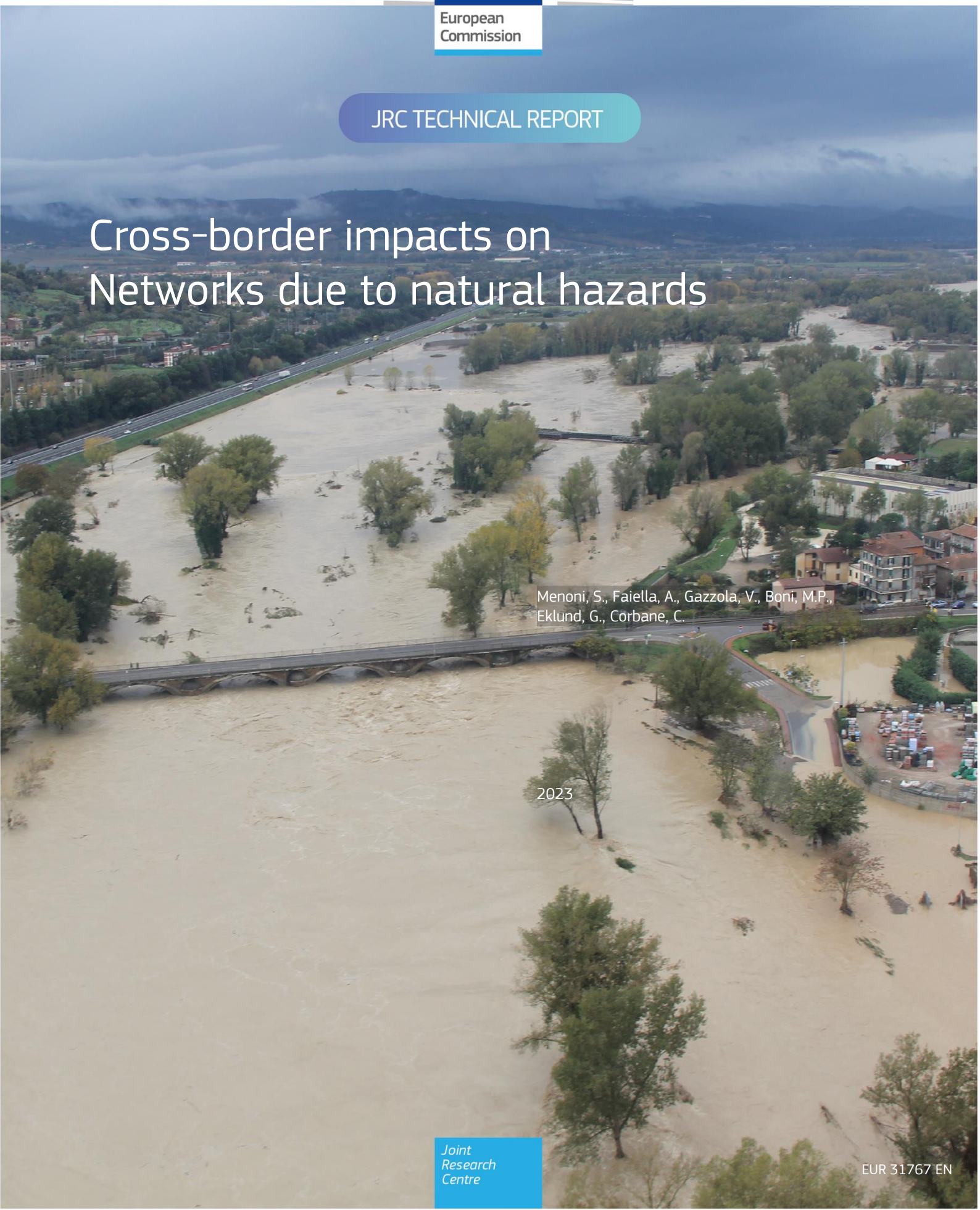
ISSN 1831-9424

European Commission

JRC TECHNICAL REPORT

Cross-border impacts on Networks due to natural hazards



Menoni, S., Faiella, A., Gazzola, V., Boni, M.P., Eklund, G., Corbane, C.

2023

Joint Research Centre

EUR 31767 EN

Contact information
Name: Christina Corbane
Email: Christina.Corbane@ec.europa.eu

EU Science Hub
https://joint-research-centre.ec.europa.eu

JRC133171

EUR 31767 EN

PDF ISBN 978-92-68-10083-7 ISSN 1831-9424 doi:10.2760/414289 KJ-NA-31-767-EN-N

Luxembourg: Publications Office of the European Union, 2023

How to cite this report: Menoni, S., Faiella, A., Gazzola, V., Boni, M.P., Eklund, G. and Corban, C., *Cross-border impacts on Networks due to natural hazards*, Publications Office of the European Union, Luxembourg, 2023, doi:10.2760/414289, JRC133171.

Contents

Abstract 1

Acknowledgements 2

1 Introduction 3

1.1 Objective and scope of this report 3

1.1.1 Definitions 3

1.2 The evolution of European Policies on Critical Infrastructures in the last two decades 5

1.3 Structure of this report 6

2 Defining cross-border impacts on networks providing essential services 8

2.1 Defining impacts 8

2.2 The cross-border dimension of impacts 8

2.3 Networks' systemic vulnerabilities: types of interdependencies 12

2.4 Nature of interdependencies among impacts occurring on networks providing essential services 13

2.4.1 Cascading 13

2.4.2 Cross-sectoral 15

2.4.3 Domino 15

2.4.4 Escalating 15

2.5 List of case studies of events/hazards with cross-boundary impacts on networks providing essential services. 15

3 Risk and resilience assessment and management frameworks for networks providing essential services 26

3.1. Risk assessment frameworks and requirements to apply them to cross-border impacts on networks providing essential services 26

3.2. Methods to enhance the Resilience and Operational Continuity of cross-border essential services 26

3.3. Good practices of cross-border cooperation 36

3.3.1. An international case: the USA and Canada collaboration 37

3.3.2. The Nordic collaboration model 37

3.3.3. Cross-border police collaboration in Europe 38

3.3.4. The Euregio Meuse-Rhine Incident Control and Crisis Management interservice collaboration 38

3.3.5. The cross-border collaboration between Italy and Switzerland 38

4. Expected future developments 40

4.1. Future developments from a conceptual/technical perspective 40

4.2. Needed changes from a risk governance perspective 43

4.2.1. Setting up a multi-sector governance structure for critical infrastructure resilience 43

4.2.2. Understanding complex (inter-)dependencies and vulnerabilities across critical infrastructure systems to prioritise resilience efforts 43

4.2.3. Establishing trust between governments and operators and securing information sharing on risks and vulnerabilities 44

4.2.4. Building partnerships to agree on a common vision and achievable resilience objectives 44

4.2.5. Defining the policy mix to prioritise cost-effective resilience measures across the life-cycle 44

4.2.6. Ensuring accountability and monitoring implementation of critical infrastructure resilience policies 44
4.2.7. Addressing the transboundary dimension of infrastructure systems 45
5. Conclusions....46
References 47
European projects 52
List of abbreviations and definitions....53
List of boxes....54
List of figures....55
List of tables 56

Abstract

Incidents involving networks delivering essential services to society across two or more countries are witnessed in the everyday life of citizens whenever exceptional weather conditions disrupt transport, power or network and information systems close to a border. Yet it proved to be more difficult than initially envisaged to compile a list of major transboundary incidents informed by official and reliable sources. It proved equally challenging to account for current examples of governance arrangements providing joint assistance to population, businesses, and services across borders in Europe.

The study makes an effort to provide first a conceptual framework for defining cross-border impacts, building on existing classifications of interdependencies and types of impacts available in literature. It then illustrates risk assessment and management methods and discusses the need to complement the latter with a resilience approach. Reasons for embracing resilience thinking are the increasing complexity of networks and the environment in which they operate, the dynamicity of both threats and systemic vulnerability of those and of sectors that depend on them for their own functioning. Because of such complexity and dynamicity not all threats, failures and impacts can be fully envisaged and anticipated. Therefore, avoiding catastrophic modes of failure and recovering in the smoothest possible way, which are the essence of resilience, become key concerns for utilities' providers and for society at large.

In the last section of this report, future pathways are proposed in the search of risk and resilience assessment and management tools better in line with multi-hazard and multi-risk understandings. On the governance side, the recommendations of an OECD report on enhanced governance of CIs are re-elaborated through the transboundary lenses.

This study makes a first timely contribution to the very recent policy development at the EU level: the Directive on the Resilience of Critical Entities (CER) and the Directive on Measures for a High Common Level of Cybersecurity across the Union (NIS2). The former address safety and security aspects of CIs in a systemic manner, whilst the latter focuses on network and information systems that have become increasingly vital for all other CIs and for a very large number of services and economic activities globally.

Acknowledgements

The authors thank Nicola Berni, from the region of Umbria, for the permission to use the picture on the cover page.

Authors

Scira Menoni

Anna Faiella

Veronica Gazzola

Maria Pia Boni

Gustav Eklund

Christina Corbane

1 Introduction

1.1 Objective and scope of this report

This report, regarding cross-border implications of potential failures of networks providing essential services due to natural hazards, is an enhancement of a study carried out in mid-2019. The latter has been updated and integrated with a renewed lens considering the most recent events and latest policy development at the EU level. The pandemic made it clear that the globalization increases our systems vulnerabilities. Challenges have proven to be always more complex than expected, climate change also plays an important role and cross border networks need to be more resilient in order to avoid disruptions as much as possible and reduce losses once they occur. It seemed therefore relevant to revise extensively the original study to address what is known and what should be further researched in order to have a better overview, understanding, and intervention capacity on impacts on networks providing essential services due to natural hazards considering how the latter will be affected by climate change. The challenges in getting such a full understanding will be highlighted and future directions of work will be proposed. Despite the advancements in modelling, tools and techniques to forecast and assess failures of networks impacting their functionality, there is still room for improvement, and significant challenges are still hampering efforts to develop solid statistics based on reliable data. In addition, there is now a clear understanding that full anticipatory approaches to risks to essential services fall short of the multiple ways in which they may be disrupted in a multi-hazard environment and as a consequence of climate change. More effort is needed to address the entire cycle of disaster risk reduction, from prevention/preparedness to response and recovery. In this respect the report will address also more recent understanding of resilience assessment and management.

1.1.1 Definitions

The European Commission first defined critical infrastructures in the Directive for the Designation and European CI and the assessment of the need to improve their Protection (ECI) 114/2008/EC[1] as "an asset or system which is essential for the maintenance of vital societal functions. The damage to a critical infrastructure, its destruction or disruption by natural disasters, terrorism, criminal activity, or malicious behaviour, may have a significant negative impact for the security of the EU and the well-being of its citizens". The new Directive on the Resilience of Critical Entities (CER) (EU) 2022/2557, shifts the focus from the assets to the entities that operate essential services (article 6). Critical entities are not defined as such, but in order to identify them, each Member State should consider three criteria: i. the fact that the critical entity is responsible for essential service(s); ii. that both the essential entity and the infrastructure are located in the country; iii. an accident or a disruption may significantly hamper the provision of such services. In Annex 1 to the CER Directive a list of entities is provided, including apart from critical networks also space infrastructures, financial services, central public administrations, health related (research facilities, laboratories, pharmaceutical and device producers), large scale food production and logistics. Whilst in the ECI Directive the main objective was the identification of European critical infrastructures, the CER Directive addresses all critical entities but points at the relevance of those whose disruption may have relevant cross-sectoral and cross-border impacts.

General definitions of essential network and services, critical infrastructures, lifelines can be found in literature. For example, Espada et al (2014): "Often called as lifeline systems, critical infrastructures refer to critical physical facilities, technological networks and logical systems that play major importance for public welfare". Cedergren et al (2018) specify "Critical Infrastructures, including transportation systems, water supply, telecommunication, power supply, and banking and finance, provide essential functions and services to our modern society. Their criticality means it is of utmost importance that these systems are resilient to accidental as well as intentional disturbances in the sense that they have an ability to resist failures and/or quickly resume their functionality when such events occur".

According to Egan (2007) a more dynamic approach is required to define and identify critical infrastructures, due to the rapid development of technologies, some assets and infrastructures are becoming increasingly "critical" (what he labelled as CI like). Criteria that have been considered for identifying critical infrastructures and which can be used also to identify new ones in the future are provided in **Table 1**.

[1] https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX:32008L0114

Table 1. Some criteria that supports the identification of CI and essential services

Main feature	**Meaning**	**Examples**
Dependability	As those services are vital for other systems functioning, high degrees of reliability, fault tolerance and continuity are required, often by law or by provisions of authorities.	Lifelines networks in particular
Complexity	Made of highly hierarchical components and sub-systems offering vulnerability targets to hazardous and malicious threats	Systems such as power are made of parts that depend on each other and the failure of a component high in hierarchy can imply total disruption even when the physically harmed part is very small and circumscribed
Large scale consequence	Dysfunction may cause very large disruption and non-trivial harm in a community, region or nation.	Lifelines networks, but also strategic economic sectors and services (hospitals, banks)
Relevance with respects to national stability & security	Strategic for defence, for the survival of people	Assets without which communities, regions and nations may become easily powerless

Source: Authors' elaboration

Dependability (Al Kuwaiti et al 2006) was a term that was used as an umbrella definition to indicate the performance requirements that critical infrastructures, essential services and the like should fulfil, both qualitative and quantitative. The term embeds also concepts such as reliability, fault free service, etc. Lifelines such as energy, water, network and information systems, transport by being the backbone of modern societies are subject to very demanding legislation and rules regarding their availability, including under extreme operational conditions such as those produced by natural disasters.

Complex behaviour is often associated to lifelines as they share many features of complex systems. In fact, the interrelationships among lifelines and with other sectors easily become complex, because the combination of different failures does not produce a linear outcome but is instead rather unpredictable (Park et al 2013). Networks providing essential services are also complex as far as their governance is considered, especially nowadays as a plethora of stakeholders both public and private own, are responsible for parts of the networks. Furthermore, often the managing companies of services are detached from the owners of the physical network a condition that creates additional constraints and difficulties in coordination when a large incident occurs.

