).

ANNEX 6: OVERVIEW OF NATIONAL POLICIES, RELEVANT EU INITIATIVES AND INTERNATIONAL FRAMEWORKS

The resilience of critical infrastructures and essential services in the European Union is the object of a wide set of policies at EU and national level, with different approaches and scope. This section aims at providing a snapshot of the relevant legislative landscape, which sets the framework for the development of this Impact Assessment. In a nutshell, this landscape can be summarised as follows:

- National critical infrastructure protection/resilience policies
- EU cross-sectoral legislative instruments (including the ECI Directive, the NIS Directive, the Union Civil Protection Mechanism, and the Foreign Direct Investments Regulation)
- Sectoral pieces of EU legislation relevant for the protection of critical infrastructures.
- Obligations/guidance set out by other international organisations, including NATO,[188] the Organisation for Economic Cooperation and Development (OECD),[189] different entities/initiatives within the United Nations system,[190] and standards bodies.

First of all, it is worth presenting the main features of national policies specifically aimed at the resilience of critical infrastructures and essential services. Several Member States already had a CI resilience policy prior to the adoption of the ECI Directive in 2008, some of which were revised or reinforced in view of such development at European scale; other Member States only developed a CI resilience framework following the adoption of the ECI Directive.

Such frameworks are generally wider in scope than the ECI Directive, both as regards the sectors and the geographical relevance of the infrastructures covered. In relation to the sectoral scope, almost all national CI resilience frameworks go beyond Energy and Transport and most cover areas such as banking and financial market infrastructure; health; drinking water supply and distribution; and digital infrastructure and

[188] NATO has identified seven 'Baseline Requirements' for national resilience that Allies, including many EU Member States, are expected to adhere to. These Baseline Requirements, along with supporting tools, including Resilience Guidelines and Evaluation Criteria, were updated in June 2020.

[189] The OECD's Framework on the Governance of Infrastructure issued in 2017 identifies infrastructure resilience as one of the key governance challenges, and has since undertaken a number of activities aimed at supporting Member States in this regard.

[190] A wide range of initiatives with bearing on critical infrastructure resilience have been taken by different UN bodies in recent years. Noteworthy examples include, for instance: UN Security Council Resolution 2341 calling on Member States to take steps to protect critical infrastructures from terrorist attacks; the UN Global Counterterrorism Coordination Compact, which includes a dedicated CIP working group; the UN Sustainable Development Goals; the UN Framework Convention on Climate Change; and the Sendai Framework for Action, which is implemented by the UN Office for Disaster Risk Reduction (UNDRR). The International Standards Organisation (ISO), meanwhile, sets out various standards that many critical infrastructure operators adhere to.

telecommunications. In relation to its geographical relevance, national policies address infrastructures located in the territory of the Member State, irrespectively of such infrastructures having a cross-border dimension. The aim is to ensure a high level of protection and/or resilience of the infrastructures underpinning vital societal functions within that Member State.

While there are differences among these national frameworks, the main elements of such policies can be summarised as follows:

- The determination of those **sectors** that are deemed vital for the State, for society and for the economy.
- The **identification and designation of critical infrastructures** and/or essential services. While there is generally one entity within the government coordinating such work (generally Ministries of Interior, the Ministries responsible for Civil Protection, or bodies attached to the Prime Minister's office), there are several other Ministries usually involved in this process, notably sectoral ministries such as Transport, Energy, Health, etc. Public authorities usually carry out a consultation of relevant operators in order to designate critical infrastructures.
- An important element for guiding the **authorities**' definition of critical sectors and infrastructures is the **assessment of risks** facing critical infrastructures. Some countries carry out comprehensive risk assessments for all critical infrastructures, others only for specific sectors.
- The **development of guidance and advice tools** by public authorities aimed at steering the work of the operators of critical infrastructures/essential services. Such tools provide operators with indications related to topics such as the main threats, the elements to take into account when operators assess their specific risks and when they decide on the measures to protect their infrastructures. The type of advice and the level of detail of the guidance varies among Member States.
- Taking into account this guidance, **operators** are expected to **assess the risks** and take the most appropriate security measures. Generally speaking, CI resilience policies are not prescriptive as to the specific security measures that operators have to put in place. Operators decide so on their own, usually in the form of a **Security Plan**. This plan generally outlines the threats and risks analysed and the measures taken to address those risks, including the organisation set-up and human resources allocated to these tasks. In some but not all Member States, CI resilience authorities have the **power to review** these plans and to require additional measures if they consider it necessary.
- Most Member States have established risk of unclear provisions **cooperation mechanisms** between the operators and the relevant authorities. This includes the designation by the operator of a point-of-contact (usually the person tasked with developing security policies within the company) to act as the interface between