"Critical" indicates also the large consequences that may occur, both in terms of magnitude of incident and especially in terms of geographic extent of functional damage. In fact, a spatial perspective is important for dealing with essential services and networks risk assessment. In fact, as highlighted in literature (Arvidsson et al 2021; Collier and Andrew 2020), essential networks do not exist in isolation, they make part of the territory they serve. Complex interrelationships between the two are easier to grasp in maps that provide at least the representation of how parts of infrastructures located in different areas and serviced areas are related to each other. The spatiality of essential services infrastructures is important for two other reasons. First because some features of the networks themselves, some properties and vulnerabilities (like systemic) emerge only at larger scale because of the interconnections (Menoni et al 2012). This explains the need to assess the vulnerability and risks to critical infrastructures at multiple scales, considering the larger dynamics that are apparent only at regional or above regional scales and the individual ruptures and failures that are often local. The second reason for taking a spatial perspective when dealing with networks providing essential services, is the important connection with urbanization and therefore with urban and land use planning. In fact, essential services' vulnerability is due to their location in hazardous zone, to their being exposed to one or multiple natural hazards and to their relation to the other functions that cities host. In fact, the vulnerability of critical infrastructures is not only due to their intrinsic characteristics but often also to the built environment with which they interact and also to the use that is made of buildings and infrastructures themselves.

The definition of critical infrastructures emerged in the security arena during the Fifties in the Cold War period. Essential services have been always, unfortunately, the target during wars. The current geopolitical situation has brought the issue of malicious and hybrid threats to critical infrastructures very high on the agenda (Tavares Da Costa and Krausmann 2021; Jungwirth et al 2022).

By aiming at addressing the issue of cross-border impacts to networks providing critical services due to natural hazards, the present report does not cover the full spectrum of essential services. More specifically, the report will address disruptions to networks such as energy related, water, transport, and, last but not least, digital services as defined in the Annex to the CER Directive.

1.2 The evolution of European Policies on Critical Infrastructures in the last two decades

The European Programme for the Protection of Critical Infrastructures was presented in the Communication from the Commission (COM(2006) 786[2], 12/12/2006) and adopted by the European Council in 2007. The program, managed by DG Migration and Home Affairs, was quite wide in scope, in that it prioritized on the terrorism threat, but enforced an all hazard approach, asked for a European framework for the protection of CI, considering not only threats but also vulnerabilities and interdependencies, internal to each Member State, cross boundaries among Member States and external. The Program followed years of background work that was carried out within the Commission and led finally to approval of the 114/2008/EC Directive for the Designation and European CI and the assessment of the need to improve their Protection (ECI) in 2008 requiring each Member State to identify, designate and manage European Critical Infrastructures located in its territory.

In the more recent review on the implementation of the ECI Directive published in 2019[3] both positive aspects and shortcomings have been thoroughly analysed after extended stakeholders' consultation and analysis of available documents at the national and European levels. Among the pros, it is highlighted how the ECI Directive triggered in some countries the whole policy on CI protection, and some important cross border initiatives. As for the cons, the limited number of sectors implied, the too limited consideration of network and information systems despite their rapid growth and the over increasing reliance on them of other sectors, the lack of flexibility in defining what are CI and of "the detail necessary for implementation". Most importantly it was felt that whilst continuing to be relevant for the protection aspect of CI, it failed meeting the requirement of the 2013 European Programme for the Protection of CI that emphasized the relevance of cross sectoral interdependencies and the crucial role of resilience thinking.

The recently approved Directive on the Resilience of Critical Entities[4] (CER, (EU) 2022/2557) is addressing the weaknesses identified in the study and calls for a more unified approach in Member States (MS). The CER Directive brings a number of important novelties. It requires first to designate critical infrastructures and then identifying those that are of European relevance. It then asks MS to develop a national risk assessment for critical entities and a plan of resilience for national critical entities. The reasoning behind is that through interconnectedness and interdependencies even a local disruption may result in a larger harm for the internal European market. From a governance perspective it is required that an officer that will liaison with the European Commission be identified to have a clear address in case of incidents, to ensure cross-border collaboration and reporting to the European Commission. The CER Directive endorses a rather different vision with respect to Directive 114/2008/EC, conceptually shifting from a concept of protection to that of resilience. It also promotes a fully systemic approach to the analysis and management of threats and vulnerabilities, acknowledging the many potential cascading and domino impacts that may arise either because of enchained threats or because of the ripple effects that CI disruption may have on societal and economic sectors. This change is mirrored also in the title: by introducing the concept of critical entities, the Directive refocuses from the assets to be protected (the CI as networks and plants) to the operators that must prepare and enforce plans for their resilience, encompassing the entire cycle from prevention to absorption of stress to response and recovery.

The term entity is also permitting a better alignment with the Directive on Measures for a High Common Level of Cybersecurity across the Union, the so called NIS 2 Directive[5], that is addressing entities, public or private, responsible for essential and important services that rely on digitalization. NIS 2 is repealing the previous

---

2 https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A52006DC0786
3 https://home-affairs.ec.europa.eu/system/files/2019-07/20190723_swd-2019-308-commission-staff-working-document_en.pdf
4 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022L2557
5 EUR-Lex - 32022L2555 - EN - EUR-Lex (europa.eu)

Directive (EU) 2016/1148[6] (NIS) passed only a few years before. NIS was setting the need to develop a national strategy for the protection of information systems (with a focus on digital services which all other services and businesses are increasingly dependent on), stronger cooperation at the European level with the creation of a European Union Agency for Network and Information Security (ENISA) and the formation of a Computer Security Incident Response Team (CSIRT). The new NIS2 Directive[7] is aimed at protecting data and information systems from risks identified as any "event having the potential adverse effect on the security of network and information system", thus aiming also at the protection of the assets that make data transfer and management possible. Cross-referencing is made in both the CER and the NIS 2 Directives in various articles (Art 5 - CER; Art 2 - NIS2), acknowledging for the interdependence between essential services and network and information systems and between the latter and several other economic activities and services.

Essential services are an important asset to be protected not only for the integrity of the internal market, nor only to guarantee security in the face of malicious and intentional threats. They are equally exposed to natural hazards (Tacker ET AL 2019) and to na-tech (Necci and Krausmann 2022). The assessment of their exposure and vulnerability to natural hazards has been always a concern for reducing the impact of a disaster, to guarantee effective emergency interventions (Tariverdi et al 2023) and recovery (Horton et al 2022). Safeguarding of the functionality of essential services has been always a key aspect for civil protection organisations and a matter to be fully included in contingency and emergency plans (GCSA 2022).

In the Decision 1313/2013/EU on the Union Civil Protection Mechanism at article 6 it is stated that Member States shall prepare and submit to the European Commission National Risk Assessments identifying, analysing an assessing risks and capacities to prevent and mitigate them. The JRC produced two Reports providing Recommendations for National Risk Assessment for Disaster Risk Management in the EU, respectively in 2019 (Poljansek et al., 2019) and 2021 (Poljansek et al., 2021) devoting a specific chapter to CI disruptions. In the 2021 chapter on CI, Theocharidou et al refer to the findings of the Overview on Natural and Man Made Hazards in the EU based on NRA in 2015 and 2017[8] highlighting the need to strengthen the reporting on critical infrastructure disruption especially as regards their interdependency and the interlinkages that account for direct and indirect impacts due to a disruption. Both the 2017 and 2020 Overview Reports highlight the limitations in providing information and assessments on the cross-border dimensions of CI disruptions.

In the 2019 Reporting Guidelines, a template is provided to MS to follow in their NRA. Question 15 focuses on CI protection measures, asking to "state whether there are measures in place to protect critical infrastructure regarded as relevant for the continuation of vital societal functions".

Finally, in the Communication on the Union Disaster resilience Goals issued on February 2023[9] "the complexity and interdependency of risks the EU faces" is addressed requiring therefore to "identifying vulnerabilities in critical sectors, anticipating hazards and threats and reinforcing collective action to better prevent and prepare for disasters". "Essential services such as energy, water, and health provision, and telecommunications are key to ensuring the well-being of people, as well as to the emergency response itself. These services need to remain operational during and after a disaster".

1.3 Structure of this report

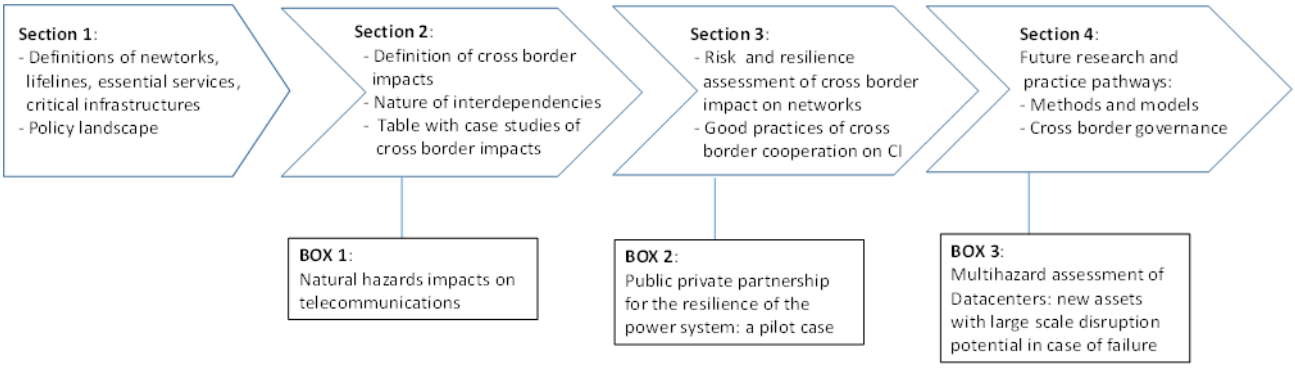
As illustrated in **Figure 1**, following this introduction (section 1), in section 2 cross-border impacts are defined considering CI's interdependencies. In the same section, a table which summarizes the most relevant failures in CI with a cross border impact is constructed, by combining information gathered from heterogeneous sources.

In section 3, frameworks for risk and resilience assessment and management are analysed with a focus on existing good practices of cross-border cooperation. In section 4, a discussion about expected future outcomes is provided. In the last section, section 5, some conclusions are drawn highlighting future trajectories for research and practice.

---

6 https://eur-lex.europa.eu/eli/dir/2016/1148/oj
7 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022L2555
8 https://op.europa.eu/en/publication-detail/-/publication/285d038f-b543-11e7-837e-01aa75ed71a1/language-en
9 https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52023DC0061

Figure 1. Structure of the report



Source: Authors' elaboration

Within the report three text boxes with selected contents are inserted. Box 1 consists in an analysis of the different annual reports published since 2012 by the European Union Agency for Cybersecurity (ENISA) with consideration regarding the impacts on network and information systems due to natural disasters at the European level. Whilst Box 2 reports a project carried out jointly by the Lombardy Region and electrical power service providers to enhance the resilience against black outs. Box 3 focuses on data centres as vulnerable assets which might have cross-border implications in case of failure.

2 Defining cross-border impacts on networks providing essential services

In this section cross-border impacts on networks providing essential services are discussed. First what is meant with cross border impacts will be explicated. Second, the nature of the impacts will be discussed more in detail. More specifically, it will be shown that in the case of networks the definition of what is a cross-border impact is not as straightforward as one may think. In fact, one needs to consider more than just an incident occurring at the border or hampering physically an infrastructure that connects two or more countries. The possibility of functional cascading impacts, the nature of spatial interrelationships between countries and regions must be considered as failures in one asset in one country may reverberate and amplify across border because of such systemic interdependencies that can take different forms. In the last part of this section a list of case studies of cross-border impacts on networks providing essential services has been compiled. Most cases are due to natural hazards. Few cases that were of particular interest because of significant cross border impacts have been considered as relevant even though not triggered by a natural hazard.

2.1 Defining impacts

In the Disaster Science Report 2020, Walia et al suggest that in the disaster risk and climate change domains, "impact" may refer either to positive or negative consequence due to an extreme event. Even though there might be positive impacts for certain sectors that benefit for example from the funds made available for reconstruction, more often the term indicates the damage and losses that may affect one or more sectors. Indeed, the nature of the impact (positive or negative) depends on who is the observer and who's the perspective to be considered. It may also well be the case that initial impacts are negative (damages) but that the latter trigger changes in the legislation or in practice that can be seen as positive. In this report "impacts" are intended as negative ones, that can be either direct or indirect. In the Disaster Risk Management Science Report 2017, Menoni et al have provided a framework summarizing several years of research and studies in both engineering and economics to provide a clear overview of direct and indirect impacts. The former is intended as physical damage and losses (damage represented in monetary terms) due to an extreme event, affecting people, assets, infrastructures. The latter refer to the systemic consequences the physical damage that has occurred in one or more component of one or more assets, infrastructures or to people may have on the functioning of interconnected systems, including markets and the economy. The interconnectedness of our world has increased in the last decade especially because of some networked services such as transport and network and information systems that favour on the one hand the escalation of disruptions from one level to higher and on the other cascading from one system to another (Thacker et al 2019).

2.2 The cross-border dimension of impacts

Cross border impacts refer to those impacts, both direct and indirect, that intersect borders between one jurisdiction and another, and especially between one country and another (or involving multiple countries at the same time). As evidenced in Walia et al (2020) both spatial and temporal scales are relevant discussing about impacts that may easily escalate from local to regional, national and beyond, and temporal as a disruption or even the mitigation measures to treat it may produce damage and losses that persist even in the longer term. As will be discussed in the following, even though at first sight it may seem straightforward to define "cross border impacts", this is not the case due to complexity of nowadays systems and the various types of disruptions, both direct and indirect, physical and functional that may occur.

In the Overview on Natural and Man Made Hazards 2017 it is suggested that "Most natural and man-made disasters present cross-border risks due to their geographical nature (earthquakes, fires, severe weather, floods and space weather), as well as the volatility and scale of their impacts (pandemics, livestock epidemics, nuclear/industrial accidents). The human, economic or environmental impacts of these hazards, as well as their likelihood of occurrence exist irrespective of national borders." In the following an attempt is made to disentangle the different factors and ways in which impacts may become transboundary when it comes to networks providing essential services.

Table 2. Criteria to define cross-border impacts

Criteria to define cross-border	Explanation	Examples	Considered aspects
Hazard based	Cross-border triggering hazard affecting potentially wide regions: flood across countries, storm (snowstorm, very intense precipitation, strong winds, hailstorm), forest fires, earthquakes.	Cross-border localised hazards: avalanches, landslides, occurring on critical infrastructures.	Failures on components of cross-border critical infrastructures (mainly lifelines) themselves.
Impact based	The failure in one asset in one country may impact the same system in other countries, with consequences that can expand to larger areas. Protective measures, including redundancy and possibility to switch to other service providers may alleviate and/or reduce the possibility for such cross border incidents.	In case of cross-border networks, the damage in one part of the system in one region or country may affect the system in other regions/countries that are connected to the same network.	This is the case that has inspired originally the 2008/114/EC Directive, focusing on networks, assets and sectors.
Systemic Vulnerability based	Dependencies that are regional or even global ones as in the case of civil aviation or when supply occur at a global scale (hardware produced in Thailand during the 2011 flood).	Systemic interdependencies and connections among lifelines that are physically cross-border or that depend on each other (e.g. gas, oil) but also depend on supply that is cross-border (ships/ports).	Failure in one system, that is located in one country or region may affect other systems in other countries or regions due to the increasing interdependency of economic and infrastructural sectors.

Source: Authors' elaboration

In the first place, the hazard itself may be transboundary (what Rinaldi et al. 2001 defined as "common mode"). Strong storms, extended forest fires, large floods, earthquakes may occur close or across a border impacting simultaneously all CIs in the transboundary area. Hazards occurring on a transboundary critical infrastructure, like a landslide or an avalanche (or a series of) affecting a transnational highway are likely to provoke a cross border breakdown of the transportation route. It may be also the case that critical infrastructures themselves suffer an incident due to a variety of causes such as malfunctioning of components, lack of maintenance, obsolescence. Some CI, such as gas pipelines or nuclear facilities, are also hazardous installations that whilst damaged may trigger a chain of devastating damage to people, the built and natural environment. This "hazard based" definition is implied in the 2017 Overview of Natural and Man Made Hazards 2017 quoted above.

Impact based criteria look at the domino effects of escalating factors given which an incident occurring in an infrastructure in one country may impact also the infrastructure(s) in the other country. This is typically the case of transboundary networks such as transportation, energy, or information and data exchange networks. Networks that are physically interconnected will suffer from the consequences of an incident that will propagate across borders. The 114/2008/EC Directive was mainly focusing on this "impact based" identification of CI.

Last but not least, cross border impacts may occur as a result of systemic vulnerability. The latter derives from the functional dependencies and interdependencies between networks the impacts of which may reverberate across borders. This is the case for example of power system (Rinaldi, 2004) that is vital for the functioning of many sectors including other networks. In the more recent years communication and especially the internet has

gained prominence as the world is increasingly relying on digital information in a very large number of sectors and in a widespread way for a vast array of activities, related to public services and to businesses (Luiijf and Klaver, 2021).

In **Box 1** the failures and disruption to the network and information systems system due to natural hazards are described, grounding on a number of reports provided by ENISA.

Box 1. Natural Phenomena causing long lasting incidents to network and information systems sector (analysis of ENISA reports)

Heavy storms, floods, wildfires, heat waves or droughts may severely impact the network and information systems infrastructure. As extreme weather events are impacted by climate change, the EU telecom sector is increasingly concerned by natural extremes as reported in the ENISA telecom security incidents annual report of 2020[10].

Since 2009 in the context of Article 13a of the Framework Directive (2009/140/EC), the European Union Agency for Cybersecurity (ENISA) publishes yearly reports on relevant incidents across European countries. According to ENISA the main causes of reported incidents are: (i) system failures intended as for example software bugs, hardware failures or software misconfigurations; (ii) human errors; (iii) natural phenomena, intended in the analysis as severe weather, earthquakes, floods, pandemic diseases, wildfires, wildlife, and so on; and, (iv) malicious actions.

Even though natural extremes cause a smaller percentage of incidents, their impacts are heavy due to longer duration disruptions. Natural hazards end up being the largest cause of impacts when the latter are measured in terms of "total user hours lost", obtained by multiplying the number of lost user connections by their duration. According to the statistics of ENISA, the number of incidents due to natural hazards is not proportional to the duration of outages, differently from incidents due to system failures that on average last for much shorter periods of time. The main reason is that natural hazards do not cause only direct damages, but also indirect and systemic consequences. Physical damage is the most well-known cause of network and information systems failures due to natural hazards. However, breakdowns caused by supporting infrastructures such as power constitute important indirect threats to the telecom sector. Modern telecom systems depend heavily on power not only for their own functioning but also for cooling. Another major cause of network and information systems failures during disasters is network congestion, which might be due to a physical damage, a loss of service or to overload connected to response activities, requests of help by affected people, rush to get information from relatives and friends.

The latest ENISA Annual Report, referring to year 2020[10], contains records of 170 incidents submitted by 26 EU Member States and 2 EFTA countries. The total user hours (h) lost in 2020 was 841 million user hours, in line with the prior years' analysis. The report mentions user hours lost due to high load caused by the COVID-19 pandemic. In connection to the latter, **Figure 2**. Incidents share by cause **Figure 2** shows an increasing trend for systems failures between 2019 and 2020. From the start of the pandemic a transition phase due to increased usage has been documented. The report, explicitly highlights that "the general take-away from the pandemic is that services and networks have been resilient during the crisis, despite major changes in usage and traffic". In 2020, 50% of the users' hours lost occurred due to system failures followed by 41% due to human errors, 7% due to natural phenomena and 2% due to malicious actions. Differently from previous years, in 2020 system failures were not only the most frequent but they also caused most of the impacts (50% of the total impacts). However, 2020 must be considered exceptional in many regards, given all the consequences triggered by the COVID-19 pandemic.

Considering a longer time scale (see **Figure 2**), in the period between 2012 and 2020 system failures are the primary cause of damage, followed by human errors, while natural hazards draw a rather irregular trend from one year to another. The trend of incidents caused by natural hazards displays three main peaks, one in 2013, one in 2019 and the highest in 2017. However, year 2018, has recorded a peak of Users Hours Lost due to natural hazards, mainly extreme weather and wildfires, as shown in **Figure 3**.

[10] https://www.enisa.europa.eu/publications/telecom-annual-incident-reporting-2020

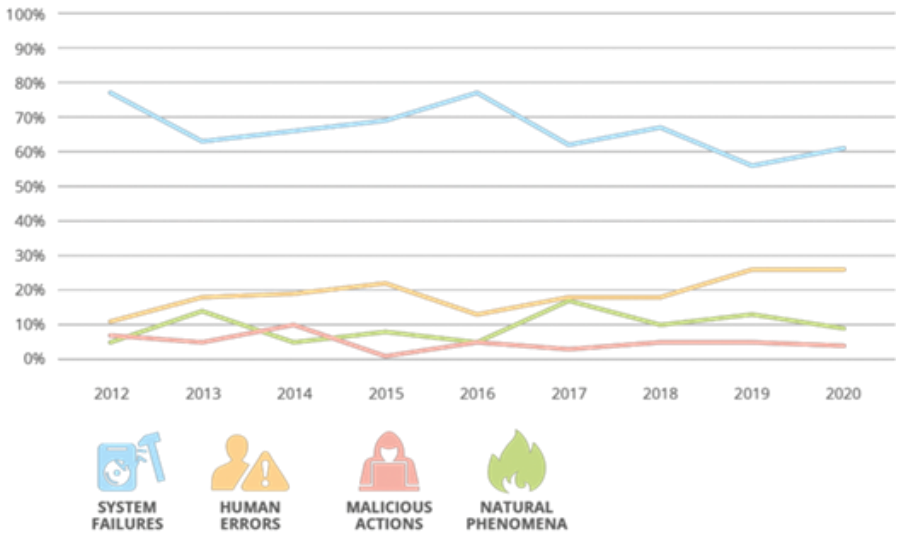
The 2018 report[11] contains records about 157 incidents submitted by NRAs from the 28 EU Member States and 2 EFTA countries. The total user hours lost, multiplying for each incident the number of users and the number of hours, was 969 Million User Hours. Since 2012, in 2018 natural phenomena account for more user hours lost than system failures. Specifically, 10% of the incidents were caused by natural hazards. Despite the relatively small percentage, especially if compared to the 67% of incidents due to system failures, natural hazards had the highest impact with 50% of hours lost compared to the 10% due to systems failure. Furthermore, 15% of the incidents involved power cut, as a detailed cause, but these incidents accounted for half of the total user hours lost (50%, 496 million user h), this is the evidence of the strong dependencies of the telecom sector on power. 52% of incidents implying power cuts were caused by natural hazards.

The year 2017 according to the report[12] recorded the highest percentage (i.e. 18%) of occurrences due to natural hazards such as heavy snow/ice, storms and wild fires. The average duration of incidents per root cause category in hours for natural phenomena is 96, an impact almost seven times longer than the impact caused by human errors and system failures. The reported incidents caused by natural phenomena (extraordinary occurrence of wildfires) had by far the longest recovery time on average per incident.

The trend of Natural hazards, depicted initially in **Figure 2**, shows two additional relative peaks one recorded in 2019 and one dating back to 2013. Following the report[13] in 2019 natural hazards were the main root cause for most of the impacts recorded accounting for a third of the total user hours lost. In 2019, natural hazards accounted for 13% of the total number of events and 30% of the total hours lost. Accordingly, the 2013 report[14] shows that natural hazards were the main cause for most of the lost hours. The average duration of incidents caused by fire and heavy snowfall had the longest duration (86 and 62 h respectively) followed by power cuts (53 h) and Storms (47 h).

Table 3 displays a data comparison between the years in which Natural Phenomena have reached relative peaks.

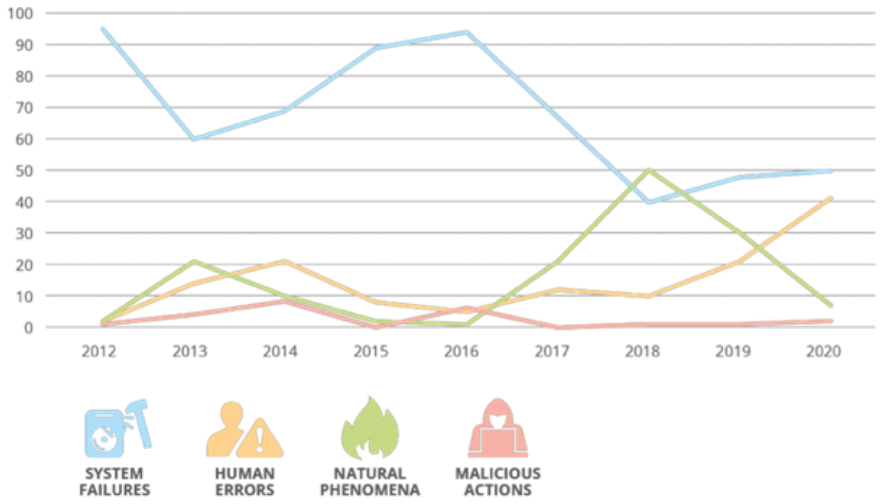
Figure 2. Incidents share by cause



Source: ENISA, Annual Report 2020[10]

11 https://www.enisa.europa.eu/publications/annual-report-telecom-security-incidents-2018
12 https://www.enisa.europa.eu/publications/annual-report-telecom-security-incidents-2017
13 https://www.enisa.europa.eu/publications/trust-services-security-incidents-2019-annual-analysis-report
14 https://www.enisa.europa.eu/publications/annual-incident-reports-2013

Figure 3. User hours lost per root cause category – multi-annual 2012-2020 (% of total user hours lost)



Source: ENISA, Annual Report 2020[10]

Table 3 Comparison between the years in which Natural Phenomena have reached relative peaks

	2013 *relative peak	**2017** *peak of incidents due to Natural Phenomena	**2018** *peak of User h lost due to Natural Phenomena	**2019** *relative peak	**2020**
No. of incidents	90	169	157	153	170
Tot. user hours lost (M)	46	89	97	99	84
% of number of incidents – natural phenomena)	14%	18%	10%	13%	9%
Users' hours lost - natural phenomena (M)	23 (52% of total users h Lost)	57 (64% of total users h Lost)	48 (50% of total users h Lost)	29 (30% of total users h Lost)	19 (7% of total users h Lost)
Detailed Causes (most recurrent| ascending order)	Fire, snowfall, Power cut, Storm, Flood	Hardware Failure[1], Power Cut[1], Software bug[1], Overload, Snow/ice, Wind, Wildfire	Power Cut[1], Wind, Cable Cut[1]	Power cut[1], winds, snow/Ice, Flood, Fire	Power Cut[1], Wind, Cable Cut[1], snow/Ice

[1] Cascading impacts of natural events

Source: Authors' elaboration

2.3 Networks' systemic vulnerabilities: types of interdependencies

Systemic vulnerability due to intra- and inter-dependencies of networks (Nojima 1998) is key to understand the root cause of cascades and escalations (Alexander (2018, p. 182). Intra-dependencies have been defined by Nojima (1998) as occurring within the same system (for example in the case of power system between generation, transmission, distribution point shaped and linear elements) whilst inter-dependencies are those between systems (i.e. a functioning transportation system is needed to reach a hospital).

Whilst most of the initial studies regarding infrastructures focused on single systems according to the literature review carried out by Pitilakis et al. (2014), the interconnections between infrastructures have been increasingly considered in the last decade. Menashri and Baram (2015) showed how the functioning and delivery of services are dependent upon each other across countries. The failure or degradation of a critical infrastructure or of

some of its functional elements can have negative cross border impacts (Rehak et al., 2016) due to the increasing dependencies and interdependencies of CI systems. Dependency is defined by Rehak et al (2016) as the (one-way) link/connection between two infrastructures through which the state of the second depends on the state of the first, but not vice-versa. By interdependency is intended a bidirectional relationship between two infrastructures through which the states of the two infrastructures affect each other (Rinaldi et al., 2001; Petit et al., 2015).