the organization and the public authority or other operators. Other channels to promote cooperation and exchange of information, between the authorities and operators as well as among operators themselves, are workshops and meetings, national programs to ensure good public-private partnerships or specific bodies set up to coordinate public and private actors concerned by CI resilience measures.

These steps at national level are reflected in the **ECI Directive**, which consists of two main elements. First of all, the requirement for Member States to identify and designate critical infrastructures with a cross-border dimension (ECIs) in the Transport and Energy sectors. Secondly, a set of requirements to ensure a common assessment as to the need to identify their security needs.

Regarding the **designation of ECIs**, the Directive provides criteria that Member States should take into account to identify potential ECIs: the impact in terms of casualties, economic effects and public effects such as the impact on public confidence or the disruption of daily life (Article 3). While providing such general factors, the Directive gives Member States a margin of discretion to determine the thresholds that would establish whether the impacts of a disruption of an infrastructure are significant enough to be considered as critical. Once identified the potential ECIs, the Directive establishes a framework for national authorities to consult with other Member States that may be impacted by the disruption of a critical infrastructure, and for the Member State where the infrastructure is located to designate it as an ECI following the agreement of the consulted Member States (Article 4). The Directive requires Member States to inform the Commission about the number of infrastructures identified and ultimately designated as ECIs, without disclosing the identities of such infrastructures.

Regarding the obligations for **operators**, the main requirement established by the Directive is for them to develop a **security plan** identifying the assets to be protected and the solutions to be applied. The Directive requires operators to follow a procedure to develop this plan which includes carrying out a **risk analysis** and provides with an indicative list of the types of counter-measures to be applied. The Directive requires Member States to ensure that operators of ECIs have such a plan and review it regularly, without establishing any power or obligation for national authorities to approve or modify the plans.

Other provisions in the Directive relate to threat assessment, cooperation and exchange of information. Article 7 requires Member States to carry out a **threat assessment** in those subsections where an ECI has been designated and to report generic data to the Commission about such threat assessment - without establishing any minimum requirements as to the content of such analyses. Article 6 requires ECI operators to designate a **Security Liaison Officer** that acts as a point-of-contact between the operator and national authorities, while Article 10 obligates Member States to designate an ECIP

point-of-contact to coordinate with the Commission and other Member States. Finally, Article 8 establishes a general obligation for the Commission to support Member States and ECI operators.

A similar logic to the one of the ECI Directive, albeit much more developed, is applied by the **NIS Directive**. The NIS Directive is at the same time narrower and broader than the ECI Directive. On the one hand, it is more limited in terms of **material scope**: it is focused on the security of network and information systems only and on cyber threats. Therefore, it does not address the security of other elements of critical infrastructures and does not explicitly address physical threats. On the other hand, the NIS Directive is much **broader in terms of sectoral scope**, covering not only the Energy and Transport sectors, but also banking, financial market infrastructures, health, drinking water supply and distribution as well as digital infrastructure. At the same time, even in the sectors covered by the ECI Directive, the NIS Directive is more comprehensive as to the types of entities included, e.g. for electricity the ECI Directive only includes electricity producers and transmission system operators, while NIS also includes distribution system operators. The NIS Directive is also broader than the ECI Directive as if focuses on ensuring secure provision of the **essential services** (rather than the individual infrastructures underpinning those services), and requires Member States to identify operators of those services without imposing an explicit obligation to assess whether their disruption would have a cross-border impact.

Considering these important differences, the NIS Directive establishes an approach to the **identification** of operators of essential services similar to the one of the ECI Directive for the designation of ECIs. Member States are obliged to identify operators of essential services in the sectors in scope of the Directive and to inform the Commission about the number of operators identified. Like the ECI Directive, the NIS Directive establishes the **criteria** to take into account in order to designate those services. While being more extensive in terms of criteria, there is also flexibility for Member States to determine their own thresholds.

In terms of **substantive provisions**, the NIS Directive goes a step further than the ECI Directive in many respects, both as regards requirements on Member States and on operators. Unlike the ECI Directive, the NIS Directive requires Member States to adopt a **national strategy**, which includes a risk assessment plan. In addition to the designation of a point-of-contact, the NIS Directive goes further by requiring Member States to provide sufficient resources to the competent authorities, including overseeing the compliance of operators. Furthermore, the Directive establishes a strong **support ecosystem** to assist the work of operators by creating the computer security incident response teams (CSIRTs) and through the role of ENISA providing expertise and advice to Member States in building national capabilities.

In respect of the operators of essential services, the NIS Directive obligates them not only to take measures to manage the risks related to the security of network and information systems but also to prevent and minimise the impact of incidents and to ensure the continuity of their services. Thus it goes beyond the protection focus of the ECI Directive to also cover resilience. Operators of essential services are also required to notify significant incidents to competent authorities.

In addition to the ECI and the NIS Directives, two other cross-sectoral pieces of EU legislation are relevant in the context of critical infrastructure protection. First, the Union's **Civil Protection Mechanism** aims at strengthening cooperation between the EU Member States in the field of civil protection, with a view to improve prevention, preparedness and response to disasters. While it contains elements which are relevant for the current analysis, such as the requirements for Member States to develop risk assessments and to develop their capabilities and planning to manage disasters, it is important to note the difference in scope and links between Civil Protection and Critical Infrastructure Protection.

Civil Protection is the combination of measures and capabilities of national authorities to prevent, prepare and to respond to disasters with the objective of protecting primarily people against their adverse impact. Critical Infrastructures themselves can be impacted by a disaster and require the intervention from civil protection authorities. However, CI resilience covers other incidents where civil protection authorities would not necessarily intervene and especially, it focuses on the specific measures that the operators of those infrastructures have to put in place to protect them and to ensure their functioning in the event of an incident, including those where civil protection authorities would not necessarily intervene.

Second, the **Foreign Direct Investments Regulation** (2019/452) which, without requiring Member States to screen foreign investments, provides for a number of requirements that Member States should take into account when they put in place a screening process, and provides criteria for determining if a foreign investments affects security. It covers a number of areas, including "critical infrastructure, whether physical or virtual, including energy, transport, water, health, communications, media, data processing or storage, aerospace, defence, electoral or financial infrastructure, and sensitive facilities, as well as land and real estate crucial for the use of such infrastructure".

Besides these cross-sectoral legislative instruments relating to the security of critical infrastructures in more than one area, there are a number of **EU sectoral legislation** specific to a given sector aimed at ensuring a high degree of security or containing security-related provisions which are relevant from a CI resilience-perspective. While a full list of relevant EU instruments is presented at the end of this section, the following

table analyses the most relevant ones against the main parameters of CI resilience policies:

- the scope in terms of threats addressed;
- the extent to which interdependencies are taken into account;
- the identification of critical infrastructures or essential services;
- the role of public authorities in:
    - setting a strategy and
    - analysing risks,
- the obligations of operators in terms of:
    - assessment of risks,
    - security measures and
    - incident reporting.

Overall the analysis below indicates that in most sectoral legislation the EU has established requirements that are relevant for the protection of critical infrastructures, but also points out a number of insufficiencies or gaps. First of all, not all instruments address all threats relevant from a CI resilience perspective. The instruments have different approaches, some being more focused on protection, others addressing mainly business continuity and resilience aspects, and a limited number of instruments covering both. Some legislation only sets obligations for Member States but not to operators. Furthermore, some elements of CI resilience policies such as risk assessments are not addressed or the EU legislative instruments do not provide a clear indication as to what should these contain or how should these be carried out. Finally, except for one, none of the legislative instruments analysed establish a process to prioritise the operators which are critical to the functioning of essential services in a given sector and which should receive further support, guidance and scrutiny from public authorities. Precisely this support from authorities specialised in security to economic operators is an element that is generally missing from most of the legislative instruments in scope.