In their seminal paper that has inspired several scholars afterwards, Rinaldi et al. (2001) provided a classification of both the nature of interdependencies among critical infrastructures and the types of interconnected impacts that may occur across CI. Interdependencies are classified as physical, geographic, cyber, and logic. Physical interdependencies occur when the output of one infrastructure serves as an input for another, for example power is needed to pump water. Geographic refers to the proximity of CI sharing the same environment, for example when water, gas pipes and information and data networks cables are tunnelled under a bridge. Geographic interdependencies are an important component even though not exhaustive of spatial interrelations introduced in section 1.1. on definitions. Cyber points at the dependence of infrastructures on informational input. Rinaldi et al (2001) classify all other dependencies as logic, mainly due to human decisions. For example, the privatization of public utilities has reduced the reliability of the power service in the USA (see also Perrow, 2007).

2.4 Nature of interdependencies among impacts occurring on networks providing essential services

Rinaldi et al. (2001) propose that multiple impacts be classified as cascading, escalating and common cause. Cascading refers to incidents in one infrastructure provoking failures in others, escalating refers to simultaneous independent failures in two or more critical infrastructures exacerbating one the disruption of the other, whilst "common mode" failure refers to conditions, such as an earthquake or a storm affecting at the same time multiple infrastructures (what we have defined as hazard based cross border failures).

In **Table 4** the types of multiple impacts across critical infrastructures that are most often used in current research and practice are listed and defined. Aspects identified in the classification of Rinaldi et al. (2001) are still considered as a reference even though concepts such as cascading, cross-sectoral, and escalating have been redefined or broadened in scope.

2.4.1 Cascading

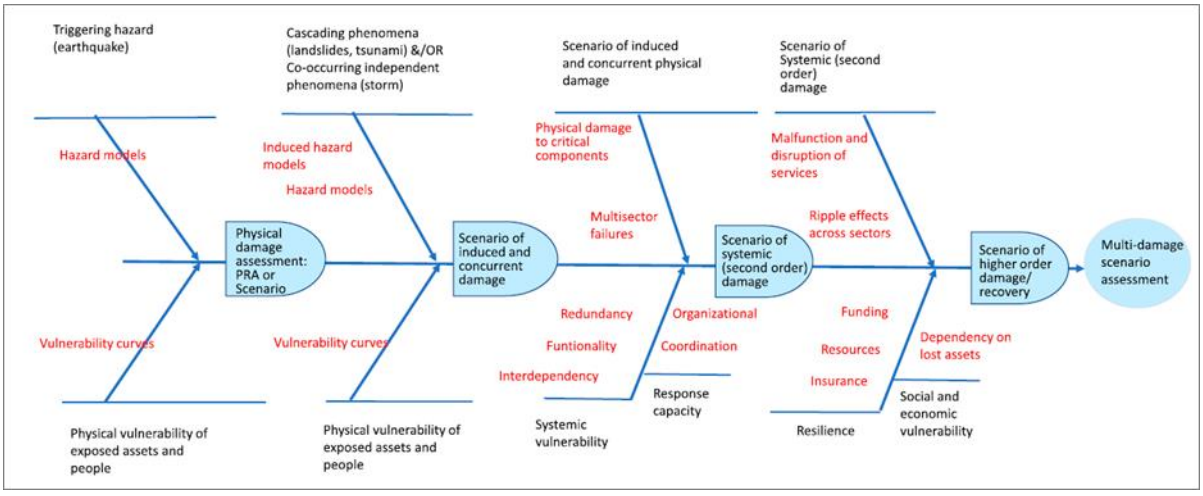
Cascading is mainly used to represent the situation in which a damage in one network or in a part of a network triggers second and higher order damage to the same infrastructures or in others (Dominguez et al., 2021). An example of framework representing the cascading impacts in different systems is represented in **Figure 4** (Menoni and Boni, 2020), a diagram that permits to put in evidence the complexities related to this kind of multiple impacts. In fact, it's possible to observe as the successions of the impacts can be influenced by: the different interdependencies of the different systems, their intrinsic characteristics and vulnerabilities, different possible combination of the occurrence of external triggering events, as the natural hazard (single, or multi-hazard), and by the territory characteristics.

Table 4. Types of multiple impacts in Critical Infrastructures

Type of impact	Explanation	Example
Cascading	A chain of impacts that can be described as *n* order impacts across spatial or temporal scales. It embeds the idea of multiple causal chains in which the failure in one part of a system transforms into a second and higher order damage in the same system or in interconnected ones.	A typical example is provided by failures across supply chains when a critical part of the chain is disrupted the repercussions can be felt far away and for long time, see for example the impact on computer components due to the Thailand flood in 2011
Cross-sectoral	An incident occurring in one infrastructure may affect physically or functionally others given the interconnections between them	Typically, loss of power may affect the capacity to pump water, treat water, traffic control, etc.
Escalating	Rinaldi et al. (2001) interprets escalating as a failure in two or more infrastructures simultaneously provoking in its turn delays and obstacles in the recovery of both, multiplying so to say the impact. Escalating may also have a purely geographic interpretation, meaning an incident occurring locally that has a much wider impact, regionally, nationally or even globally	Rinaldi et al. (2001) refer as an example to a failure in telecommunication and in the road network hampering the arrival of technicians for the repair of the former. Considering spatial scales, one may recall the impact of the Eyjafjallajökull eruption affecting flights in all the Northern Hemisphere in 2010.
Domino	In industrial risk analysis it refers to an incident affecting a part of a hazardous plant spreading to other units and even to a larger area where other facilities may be located	Typically, an explosion or a fire starting in a unit spread that may spread to the entire plant and even outside the fences of the facility

Source: Authors' elaboration

Figure 4. Cascading impacts framework (Menoni & Boni, 2020**)**



Source: Menoni & Boni, 2020

2.4.2 Cross-sectoral

Cross-sectoral is used to highlight the interdependencies across different sectors through for example supply chains. Economic activities depend on transport, energy, network and information systems for business continuity, and on the other hand some economic activities produce components that are key for the functioning of CI. "Cross-sectoral" serves to underline the more complex interconnections that characterize nowadays economic and societal activities that have become even clearer during and after the COVID-19 crisis. According to the Chartered Institute of Procurement and Supply, a United Kingdom-based global professional body working for the purchasing and supply professions, 86% of supply chains (production, packaging, transportation, and distribution) have been impacted by the COVID-19 pandemic (Remko, 2020). The COVID-19 crisis evidenced the relevance of supply chains in the pharmaceutical and medical devices industry, whereas the crisis triggered by the Russian invasion of Ukraine evidenced the fragilities of the food supply chains worldwide (Gheibdoust et al 2023).

2.4.3 Domino

Domino is often considered as a synonym of cascading, meaning propagation of failures, from one infrastructure which causes a failure in a second infrastructure. However, in industrial risk analysis, domino failures refer to impacts that propagate spatially from one apparatus where the original incident has occurred to other parts of the plant or other plants or triggering multiple failures in a large area. Whilst initially this term indicated failure propagation due to proximity and physical closeness, it has been used more recently to address widespread impact of natural hazards on critical infrastructures physically or geographically connected.

2.4.4 Escalating

In literature (Forzieri et al., 2018; Sawalha 2014) the term escalating generally refers to cases in which the emergency gets out of control and deteriorates into a much more severe, larger crisis or disaster. The term is rarely explicitly defined as it is used in its more intuitive meaning. Rinaldi et al. (2001) provides one of the few definitions of escalating referring to an incident occurring in one system that exacerbate another independent incident that occurred in another system. Considering the list of transboundary incidents to CI provided below in **Table 5**, a good example is provided by the snowstorm affecting roads that hampered the effort to provide isolated areas with generators needed to recover electricity as the power system was also disrupted. Taking a spatial perspective (Heri et al., 2010), escalating may mean literally overcoming the confined area where the incident has occurred initially (for example a local level incident) reaching another level, that can be regional, national, or even global. The Eyjafjallajökull volcano eruption in 2010 is a good example of such escalating crisis, as it started with a regional hazard that provoked a large ash cloud that required the halt of flights for one week in the Northern Hemisphere.

2.5 List of case studies of events/hazards with cross-boundary impacts on networks providing essential services.

In **Table 5** a number of incidents on CIs with transboundary impacts have been gathered.

The table is organized as a matrix structuring the information as follows. The first column serves to number the case studies linking to the source of information of each provided in the lower part of the table. The second, third and fourth columns report respectively the date, the infrastructure and the countries involved. In the fifth column the triggering hazard is reported while the following three columns relate to the direct damage and to the systemic failure such damage triggered in other sectors and systems. The last column provides information regarding the type of intervention and recovery that has been undertaken to counteract the failure.

The sources of information listed at the bottom of the table can be grouped in three categories: official reports made by public administration to declare the state of emergency or to account for the event and the damage it provoked, press reports and in some cases reports or articles written by researchers. One significant challenge was though that most reports and media coverage are nation based. In order to account for the transboundary consequences either research reports or media coverage from the two (or more) countries involved had to be consulted and even then, it was not always straightforward to identify cross-border impacts. In fact, there is no European database comprising information on transboundary events affecting CI and this is certainly a severe limitation to conduct a study such as the present one. Even national databases reporting damage to CI are very limited or no publicly accessible (as the relevant example of the TNO Database in the Netherlands). As a consequence, **Table 5** can neither be considered exhaustive nor comprehensive. Nevertheless, it probably contains some of the most severe failures that occurred to CI in recent times as they got enough coverage to

be found in one of the open sources mentioned above. Another limitation is that in the absence of a structured database, information on the hazard(s) and damage are not always easy to match, together with the exact identification of the areas involved. In fact, speaking about CI, the areas involved may be rather large and it is now always possible to find in newspapers or even in public administration reports the full coverage of all areas impacted by a given hazardous occurrence. It must be also pointed out that the first two cases studies are not actually referring to one specific event but to a range of incidents occurring over a relatively long period of time that were examined by projects attempting to provide risk assessment as well as mitigation measures to diminish the potential of direct and cascading impacts in the future.

Despite the limitations, some interesting observations can be drawn from the table and from **Figure 5**. The latter shows at a glance some relevant facts provided in the table. For example, most reported cases relate to the energy and the transport sectors. Case studies seem to be clustered along the borders of Germany and in general in Central Europe, even though caution is needed in drawing conclusions given the pitfalls in the completeness and reliability of the provided information.

This is certainly the case for the Elbe flood in 2002 that most probably provoked more widespread transboundary impacts on CI than the one that could be actually identified in the available sources. The 2003 blackout that affected Italy due to an incident that occurred in Switzerland is a very good example of cross-border impacts due to systemic vulnerability (Menoni and Margottini 2011, p.79).

The November 2006 wide power cut that concerned more than 15 Million customers in Central Europe was not caused by a major natural event, yet highlighted once more the vulnerabilities of the energy system to cascading failures (ENTSO, 2007).

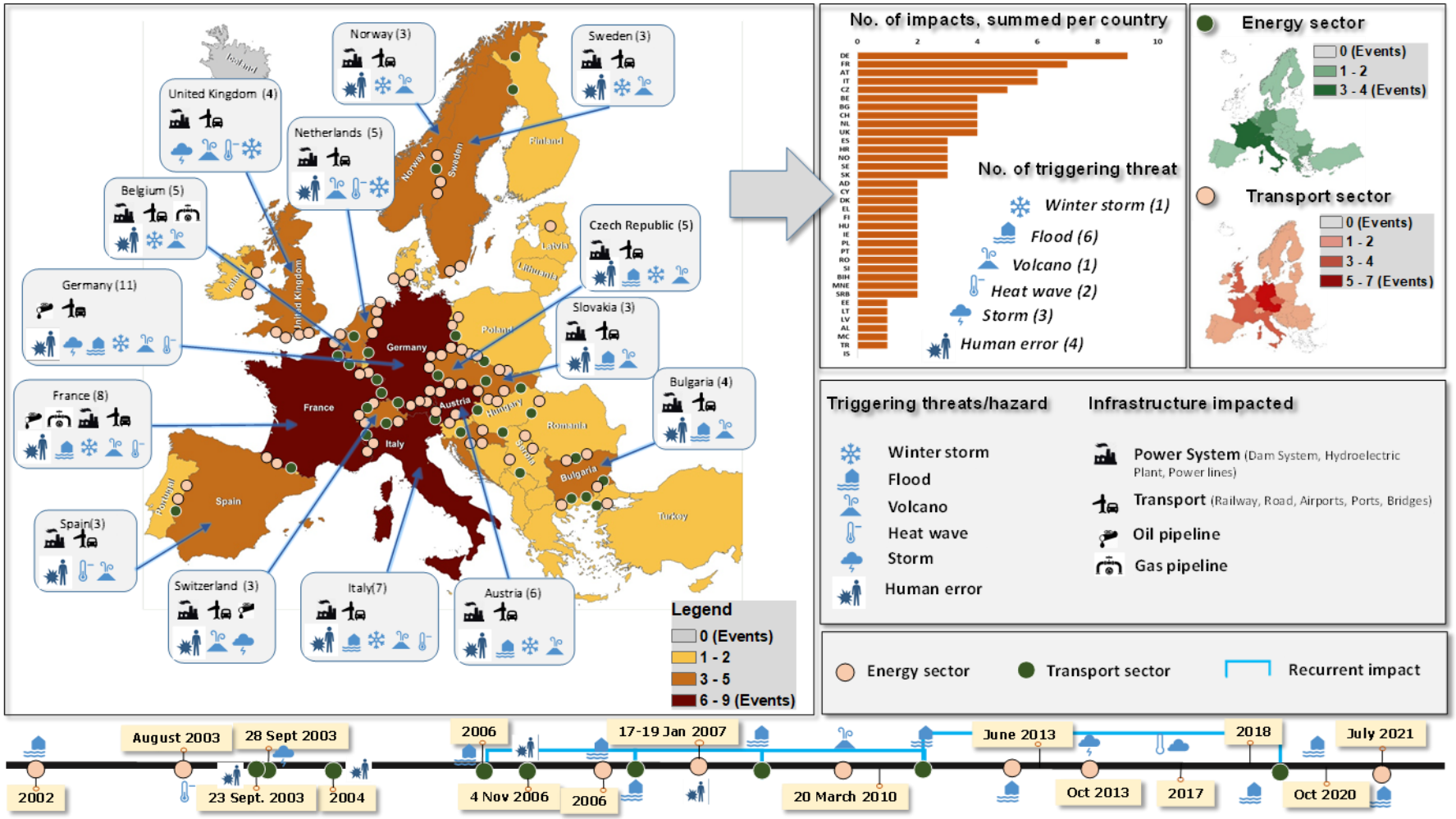
The 2010 eruption of the Eyjafjallajökull volcano in Iceland certainly rang an alarm bell on the interdependency of economic sectors on the aviation industry and on the huge indirect or second and higher order damage (Rose, 2004) that such an event could provoke of much larger proportion than the direct damage of the eruption itself or even on the aviation sector alone (Oxford Economics, 2010).