Provisions	**Sectoral policy coverage**
Hazards in scope	*Energy* - The Electricity Risk-Preparedness Regulation covers "all relevant risks". - The Security of Gas Supply Regulation covers "all relevant risk factors", explicitly mentioning "natural disasters, technological, commercial, social, political and other risks". *Transport* - The Civil Aviation Security Regulation focuses on acts of unlawful interference that jeopardise the security of

	civil aviation (but not other types of intentional threats as well as unintentional threats). - The Ship and Port Facility Security Regulation is limited to intentional unlawful acts. - While the Directive on Ports Security covers "possible threats to the assets and infrastructure", the focus is on man-made intentional threats (e.g. point 17 of annex I specifically refers to "security concerns, such as 'suspect' cargo, luggage, bunker, provisions or persons, unknown parcels, known dangers (e.g. bomb)." *Banking and financial market infrastructures* - The Payment Services Directive generally refers to "operational and security risks". - The ECB SIPS Regulation refers to "the range of risks that arise or are borne by the SIPS". - The DORA proposal is focused on ICT risks, defined as risks "in relation to the use of network and information systems", including any "type of malicious or non-malicious event", that may compromise the security of such ICT systems, related tools and processes, or the institutions' operations and the provision of services and which may end up causing, among others, "a damage to physical ICT infrastructure". *Health* - The Decision on cross-border serious threats to health covers threats of biological (communicable diseases, antimicrobial resistance, biotoxins or other harmful biological agents), chemical, environmental or unknown origin. *Drinking water supply and distribution* - The Drinking Water Directive is focused on "the adverse effects of any contamination of water". *Digital infrastructures* - This sector is only covered by the NIS Directive, which is explained above. *Space*

	- While the Space Programme 2021-2027 Proposal refers to ensuring "the security of the components of the Programme" (i.e. Galileo, EGNOS, Copernicus, SST and GOVSATCOM), the focus is "particularly against physical- and cyberattacks". *Telecommunications* - The Electronic Communications Code makes a general reference to "risks posed to the security of networks and services".
Designation of critical operators	*Banking and financial market infrastructures* - The ECB SIPS Regulation is the only legislative instrument besides the ECI and NIS Directive establishing a process for designating the critical operators, i.e. the Systematically Important Payment Systems or SIPs. The designation criteria include the market share, volume of payments, cross-border activities or the use by other financial institutions.
National strategies related to the protection/resilience of infrastructures or services	*Energy* - The Electricity Risk-Preparedness Regulation requires Member States to establish a risk-preparedness plan which "shall set out all national measures that are planned or taken to prevent, prepare for and mitigate electricity crises". - The Security of Gas Supply Regulation requires national authorities to establish "a preventive action plan containing the measures needed to remove or mitigate the risks identified" and "an emergency plan containing the measures to be taken to remove or mitigate the impact of a disruption of gas supply". - The Minimum Oil Stocks Directive is limited to requiring Member States to "have contingency plans to be implemented in the event of a major supply disruption", i.e. it is limited to business continuity. *Transport* - The Civil Aviation Security Regulation requires Member States to "draw up, apply and maintain a national civil aviation security programme". - The EU Rail Security Action Plan invites Member States to establish a "programme for rail security

	management at national level". - The Ship and Port Facility Security Regulation requires Member States to adopt national programmes for the implementation of the Regulation. *Health* - Member States have to provide information about their national preparedness and response planning, including a "description of the business continuity plans, measures or arrangements aimed at ensuring the continuous delivery of critical services and products". No requirements related to national protection/resilience strategies existing in the following sectors: drinking water supply and distribution (although the Drinking Water Directive requires Member States to establish monitoring programmes to check that water intended for human consumption meets the requirements of the Directive); space; and telecommunications.
Assessment of risks and interdependencies by authorities	*Energy* - The Electricity Risk-Preparedness Regulation requires authorities to "ensure that all relevant risks relating to security of electricity supply are assessed" and to "identify the most relevant national electricity crisis scenarios". This instrument also tasks ENTSO-E with identifying "regional electricity crisis scenarios" and to develop a "methodology for identifying regional electricity crisis scenarios". - The Security of Gas Supply Regulation requires Member States to make a national risk assessment and tasks ENTSOG with carrying out "a Union-wide simulation of gas supply and infrastructure disruption scenarios". *Transport* - The Civil Aviation Security Regulation (300/2008) only refers to risk assessment when Member States want "apply more stringent measures than the common basic standards" (Art 6) or when they want to deviate from the common basic standards contained in the Regulation (Art 4). Besides this, the Regulation refers to Annex 17 to the Convention on International Civil

	Aviation, which sets international standards and recommendations and includes also obligations on implementation of international security measures, including risk assessments. - Furthermore, the Commission Implementing Decision (2015/8005) laying down detailed measures for the implementation of this Regulation establishes requirements to carry out risk assessments for different types of security controls, in the majority of cases to be carried out or approved by national authorities. - In addition to the requirements in legislation, which establishes the mandate for Union Risk assessments (reference to high risk cargo), the European Commission has played a facilitating role in the development of EU risk assessments in the field of aviation for the benefit of Member States and to ensure that new aviation security measures are developed on the basis of common EU approach. - The Ship and Port Facility Security Regulation and the Directive on Port Security require Member States to ensure that port facility and port security assessments are carried out and to approve them. - The EU Rail Security Action Plan implicitly invites Member States to carry out an "analysis and assessment of risk" when developing their "programme for rail security management". The EU Rail Security Platform has developed a risk-assessment methodology to assist Member States. *Health* - The Decision on cross-border serious threats to health does not establish requirements on national risk assessment but tasks the Commission with "risk assessment of the potential severity of the threat to public health, including possible public health measures" upon certain conditions. *Drinking water supply and distribution* - While the Drinking Water Directive points to a risk-based approach, the only explicit reference to risk assessment is limited to the situation where Member States want to derogate from the requirements on

	parameters and sampling frequencies (part C annex II). No requirements related to national risk assessments in the following sectors: banking and financial market infrastructures[191]; telecommunications. There are no requirements on assessing interdependencies in any sectoral legislation except for the reference in the Electricity of Supply Regulation for ENTSO-E to consider "the risks of disruption of gas supply in the context of identifying the risks".
Assessment of risks and interdependencies by operators	*Energy* - Acquis in the energy sector requires to adopt an all-hazards risk-based approach in gas and electricity. Moreover, annexes to Security of Gas Supply Regulation and the risk preparedness Regulation indicate what the risk assessment/risk preparedness plans should cover. *Transport* - Although it is not directly spelled out in the Civil Aviation Security Regulation, the airports and all other entities involved in aviation (except air carriers) are expected, as part of their security programme, to include risk assessment procedures. - The Ship and Port Facility Security Regulation requires operators to carry out a port facility security assessment, i.e. a risk analysis of all aspects of a port facility's operation in order to determine which part(s) of it are more susceptible, and/or more likely, to be the subject of attack. - The Directive on Port Security requires operators to carry out a port security assessment. - Reference to "an analysis and assessment of risk" by railway undertakings in the EU Rail Security Action Plan, as the basis for their security management plan (see below).

[191] While no requirements on national risk assessments have been identified in the legislation analysed relating to the banking and financial sector, the EU has introduced a specific supervisory architecture at EU level which includes the monitoring of risks. The three regulatory authorities thereby established carries out regular assessment of risks from a financial perspective (https://eba.europa.eu/risk-analysis-and-data/risk-assessment-reports)