A particularly interesting case of multi-hazard occurrence involving multiple critical infrastructures is provided by the snowstorm and one of the main shocks of the seismic swarm that affected simultaneously Central Italy in January 2017. Even though it is a trans-regional and not cross-countries event, it constitutes a very interesting case of transboundary multi-hazard event affecting CI with multiple failures due to multiple hazards to different networks. The latter displayed high levels of systemic vulnerability, given the low accessibility of several settlements in the mountain areas to where it was impossible to bring generators for days.

Storms can be considered also as multi-hazard events, as often strong winds, intense precipitation, landslides and flash or debris flows, riverine floods are either associated in the same area (usually mountain) and occurring almost at the same time in very large areas. They provide an example of hazard-based type of transboundary failure. As an example, the case of the October 2020 severe storm impacting various countries in Europe can be recalled. The storm was named Alex in France and Italy, Brigitte in Central Europe and Aiden in Ireland and the UK. In the **Table 5** information regarding the transboundary impact on CI between Italy and France are listed.

Damage to CI during the July 2021 floods in Central Europe have been quite well reported in publicly available reports (Koks et al., 2022; Fekete and Sandholz, 2021). The latter though describe the damage in each county, highlighting that almost any CI has been affected. For example, Koks et al. (2022) describe the extensive damage to the transport system in Germany with long segments of the motorway severely affected and closed after two months of the event, 62 bridges destroyed in the Ahr Valley, several components of the railways damaged, including tracks, energy supply systems, signals, and level crossings. The Authors report also damage in the Belgian railways (such as between the towns of SPA and Pepinster reopened three months later). As for power, more than 200.000 outages reported in Germany, more than 40.000 in Belgium, far less in the Netherlands. Further damage to network and information systems and water services occurred in the three countries. This event can be certainly considered transboundary based on hazard criteria, as the flood affected the area across the border between Germany, Belgium and the Netherlands. Information on cross-border or cascading impacts on services was not reported, it would perhaps require further investigation to assess if those have actually occurred as it may well be expected.

Figure 5. Map locating the various cross-border incidents described in **Table 5**



Source: Authors' elaboration

Table 5. Case studies of events with significant cross-border impacts on networks providing essential services

N.	Events	Infrastructure(s) involved	Countries involved	Initial triggering hazard/threat and initial conditions	Direct damage and failure to CI	Systemic damage and failure	Second order damage to another CI (cascading)	Source of the case study and brief description of recovery intervention (when available)
1	Increasing storms severity/ frequencies due to climate change	Rotterdam Port and shipping lanes	The Netherlands and all countries shipping to and receiving goods from the port	Climate Change related hazards (storm, flooding, rainfalls)	Navigation system interruption	Extreme weather has recently often impacted shipping requiring the closure of the port. Long lasting disruption (more than one week) can lead to blockage of goods to the hinterland and to neighbouring EU countries.	Disruptions in the transport chains at the port can have costly ramifications impacting crucial supply chains for example raw materials for the German steel industry.	Case study in EU_ INTACT Project. The project examines the current status of the EWE and CI hazards in detail, the risk analysis, analysis of future risks, and an assessment of measures and strategies to alleviate these risks.
2	1981- 2011	Transport system; Dam System and Hydroelectric Plant	France, Italy	Floods, landslides, avalanche's, flows (of mud and debris), collapses (falling of blocks)	Roads crossing the Alps have been affected several times by avalanches and various types of landslides.	Apart from the functional damage due to the interruption of major transport networks connecting Northern to Southern Europe, particularly warrying are scenarios affecting dams that may have very dramatic impacts on downstream settlements.	Access to public buildings or open to the public; access to Industrial plants / manufacturing / tourism; access to facilities related to the operation of essential services or the civil protection activities. Water and electricity supply lines	Case studies in the PICRIT project. The analysis of the impacts resulting from the damage to the road infrastructure has been performed using the guidelines of the INSPIRE Data Specification on Production and Industrial Facilities' - 2012. Simulated application of intervention protocols foreseen in the event of structural collapse of the dam.

3	2002	Transport system	Germany, Czech Republic, Austria and Poland	Elbe river flood	Railway line and station in Dresden	Widespread damage to transport systems, in particular to the railway network, famous are the images of the train station in Dresden completely flooded	-	The International Commission for the Protection of the River Elbe, established in 1990 including since 2009, the Czech Republic, Germany; Poland, Austria, the European Union, the river basin Commissions for the Danube, Rhine and Oder as well as several NGOs that participate as observers.
4	August 2003	Transport system	France, Portugal, the Netherlands, Spain, Italy, Germany, the United Kingdom, Switzerland, Ireland, Sweden	Heat wave	Rails buckling; Degradation of signalling systems of railway system; Deformations of road surfaces; Break of London underground trains	Delays and failure of European transport systems	-	Speed restrictions for trains have been imposed since then when the temperature was above 30 °C; the French government has implemented (with The Heat Wave Plan) a number of preventative measures including effective alerting systems.
5	23 September 2003	Power System	Scandinavian Countries	5 transmission lines and 4 generation units out of service before the incident	-	Water supply, Transportation, Communication, Hospitals	Loss of generation, damage to isolator, busbar fault, transmission lines disconnection, power swings and voltage collapse. A total of 4700 MW of load was lost in Sweden (1.6 million people affected) and 1850 MW in Denmark (2.4 million people affected). Duration of the disruption: 5h	The technical report on the event highlighted the need for tightening procedures for improved for communication between operators.

6	28 September 2003	Power System	Italy and Switzerland	Tree flashovers; High power transfers toward Italy. Loss of synchronism of Italy with the rest of UCTE, instantaneous isolation of Italy from the rest of UTCE, thermal plants tripped due to low voltage, complete blackout.	Tripped power lines by trees flashover, high voltage line damaged	Water supply, Transportation, Communication, Hospitals	Reported damages: 640 Mln Euro, aborted liver transplant, 4 deaths. People without service: 57 mln; Lost Load: 2400 MW; Duration: 5-9 h, in some Southern regions up to 48 hours.	To contain the incident Italy was isolated from the rest of Europe, this separation caused strong instability and after few minutes the peninsula was without power. Improved shared situational awareness mechanisms and instruments between the two countries were highlighted as key risk mitigation measure. The failure of the three lines of defence of the Italian national strategy has been scrutinized and addressed.
7	2004	Gas pipeline	Belgium and France	-	Leakage and explosion	-	A transit gas pipeline exploded causing 24 fatalities and more than 120 injuries in Belgium. Damages: 100 mln Euro.	-
8	2005 - 2006	Power system; Wide areas of farmland, Bridges	Bulgaria, Turkey and Greece	Maritsa river flood	Supply interruption, connection interruption	Energy procurement	Reduced dam reservoir levels; hydroelectric power generation loss; agricultural land loss	Case descriptions in - UNECE - Convention on the Protection and Use of Transboundary Watercourses and International Lakes. *Transboundary flood risk management Experiences from the UNECE region, 2009.* Improvement in measures for flood prevention and reduction of flood impacts. Until 2003, there was no communication between neighbouring countries about floods. As a first step for cooperation, a hydrological model was jointly developed.

9	4 November 2006	Power System	Europe	The incident started from a planned routine interruption in Northern Germany to allow the passage of a large cruise ship in the North Sea. A combination of events caused overload that led to automatic protection measures of the system with cascading impacts across EU countries.	-	Water supply, Transportation, Communication, Hospitals	People without service: 45 mln; Lost load: 14500 MW; Duration: 2 h	
10	2006	Transport system	Austria, Czech Republic, Slovakia	Morava river flood, Danube river flood	Railway line	Damages from the 2006 flood were estimated to be € 35 million. The source and the largest stretch of the river are in Czech territory. It forms a (small) part of the Czech-Slovak border and of the Slovak-Austrian border. On the latter, the Morava joins the Danube. The main tributary to the Morava is the river Dyje. The Morava River is dangerous due to both floods caused by regional rainfall and flash floods, so several flood risk management problems need to be solved at the same time.	AUSTRIA. Three dikes broke on the March/Morava flood protection dam. The main line from Vienna to Prague and some roads were damaged/destroyed. Infrastructure losses total approximately €40 million (rail line and road.	Case descriptions in - UNECE - Convention on the Protection and Use of Transboundary Watercourses and International Lakes. *Transboundary flood risk management Experiences from the UNECE region, 2009.* See Also CEFRAME Project Central Europe, running from 2010 - 2013. https://www.ceframe.eu/

11	17-19 January 2007	Transport system	The United Kingdom, Norway, Ireland, France, Belgium, the Netherlands, Denmark, Sweden, Austria, Germany, Czech Republic, Slovakia, Slovenia, Switzerland, Poland	Winter storm	Abandonment of the container ship MSC Napoli in the English Channel; Roof damage of the railway stations in London and Amsterdam; Structural damage of the railway station in Berlin; Fall of trees onto rail tracks	In the European major airports, flights were cancelled or delayed; Ferry services were cancelled; Major motorways and bridges were closed; Long queues developed around blackspots	-	Speed restrictions in railway systems; Warning systems
12	20 March 2010	Transport system	All EU Member States and countries	Eruption of the Eyjafjallajökull volcano (Iceland)	-	Airspace of many countries were closed; 104.000 flights were cancelled; passengers unable to reach their destination	-	Restrictions in the air traffic for precautionary reasons. Follow up studies to assess the actual risk of ashes on plains' engine.
13	8 August 2011	Power System	Arizona, California and Mexico	High temperature and load level; Some generation and transmission maintenance outages	-	Water supply, Transportation, Communication, Hospitals	Loss of transmission line, cascading outages, system operating at its limit, violated the transmission operations and facilities design, collapse of the system. PEOPLE WITHOUT SERVICE: 8,1 mln; LOST LOAD: 7835 MW; DURATION: 6-12 h	The event was initiated by the loss of a transmission line, which caused cascading outages, since the system was not being operated in a secure N-1 state. The failure was produced primarily from weaknesses in operation planning and real-time situational awareness. Entities responsible for the transmission system could not maintain the reliable operation nor prevent cascading outages.

14	June 2013	Transport system	Austria, Bulgaria, Croatia, Germany, Hungary, Romania, Serbia, Slovakia	Danube river floods	Damage to roads and bridges	Large scale disruption to the transportation system across the countries	-	Disaster alarms and timely flood warnings; flood protection measures (i.e. flood protection walls or sandbags, Removal and disposal of debris and biomass from drainage channels); timely evacuation of the most exposed
15	28 October 2013	Transport system	Germany, the United Kingdom, the Netherlands, Denmark, France, Sweden, Estonia, Russia	Cyclone/Storm	Loss of several shipping containers; Roof damage to the railway stations in Denmark; Fallen trees and damage to the catenary of tram services in South Holland; in London, Tube lines were affected because of debris on the tracks	Sailing, ferry, tramway and air services were cancelled or delayed; Major ports, roads, bridges and railways were closed;	-	Warning systems for delays; People evacuation; Preventative closure of railway stations
16	August 2017	Transport	Germany but with repercussion across the Rhine-Alpine railway corridor	Not exactly a natural hazard, but soil conditions probably worsened by the combination of a very hot summer and heavy rains	Damage to a segment of the existing railway near the city of Randstatt that is part of the Rhine-Alpine corridor from Genova (IT) to Rotterdam (NL)	The incident occurred in the railway but the consequences were on the multi-modal shipping and inland transport of goods. The disruption in indirect damage in the added value totalled 2 billion according to an official study that was conducted.		The reputational damage to the railway system was very large with negative consequences on climate change mitigation policies. It also showed the difficulties in providing alternative routes across countries in case of major incidents.

17	October 3 2020	Transport system and power	Alex storm hit Europe between October 2-7 with different names (Brigitte in Central Europe, Aiden in the UK and Ireland)	Storm	In particular across the Roya Valley at the border between France and Italy, transportation networks connecting the two countries were cut and severely damaged.	14 bridges on the Roya river were severely damaged. The railway has been cut and substitutive bus have been organised. All lifelines suffered damage, with 800 households affected by power cuts days after the disaster whilst more than 15.000 the same days.	The tourist sector has been affected, in particular the lodges in the upper part that could not be accessed due to the damage to trails. Several villages were isolated for days.	The trainline was re-established 7 months after the event. Damage was assessed to be as high as 1.5 billion Euros according to the Prefecture in Nice. In the Italian side of the Cuneo Province 18.5 Million Euros were assigned by the national government for the recovery.
18	July 2021	Transport system, power system, network and information systems and manufacturing	Western Europe (Belgium, Luxembourg, Germany, Netherlands, Austria, Switzerland)	Severe flooding caused by strong storms	At least 183 people have died. Entire villages were severely damaged. Dozens of highways and roads closed due to debris and floodwater.	Widespread disruption to logistics and manufacturing operations. Dozens of areas remained without power, telephone, or cell phone networks.	Manufacturing sector with delivery delays and supply shortages. Several companies in the most severely affected industrial areas have been inundated by floodwater that caused extensive damage to machinery, production facilities, and warehouses.	The EEA Report (2014) outlines a series of recommendations to support companies in identifying of sub-tier suppliers and alternative sources for the most critical components; investing in technological solutions to map out and providing better access to supplier networks.
19	14 August 2003	Power System	North America	Tree flashovers; High temperature and load level; generators and 5 capacitor banks out of service	-	100 deaths and $6 billion losses were reported as a consequence. Water supply, Transportation, Communication, Hospitals were severely affected	The blackout triggered by initial outages in Northern Ohio spread to the whole region. Systemic lack of coordinated real-time security assessment, information exchange and control led to the collapse. People without service: 50 mln; Lost load: 61800 MW; Duration: 16–72 h in USA and up to 192 h in Canada	Full restoration took several days.