	Banking and financial market infrastructures - The Payment Services Directive requires payment service providers to submit at least once a year an "updated and comprehensive assessment of the operational and security risks". - The ECB SIPS Regulation requires SIPS to "identify specific scenarios that may prevent it from being able to provide these critical operations and services". - The DORA Regulation requires financial entities to identify all sources of ICT risk, in particular the risk exposure to and from other financial entities on a continuous basis, and to assess cyber threats and ICT vulnerabilities. *Space* - The Space Programme 2021-2027 Proposal requires the entity responsible for the management of a component of the Programme to "carry out risk and threat analysis". Besides these explicit requirements on operators to perform risk assessments, many of the policy documents analysed in the health, drinking water supply and distribution, and telecommunications sectors implicitly require operators to adopt a risk-based approach, without providing any clear mandate or no indication of the elements to be covered or the methodology to be applied. The only reference to assessment of interdependencies by operators is the requirement for SIPS to "review the material risks the SIPS bears from and poses to other (financial) entities (…) as a result of interdependencies".
Operators plans and measures to ensure protection and/or resilience	*Transport* - The Civil Aviation Security Regulation and its Implementing Regulation, besides establishing a detailed list of protection measures, require airports, air carriers and entities to have a security programme, to be submitted to the appropriate authorities for approval (EU inspectors also verify that the content includes the require security programme parameters). In addition, operators are also obliged to implement their own quality control programmes and report on

	their monitoring activities to national authorities. - The Ship and Port Facility Security Regulation requires port facilities to have a security plan. - The Directive on Ports Security requires ports to have a security plan. - The EU Rail Security Action Plan invites Member States to "require railway undertakings and infrastructure and station managers to adopt a security management plan at company level". *Banking and financial market infrastructures* - In addition to submitting a security policy document when applying for the authorisation to provide payment services, the Payment Services Directive requires that financial institutions "establish a framework with appropriate mitigation measures and control mechanisms to manage the operational and security risks". - The ECB SIPS Regulation requires SIPS to establish a "robust framework with appropriate systems, policies, procedures and controls to identify, monitor and manage operational risk". - The DORA Regulation requires financial entities to have in place an ICT risk management framework to address ICT risks, including a digital resilience strategy setting out how the framework is implemented, and to put in place a comprehensive ICT Business Continuity Policy. *Telecommunications* - The Electronic Communications Code requires "providers of public electronic communications networks or of publicly available electronic communications services take appropriate and proportionate technical and organisational measures to appropriately manage the risks posed to the security of networks and services" *Space* - The Space Programme 2021-2027 Proposal requires the entity responsible for the management of a component of the Programme carry out "all the necessary activities to ensure and monitor the security

	of that component". No obligations on operators to have a security plan exist in the following sectors: energy; health; and drinking water supply and distribution.
Reporting on incidents	*Energy* - The Electricity Risk-Preparedness Regulation establishes provisions for Member States to issue early warning in the event of electricity crises, to inform the Commission about a crisis, including its causes and the measures to take, and to provide an ex-post evaluation at the latest 3 months after a crisis. Similar requirements apply for the gas sector. *Transport* - Annex III of the Ship and Port Facility Security Regulation requires port facility security plans to detail reporting procedures to the appropriate contact points. - Annex II of the Directive on Ports Security requires port security plans to set out incident reporting to authorities. *Banking and financial market infrastructures* - The Payment Services Directive requires payments institutions to notify the competent authority in their home Member State "in the case of a major operational or security incident." - The DORA Regulation requires financial entities to report major ICT-related incidents to the relevant competent authority –determined according to the type of financial entity by different legislative instruments. *Telecommunications* - The Electronic Communications Code requires operators to "notify without undue delay the competent authority of a security incident that has had a significant impact on the operation of networks or services". There are no provisions for incident reporting in reviewed policy documents in the following sectors: health (the Decision on cross-border serious threats to health has established an early warning and response system, but this is limited to the Commission and competent authorities, thus not

	regulating incident notification by operators); drinking water supply and distribution; or space.

The following is a list of EU-level sectoral and cross-sectoral legislation and initiatives that have been accounted for as part of the analysis in the context of the Impact Assessment.

Sectoral initiatives

Energy

- Electricity
  - Regulation (EU) 2019/941 on risk-preparedness in the electricity sector
  - Regulation 714/2009 on conditions for access to the network for cross-border exchanges in electricity
  - Regulation (EU) 2019/943 on the internal market for electricity
- Gas
  - Regulation 2017/1938 concerning measures to safeguard the security of gas supply (Gas Supply Regulation)
- Petroleum
  - Directive 2009/119 imposing an obligation on Member States to maintain minimum stocks of crude oil and/or petroleum products

Transport

- General
  - Regulation 1315/2013 on Union guidelines for the development of the trans-European transport network
- Aviation
  - Regulation 300/2008 on common rules in the field of civil aviation security
  - Regulation 2015/1998 laying down detailed measures for the implementation of the common basic standards on aviation security
  - Commission Implementing Regulation (EU) 2019/103 amending Implementing Regulation (EU) 2015/1998 as regards clarification, harmonisation and simplification as well as strengthening of certain specific aviation security measures
- Maritime
  - Directive 2005/65/EC on enhancing port security
  - Regulation 725/2004 on enhancing ship and port facility security
- Rail
  - Directive 2016/798 on railway safety, accompanied by Delegated Regulation 2018/762 establishing common safety methods on safety management system requirements
  - EU Rail Security Action Plan, COM(2018) 470 Annex

Banking/financial market infrastructures

- Regulation 600/2014 on markets in financial instruments
- Directive 2014/65 on markets in financial instruments

- Regulation 909/2014 on improving securities settlement in the European Union and on central securities depositories
- Directive 2015/2366 on payment services in the internal market
- Directive 2013/36 on access to the activity of credit institutions and the prudential supervision of credit institutions and investment firms
- Regulation 575/2013 on prudential requirements for credit institutions and investment firms
- Regulation 462/2013 - see Regulation (EC) No 1060/2009 of the European Parliament and of the Council of 16 September 2009 on credit rating agencies - consolidated version.
- Directive 2015/2366 on payment services in the internal market
- Regulation of the European Central Bank 795/2014 of 3 July 2014 on oversight requirements for systemically important payment systems (ECB/2014/28).
- Digital Operational Resilience Framework for financial services

Health

- Decision 1082/2013 on serious cross-border threats to health

Drinking water supply and distribution

- Council Directive 98/83/EC of 3 November 1998 on the quality of water intended for human consumption
- Commission Directive (EU) 2015/1787 amending Annexes II and III to Council Directive 98/83 on the quality of water intended for human consumption
- Council Directive 98/83/EC of 3 November 1998 on the quality of water intended for human consumption (Drinking Water Directive) (currently under evaluation as a follow-up of the European Citizens' Initiative (ECI) Right2Water)

Telecommunications

- Directive (EU) 2018/1972 of 11 December 2018 establishing the European Electronic Communications Code

Space

- Decision 541/2014 establishing a Framework for Space Surveillance and Tracking Support
- Regulation 1285/2013 on the implementation and exploitation of European satellite navigation systems (Galileo Regulation)
- Council Decision 2014/496/CFSP on aspects of the deployment, operation and use of the European Global Navigation Satellite System affecting the security of the European Union
- Regulation 377/2014 establishing the Copernicus Programme and repealing Regulation 911/2010

Cross-cutting legislation

Digital infrastructure

- Directive 2016/1148 concerning measures for a high common level of security of network and information systems across the Union (the NIS Directive)

Civil protection

- Decision (EU) 2019/420 on a Union Civil Protection Mechanism (UCPM)

Environment (including in a marine context), including climate adaptation

- EU Adaptation Strategy (COM (2013) 216), including the development of guidelines of climate proofing
- Directive 2012/18 on the control of major-accident hazards involving dangerous substances (Seveso III)
- Directive 2007/60 on the assessment and management of flood risks (Flood Directive)
- Directive 2000/60 establishing a framework for Community action in the field of water policy (Water Framework Directive)
- Directive 2006/118 on the protection of groundwater against pollution and deterioration (Groundwater Directive)
- Directive 2008/56 establishing a framework for community action in the field of marine environmental policy (Marine Strategy Framework Directive)

Foreign direct investment

- Regulation 2019/452 establishing a framework for the screening of foreign direct investments into the Union

Hybrid threats

Joint Framework on countering hybrid threats a European Union response (2016)

ANNEX 7: OVERVIEW OF THE POLICY OPTIONS

- **Main problem:** Critical Infrastructure operators are not adequately equipped to address current and future risks that may result in disruptions to the provision of essential services

- **General objective:** To establish harmonised minimum rules to enable and ensure the provision of essential service in the internal market by enhancing the resilience of critical infrastructure operators

The table below summarises the 4 policy options considered and their links with the problem drivers and specific objectives.