Case studies – **REFERENCES**	
Case study 1	Becker A., Ng A., McEvoy D., Mullett J. (2018). Implications of climate change for shipping: Ports and supply chains. *Wiley Interdisciplinary Reviews: Climate Change*, e508 Ruiten K., Bles T., Kiel J. (2016). EU-INTACT-case studies: Impact of extreme weather on critical Infrastructure. E3S Web of Conferences. 7. 07001. 10.1051/e3sconf/20160707001
Case study 2	Leone F., Colas A., Garcin Y., Eckert N., Jomelli V., Gherardi M. (2014). The snow avalanches risk on Alpine roads network. *Journal of Alpine Research|Revue de géographie alpine* [Online], 102-4
Case study 3	Heinz Engel (2004). The flood event 2002 in the Elbe river basin, causes of the flood, its course, statistical assessment and flood damages. *La Houille Blanche*, 90:6, 33-36.DOI: 10.1051/lhb:200406003
Case study 4	Dobney K.,Baker C., Quinn A., Chapman L. (2009). Quantifying the effects of high summer temperatures due to climate change on buckling and rail related delays in south-east United Kingdom. *Meteorological Application*s, 16: 245-251 United Nations Economic Commission for Europe (2002). Climate Change Impacts and Adaptation for Transport Networks and Nodes. UNITED NATIONS PUBLICATION , ECE/TRANS/283
Case study 5	International Energy Agency (2005). Learning from the Blackouts. Transmission System Security in Competitive Electricity Markets. IEA PUBLICATIONS. ISBN 92 64 10961 7
Case study 6	
Case study 7	French Ministry for Sustainable Development (2009). Rupture and ignition of a gas pipeline 30 July 2004. No. 27681
Case study 8	United Nations Economic Commission for Europe (2009). Transboundary flood risk management Experiences from the UNECE region. UNITED NATIONS PUBLICATION, ECE/MP.WAT/31
Case study 9	Federal Network Agency for Electricity, Gas, Network and information systemss, Post and Railways (2007). Report on the disturbance in the German and European power system on the 4th of November 2006 Available at: www.bundesnetzagentur.de/SharedDocs/Downloads/EN/Areas/ElectricityGas/Special%20Topics/Blackout2005/BerichtEnglischeVersionId9347pdf.pdf?__blob=publicationFile&v=4
Case study 10	International Commission for the Protection of the Danube River (2008). The Analysis of the Danube Floods 2006. Available at: www.icpdr.org/main/sites/default/files/The%20Analysis%20of%20the%20Danube%20Floods%202006%20FINAL.pdf
Case study 11	Kettle A.J. (2023). Storm Kyrill and the storms of mid-January 2007: Societal and Energy Impacts in Europe. *Adv. Geosci.*, 58, 135–147
Case study 12	Petursdottir G., Reichardt U., Bird D., Donovan A., Gísladóttir G., Hauksdottir A., Johannesdottir G., Sigmundsson F., Thordardottir E.B., Ulfarsson G.F (2020). Eyjafjallajökull eruption in 2010. In: Casajus Valles A., Marin Ferrer M., Poljanšek K., Clark I. (eds.), *Science for Disaster Risk Management 2020: acting today, protecting tomorrow*, EUR 30183 EN, Publications Office of the European Union, Luxembourg, 2020, ISBN 978-92-76-18182-8, doi:10.2760/571085, JRC114026
Case study 13	FERC/NERC (2012). Arizona-South California Outages on September 8, 2011. Causes and Recommendations. Available at: www.nerc.com/pa/rrm/ea/September%202011%20Southwest%20Blackout%20Event%20Document%20L/AZOutage_Report_01MAY12.pdf
Case study 14	International Commission for the Protection of the Danube River (2008). The Analysis of the Danube Floods 2006. Available at: www.icpdr.org/main/sites/default/files/The%20Analysis%20of%20the%20Danube%20Floods%202006%20FINAL.pdf
Case study 15	Risk Management Solutions (2014). 2013–2014 WINTER STORMS IN EUROPE An Insurance and Catastrophe Modeling Perspective. Available at: https://forms2.rms.com/rs/729-DJX-565/images/ws_2013_2014_europe_winter_storms.pdf
Case Study 16	ERFA, NEE, UIRR (2018) Estimation of the economic damage of the Rastatt interruption from a rail logistics perspective see https://www.uirr.com/en/media-centre/leaflet-and-studies/mediacentre/960-estimation-of-the-economic-damage-of-rastatt-htc-study-de.html; RailEngineer (2017) Why Europe's busiest railway collapsed at Rastatt at https://www.railengineer.co.uk/why-europes-busiest-railway-collapsed-at-rastatt/; Borghetti et al (2020) Cross border critical infrastructure: a new approach for the protection evaluation, Baraldi, P., Di Maio, F., Zio, E. (Eds) Proceedings of the 30th European Safety and reliability Conference and the 15th Probabilistic Safety Assessment and Management Conference
Case Study 17	Carrega P., Une catastrophe hors norme d'origine météorologique le 2 octobre 2020 dans les montagnes des Alpes-Maritimes, Physio-Géo Géographie physique et environnement, Volume 16 | 2021. Regione Piemonte, Evento alluvionale del 2-3 ottobre 2020. Relazione a supporto della richiesta di dichiarazione dello stato di emergenza ai sensi della Direttiva del Presidente del Consiglio dei Ministri del 26/10/2012. Aggiornamento del 9 ottobre 2020. Local online Newspaper Cuneo.Dice.it, March 28 2022
Case study 18	Koks E.E., Van Ginkel K.C.H., Van Marle, M.J.E., Lemnitzer A. (2022). Communication: Critical Infrastructure impacts of the 2021 mid-July western European flood event. *NHESS*, 22: 3831–3838; EEA Report 8 (2014) Adaptation of transport to climate change. Challenges and opportunities https://www.eea.europa.eu/publications/adaptation-of-transport-to-climate
Case study 19	U.S.-Canada Power System Outage Task Force (2004). Final Report on the August 14, 2003 Blackout in the United States and Canada. Causes and Recommendations. Available at: www.energy.gov/oe/articles/blackout-2003-final-report-august-14-2003-blackout-united-states-and-canada-causes-and

Source: Authors' elaboration

3 Risk and resilience assessment and management frameworks for networks providing essential services

In this section the tools for assessing and managing transboundary threats to the physical integrity and operational continuity of lifelines are briefly discussed. Risk and resilience assessment and management will be considered as complementary and available models and methods will be briefly discussed to highlight the implications for anticipating, responding and recovering from transboundary impacts.

3.1. Risk assessment frameworks and requirements to apply them to cross-border impacts on networks providing essential services

Following Giannopoulos (2013) and Theocharidou & Giannopoulos (2015), existing methodologies for risk assessment for critical infrastructures can be divided in three main categories:

- engineering based;
- economic based;
- a combination of the latter considering as a key central element the territorial context where the infrastructures are located.

The first is actually divided in two further sub-categories. The first type of analyses focuses on the physical vulnerability of assets. Each critical infrastructure is divided into its components, some linear some point-shaped, the intrinsic fragilities of each is evaluated to identify possible causes of malfunction, error of design, lack of maintenance. The second type looks at more systemic aspects such as the organization of components at different hierarchical levels, the number of customers that rely on a given part of the system, and the physical and functional interconnections with other infrastructures.

Economic based approaches provide an estimation of costs associated to case of failures, multiple or single. Such costs can derive from the need to repair or reconstruct parts of the infrastructures, to lost revenue in case of service interruption. An interesting expansion of the economic approach relates to the estimation of costs incurred in other sectors that depend on critical infrastructures for their own functioning. In this respect for example the cost due to business interruption, lost production, failure to reach markets is derived from failures to vital services such as electricity, transportation, and increasingly communication. In this area future development can be foreseen for transboundary risk assessment, as independently from what country the initial incident to CIs has occurred, the costs in dependent sectors may be well paid by neighbouring countries. This was the case for example of the 2021 volcanic eruption in the Cordon Caulle in Chile, the impact of the ashfall almost exclusively affecting cross border areas in Argentina (Dominguez et al., 2021).

A combination of the latter approaches aims at characterizing losses by type of territory (if central metropolitan areas or remote islands or peripheral regions are involved) and by type of affected sectors, considering their intrinsic vulnerability (for example different business sector that may or not be relatively autonomous in terms of energy, water etc.). Such approach makes vast use of mapping techniques to elicit potential relationships between geographical features, exposure, vulnerabilities, and impacts.

The complexity of critical infrastructures coupled with reluctance to share data on both assets and past cases of failures makes the development of consistent and comprehensive risk assessment methods very hard to achieve (Van Eeten et al., 2018). Even more so when speaking about cross-border, transboundary infrastructures. The fora that have been created in some countries and regions for the coordination between civil protection authorities and critical infrastructure organisations provide certainly an important opportunity for getting more information and knowledge on the complex reality especially of lifelines, i.e. the Italian forum for Critical Infrastructures Protection (PIC). Nevertheless, in normal times such fora do not provide systematic access to well organized data and information, as the latter is provided occasionally and in the form of anecdotes that are rarely re-worked upon. Such fora are certainly very positive during crises as they have created a platform of people who know each other and are more inclined to collaborate. However shared risk assessment or management schemes are rarely developed.

3.2. Methods to enhance the Resilience and Operational Continuity of cross-border essential services

People's lives and their economic activities, therefore their quality of life and wealth, depend on CI functioning and service continuity; considering CI potential for producing high losses and extensive community disruptions

in case of a hazardous event, makes their resilience and operation continuity a priority. Their ability to absorb and/or adapt to the circumstances and recover in the shortest time possible from a disruption is fundamental as also explicitly exhibited in the new visions that characterizes the latest EU CER and NIS2 Directives.

Ordinary activities, in schools, universities and offices fully rely on the functioning of lifelines such as power system and network and information systems, and even more since the outbreak of the Covid-19 pandemic; banks operations and transactions or online shopping are possible only through power and telecom services, a fault of even few seconds of loss of service could lead to loss of essential data with high costs.

Bruneau et al. (2003) provide criteria to measure resilience according to a mainly engineering perspective. Such criteria are:

- Reduced failure probabilities.
- Reduced consequences from failures (i.e. damage and losses).
- Reduced time to recovery (restoration of the level of performance).

Planning, preparing, adapting and recovering within the interrelated technical, organizational, social, and economic dimensions is the essence of CI resilience. Mainly by addressing the following features:

- Robustness: strength, or ability of elements/systems to withstand a stress or demand without suffering degradation or loss of function.
- Redundancy: extent to which elements/systems are capable of accomplish functional requirements during the stress.
- Resourcefulness: capacity to identify problems, establish priorities, and mobilize resources.
- Rapidity: relates to the capacity to restore the functionality of the system in a short period of time to contain losses and avoid further disruptions.

There is however the need to complement such engineering understanding of resilience with a stronger social perspective. The pressure of the global COVID-19 crisis strained critical infrastructure into a condition never experienced before (Galbusera et al., 2021), as information technology had to transform and adapt rapidly to respond to the COVID-19 stresses, the massive shift to remote work and school on an unprecedented scale highlighted the need to shift from an object-oriented towards a more services/functions approach considering not only the technical features of the networks but also their socio-economic implications (Scholz et al. 2022).

In addition, the COVID-19 pandemic made even more manifest the importance of essential workers for the functioning of society (Scholz et al., 2022; Carvalhaes et al., 2020; Walters et al., 2020). The reliance on workforce in place (Scholz et al., 2022) to guarantee infrastructure operations, and even more so in times of crisis, should be properly considered as it creates a "social interdependency" in addition or to be integrated with the various categories of interdependencies discussed in section 2. The availability of workforce was intensely impacted by the interruption of transportation, closure of borders and the isolation policies to reduce the spread of the virus. In such a context people are not only the end-users of the services, but a crucial (skilled and qualified) element of essential services.

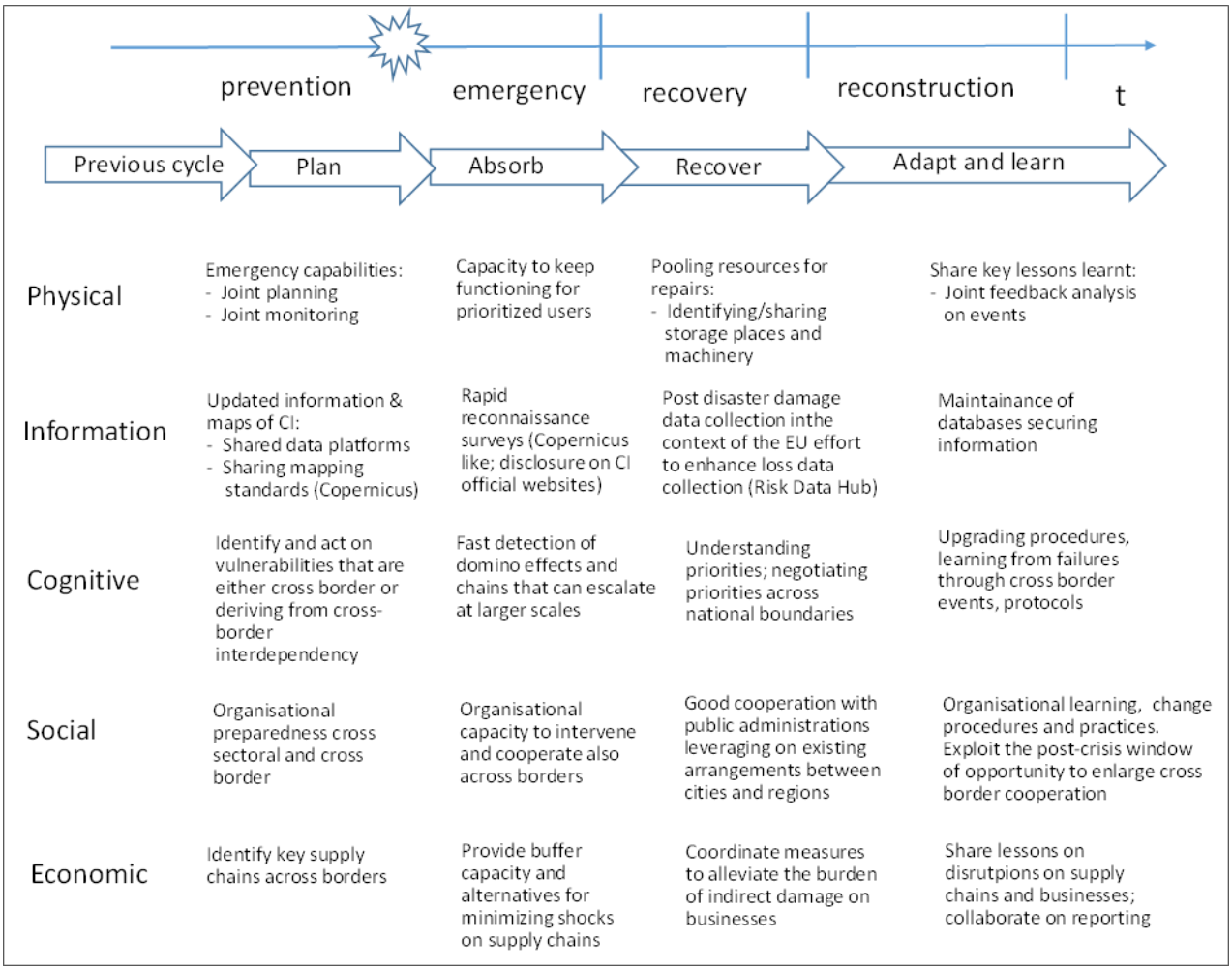
Resilience has therefore to be understood as the result of the complex interaction between society, economy and the services provided by networks. Such interaction is bi-directional. On the one hand networks are vital for the functioning of economic activities and for everyday community life; on the other the interface between human-CI must be fully appreciated for enhancing the capacity to anticipate, prevent as far as possible, but also absorb, respond and recover in a successful way. The critical capacity to address lifelines' failures and consequent recovery in the best possible ways are the essence of resilience thinking (Manyena, 2006; Jin et al., 2021). In this regard Zio (2016) stresses among other elements, the need to establish appropriate frameworks to tackle the complexity of CI, and consequently to address not only risk analysis of well-known variables but also resilience aspects relating more to the technical-human interface and to organizational vulnerabilities.

A systemic approach to assess and address resilience and operational continuity of CIs has been proposed for example by Menoni et al. (2007) building on a collaborative effort of government, public administrations, and private operators to take proper actions, strategies and working frameworks.

More recently Linkov et al. (2013) have proposed an integrated perspective bringing together technical, social, cognitive factors to assess resilience behaviour of CI.

In **Figure 6**Error! Reference source not found. we propose a re-elaborated version of the framework proposed by Linkov et al (2013) on the resilience of CI. Our framework displays what actions are needed for a more integrated cross sectoral and transboundary management of CI risks along the entire crisis cycle, from prevention to response to recovery.

Figure 6. A resilience framework for cross-border critical infrastructure risk assessment and management



Source: adapted from Linkov, 2013; re-working of the framework provided in the Educen project[15], section 3

At the core, as highlighted by the few good practices that exist (see section 3.3), there is the need to improve information sharing, to learn lessons jointly and to establish protocols for the merge of resources and means for repair. An important strand regards the collection and maintenance of data related to incidents damage, including the so-called indirect impact (second and higher order damage) as a routine task. Gathering and analysing damage and loss data on networks providing essential services proves to be challenging already at the national level, let alone across two or more countries. Here is where initiatives at the EU level could display a significant added value, like the **Risk Data Hub[16] platform** (RDH) of the Disaster Risk Management Knowledge Centre (DRMKC).

The RDH platform hosts disaster loss and risk data to support evidence-based disaster risk management activities in Europe. It enables reporting on, assessing and sharing disaster risk, damage, and loss data at the EU scale for different sectors or assets such as critical services.

---

15 Menoni, S., Atun, F., Alessandro, P., & Giordano, R. (2017). Cities and DRR. H2020 project Educen, see www.educenhandbook.eu (last accessed April 2023).

16 https://drmkc.jrc.ec.europa.eu/risk-data-hub/

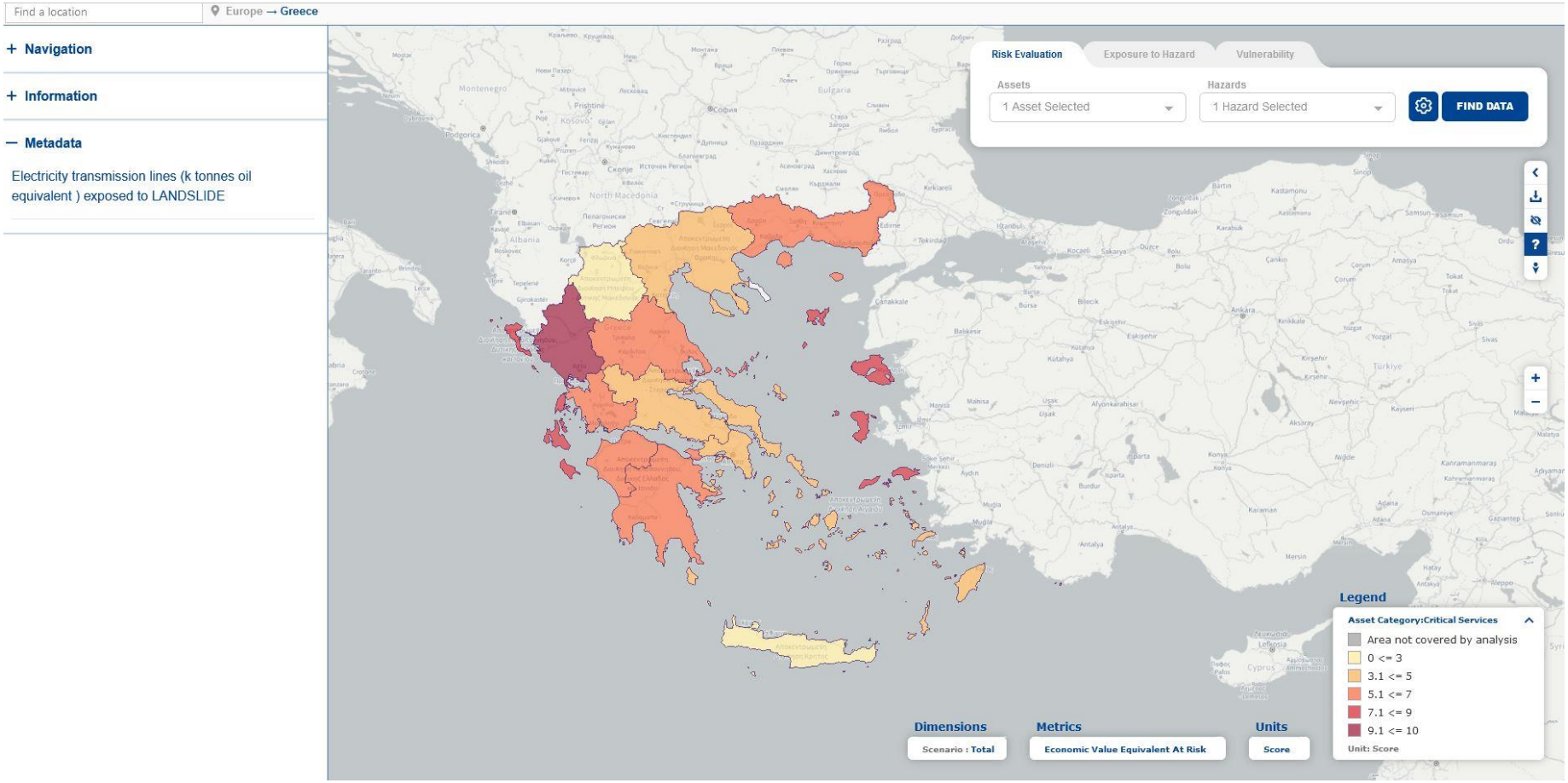
Within the RDH, critical services include the following assets: education, energy, fire departments, health facilities, others, police departments, railways, roads. The analysis of losses data is performed at different scales and hence can provide insights into local and cross-border information on disruptions to CI. Such type of implementation could add value to critical infrastructure research and disaster risk management enhancing sharing and communication among the different Member States and the multiple actors involved.

In **Figure 7** and **Figure 8**, the exposure of electricity transmission lines (k tonnes oil equivalent) to landslides was generated using the European Landslide Susceptibility Map version 2 (ELSUS_v2 - 200 m resolution), combined with the Global Precipitation Climatology Centre data layer of daily precipitation (GPCC - 5km resolution) - with the different return periods (return periods T = 2, 5, 10, 20, 50, 100, 200, 500). The data for the exposure layer of electricity transmission lines have been retrieved from a geographical database of infrastructures in Europe based on LUISA modelling platform[17].

Figure 9 shows data retrieved from the RDH loss database, with economic losses due to hydrological hazards available (coastal, river, flash floods) on critical services (infrastructure and transport) over the past 25 years in Italy.

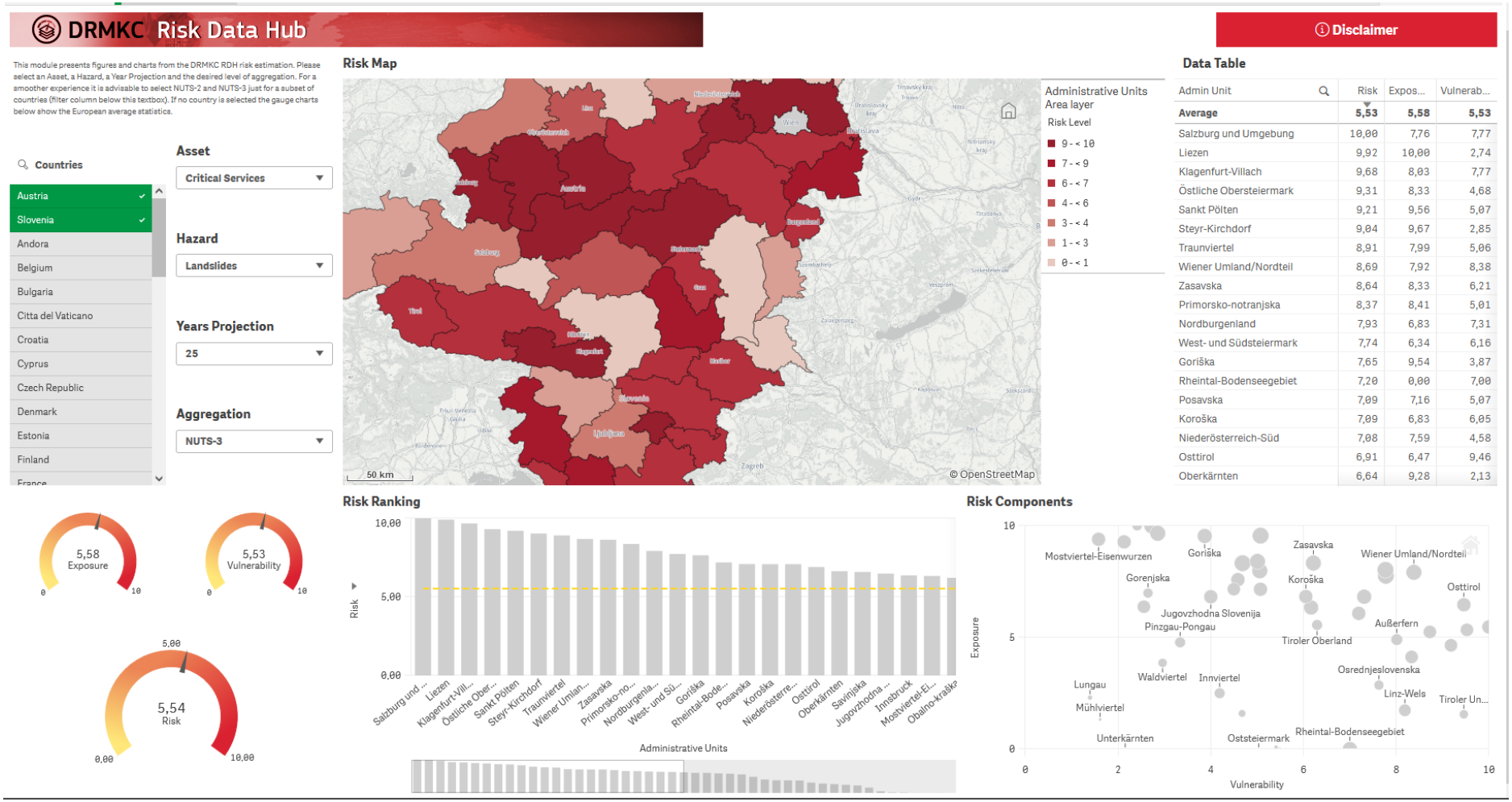
[17] Marin Herrera M, Batista e Silva F, Bianchi A, Barranco R, Lavalle C., (2015). A geographical database of infrastructures in Europe – A contribution to the knowledge base of the LUISA modelling platform. JRC Technical Report. EUR 27671 EN, doi:10.2788/22910