Problem drivers	Specific objectives	Option 1	Option 2	Option 3	Option 4[192]
Driver 1: Risk assessment requirements are not comprehensive and do not account for complex interdependencies	**SO 1:** Ensure higher level of understanding of risks and interdependencies, as well as the means to address them	Commission threat updates/reports to support risk assessments. Structured dialogue between Member States, Commission and as relevant operators and experts. Topical discussions and exchange of practices/guidelines.	Risk assessments requirements: - at national level by Member States, covering all ECIs on the territory - at operators level for individual ECIs	Risk assessments requirements: - at national level by Member States, covering at least all sectors in scope - at operators level for the risks to the provision of their services.	Risk assessments on the basis of binding methodologies.
Driver 2: Diverging sectoral coverage and designation criteria	**SO 2:** Ensure that all relevant entities in all key sectors are identified as critical	Structured dialogue/topical discussions and exchange of practices/guidelines with the aim to facilitate more common approaches in national policies.	Sectoral scope expanded beyond energy and transport, to include banking, financial market infrastructures, health sector, drinking water supply and distribution, digital infrastructure	Sectoral scope expanded beyond energy and transport, to include banking, financial market infrastructures, health sector, drinking water, waste water, digital infrastructure	Designation process: - thresholds defined for cross-cutting criteria Commission/Agency

[192] Option 4 includes all elements outlined in Option 3. The table only presents the elements that are in addition to Option 3.

Problem drivers	Specific objectives	Option 1	Option 2	Option 3	Option 4[192]
			(current NIS sectors). <u>Designation process of ECIs updated:</u> -existing cross-cutting criteria refined, new criteria added (e.g. the extent of interdependency with other sectors, the number of users). -Member States to consult with other concerned Member States/operators -Member States to report back to Commission on application of criteria **→ choice of critical infrastructures by Member States, on the basis of process involving other concerned MS**	(including telecommunications), public administration, and space sectors. <u>Identification process of critical entities:</u> - existing cross-cutting criteria refined, new criteria added (e.g. the extent of interdependency with other sectors, the number of users). - Member States to apply criteria, in combination with results of national risk assessments **→ choice of critical operators of services by Member States**	role in identification together with Member States
Driver 3: Critical infrastructure resilience policies and approaches are divergent at different levels and between sectors	**SO 3:** Ensure that the full spectrum of resilience activities is included in public policies and operational practice	Structured dialogue/topical discussions and exchange of practices/guidelines with the aim to facilitate more common approaches in national policies.	<u>Operators Resilience plans</u> to also include business continuity and recovery arrangements, and arrangements on employee security. Focus on resilience of individual infrastructures. <u>Oversight</u> role by Member States over designated ECIs.	<u>National strategy</u> on CI resilience. <u>Operators Resilience plans</u> to also include business continuity and recovery arrangements, and arrangements on employee security. Focus on resilience of services.	<u>Oversight role</u> by Member States, supported by EU Agency.

Problem drivers	Specific objectives	Option 1	Option 2	Option 3	Option 4[192]
				Oversight role by Member States over identified operators - possibility for Member States to require information and issue instructions to operators as relevant. Role of Commission together with Member States on identification, support and oversight of critical entities of European significance	
Driver 4: Uneven capacities and limited exchange of information	**SO 4:** Strengthen capacities and improve cooperation and communication between stakeholders	Structured dialogue/topical discussions and exchange of practices/guidelines with the aim to facilitate more common approaches in national policies. Improved CIWIN platform.	- Provision facilitating sharing of sensitive data. - Strengthened cooperation between Member States and operators of ECIs. - Requirement on Member States to ensure appropriate capacities. - Commission support to Member States and designated ECIs.	- Cooperation structures by Member States - Points of Contact designated by Member States and operators. - Requirement on MS to ensure appropriate capacities. - Commission support / knowledge hub. - Existing CIP-PoCs group replaced by a formal Commission expert group. - European Resilience Advisors.	Dedicated EU Agency to support Member States and operators.