Figure 7. RDH application - Risk assessment for energy transmission lines in Greece due to landslides



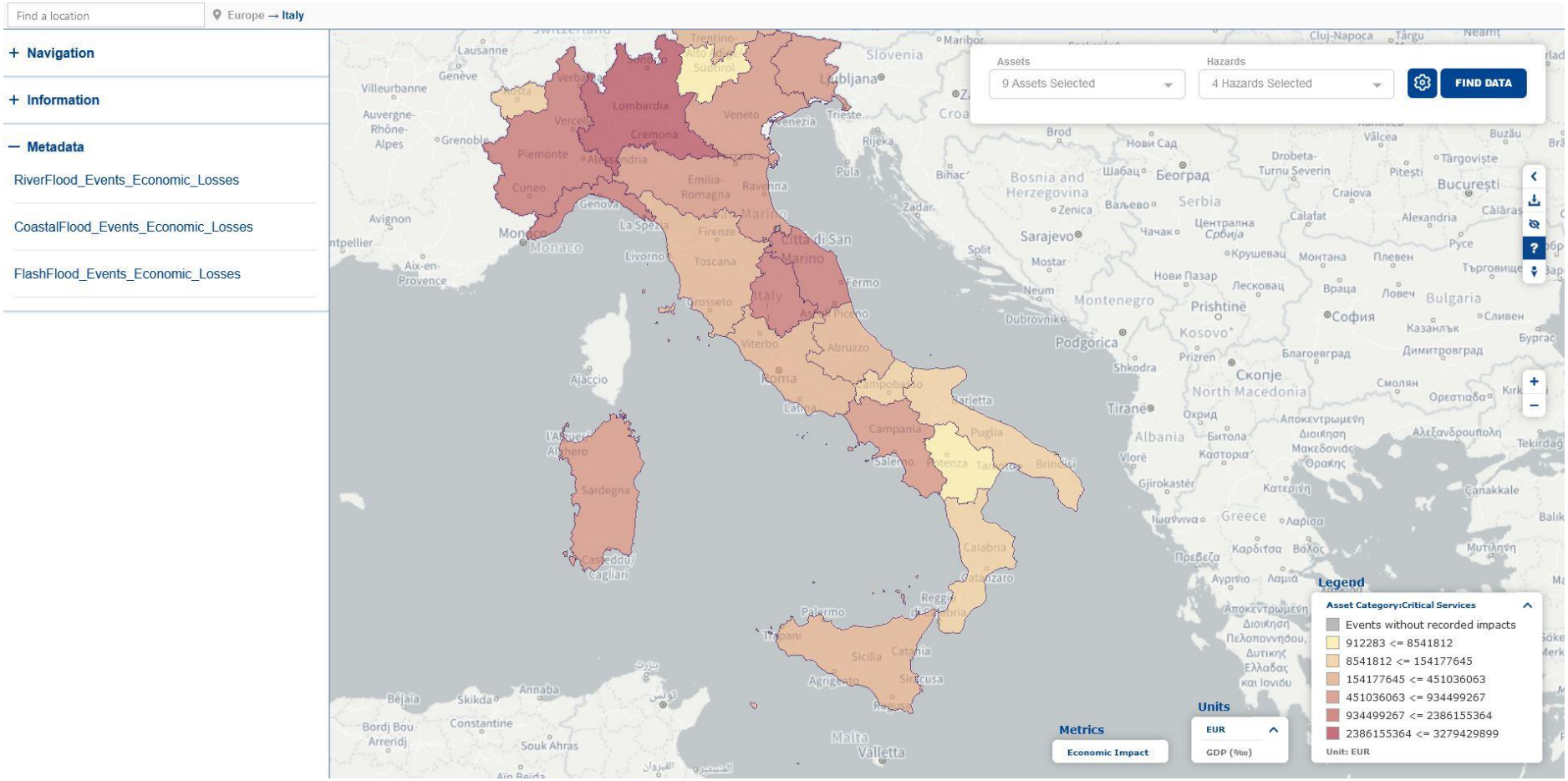
Source: RDH Risk module

Figure 8. RDH application – Analysis of risk of landslides on critical services in Slovenia and Austria at NUTS3



Source: RDH Risk dashboard

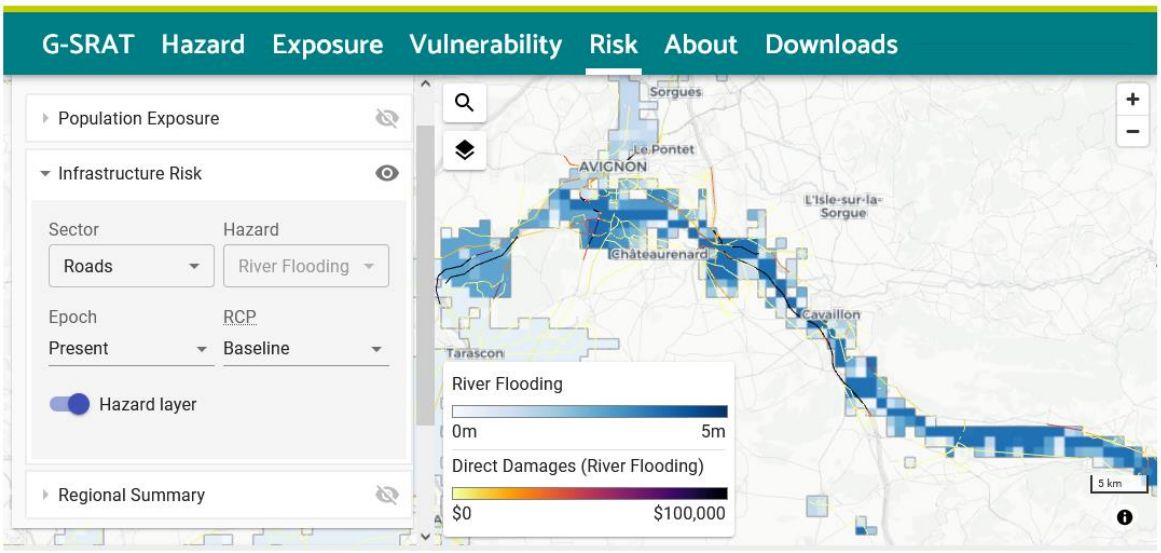
Figure 9. The data displayed are retrieved from the RDH loss database, specifically the application shows the total economic impacts of coastal, river and flash floods on critical services over the past 25 years in Italy disaggregated at regional level



Source: RDH disaster loss data module

Another recent example of on-going efforts in this regard is represented GRII's Global Systemic Risk Assessment Tool (G-SRAT) tool[18] (see **Figure 10**), a project led by the Oxford Programme for Sustainable Infrastructure Systems in the Environmental Change Institute of Oxford University and supported by different founding organizations and launched in November 2022 in COP27. The tool displays risk from climate hazards at a global scale focusing on different hazards; currently allowing to depict information about the risk of essential services such as power, rail and roads in case of river floods for the present and for future climate scenarios with forecasting up to 2080.

Figure 10. Expected Direct Damage to Road network due to risk of river flooding around the city of Avignon in France



Source: Global Systemic Risk Assessment Tool

Natural phenomena will continue to be a concern for managers of networks providing essential services across the EU, with extreme weather becoming more common due to climate change. Climate change is also provoking increasing stress on both natural and built environments.

The current rapid global changes of our time and the technological improvements that we experience in short times create conditions in which interdependencies and interconnections intensify creating a complex context in which it is increasingly difficult to reduce uncertainties and construct robust knowledge necessary to delineate operational plans and frameworks (Curt, 2018). Both CI systems (i) settings and (ii) threats (in particular climate impacts) evolve in time, leading to unexpected circumstances alongside relevant cascading and domino effects which are worsened by the strong relations existing between the various networks. The dynamicity of the conditions of the CI systems and of the served areas and people need to be contemplated to deliver efficient plans that can booster (operational) resilience addressing operational continuity, in terms both of (i) either accelerating recovery or/and (ii) forging both plans and systems able to adapt to and withstand evolving conditions in order to avoid failures.

The Covid 19 crisis has both highlighted the adaptability and resilience of network and information systems and our strong dependency on their services alongside the intense reliance on the power system. This is consistent with the findings of Van Eeten et al. (2018) who carried out an analysis of the TNO database on critical infrastructures disruption along with a sensitivity analysis using other available datasets, albeit less complete. They found that the majority of cascades originate from the power and the network and information systems, yet in a much less intense and severe way than feared by the most pessimistic visions regarding tightly coupled systems and advanced technologies (Perrow, 1984). In fact, Van Eeten et al. (2018) raise the

[18] https://www.cgfi.ac.uk/global-resilience-index-initiative/try-grii-now/

issue of the reasons behind such relatively resilient performance displayed by critical infrastructures that is coherent with observations during the pandemic.

Some authors (Hollnagel et al., 2006; Grøtan, 2014) suggest that in fact systems continue to display high levels of resilience even in the face of departure, sometimes significant, from original boundaries of safe operational conditions. Yet, beyond a given threshold systems will not be able to adapt. In the meantime, resilience imply that the possibility of failure or partial failure has to be somehow embedded in the design, striving for avoiding catastrophic failures, those with the highest potential of severe cascading, domino and escalating impacts.

On the other hand, authors such as Jin et al. (2021) warn that in order to be resilient redundancy and buffer capacity must be put in place and investment should address not only risk assessment and management for events that cannot be always anticipated and prevented, but also for recovery. Horton et al. (2022) report as an example the decisions implemented in the Dallas-Fort Worth International Airport, Texas for severe snowstorms. In the decade between two major events, 2011 and 2021, investment was made to increase the resistance capacity of the airport for accumulation of snow beyond the threshold experienced in 2011. However, when the next snowstorm occurred, whilst the airport was able to continue operations for a longer period of time compared with the previous occurrence, once the emergency fixes were overwhelmed it took much longer to recover full operations. The plea for complementing risk management practices with resilience-oriented approaches is made also in the recent opinion on Strategic Crisis Management in the EU (GCSA, 2022). In practice it means that critical infrastructure services providers should not overlook their own dependencies from others when preparing their emergency plans. It also means that plans prepared by jurisdictions at different levels should account for the potential disruption to emergency operations caused by the loss of one or more infrastructures essential to counteract the extreme events for which plans are prepared. In a subsequent recommendation, the GCSA also introduce the notion of stress testing for resilience to assess such capacity to absorb and recover from a failure building on lessons learnt, near misses to avoid large scale disruptions (Linkov et al., 2022). Therefore, resilience should be enhanced and investments properly allocated to ensure operational continuity of essential services. An interesting attempt in this direction has been carried out within a collaborative effort between a research organisation, the government of a Region and entities of the power sector in Italy as reported in **Box 2** on the risk of blackouts. As a socio-technical perspective must be taken, through this collaborative effort the minimal supply that must be guaranteed to fragile groups, to certain vital services and for which recovery must be prioritized has been agreed upon, considering also the assessments of the local communities (by Garschagen and Sandholz, 2018).

When transboundary infrastructures or cross-border impacts on networks can be foreseen, the international dimension of cooperation needs to be prepared for and managed to overcome obvious as well as sometimes unexpected challenges as proposed by Adrot et al (2022) et al who explicitly address the issue of transboundary resilience. According to them also cultural aspects must be factored in, related not only to linguistic barriers but also to how organisation and procedures work across the border. As an example, Adrot et al. (2022) mention the fact that during the July 2021 floods difficulties arose as civil protection is a national competence in Belgium, but regional in the Netherlands and in Germany with problems that are both procedural and technical.

Box 2. Electrical black-out: collaborative measures to mitigate risk

As Critical Infrastructure currently exposed and vulnerable to the increasing impacts of different types of phenomena (i.e. natural, technological, na-tech), the power system has to guarantee higher performances in service provision in terms of quality, adequacy, reliability, efficiency and resilience (Terna, 2020). With particular regard to the emerging dimension of Resilience (§ 3.2), the power system and its subcomponents are resilient if able to withstand/absorb new types of stressful conditions (Horrocks et al., 2010, Mukherjee, 2018) and return to normal operating conditions with the shortest possible delay and with the minimal level of disruption. "Power system protection supporting Resilience" has been a collaborative project between the Politecnico di Milano and the Lombardy Region (DG Territory and Civil Protection). The project resulted in guidelines delineating key preparedness measures to deal with power black-out risk in consequence of extreme weather events (heavy rainfall and snowfall, heat wave, wind storm) causing outages and/or hampering the service recovery. The direct and indirect consequences of black-outs, with cascading effects on the other CIs (in particular information technology and network and information systems, transport and traffic) have been considered. In addition to the adoption of CIs control and protection techniques/equipment, black-out risk management requires the implementation of collaborative strategies and governance actions aimed at developing co-responsibility among all the involved stakeholders (i.e. electrical power distribution operators, local authorities, exposed populations, etc.) during the entire event cycle (ante and post) in a multi-hazard/risk perspective (Abele-Wigert 2006). In this sense, some strategic measures are proposed to minimize electrical black-out risk by different categories of action differentiated for mountain and plain territorial contexts in Lombardia Region, Northern Italy. The operational guidelines aimed at: 1) increasing forecasting and monitoring capabilities of extreme weather conditions to identify preventive solutions able to reduce recovery time (preparation actions), 2) minimizing the likelihood of adverse effects of extreme weather events and improving the infrastructure's ability to withstand/absorb new stress condition (prevention actions), 3) reducing response and recovery time in case of severe weather event (response and recovery actions). Each action is detailed in terms of technical recommendations describing main goals, and expected practical outcomes (i.e. thematic maps, list of contacts, agreement proposals, etc.), the relevant territorial scale (i.e. local/provincial/regional), and the list of stakeholders involved for the implementation of those measures. In line with the European Disaster Resilience Goals (anticipate, prepare, alert, respond, secure) adopted by the European Commission on 8 February 2023 setting out common goals to boost disaster resilience in the areas of civil protection, the provided guidelines have been conceived in a way that they can inform both urban and regional plans intended as form of preparedness and prevention (i.e. in the urban or regional land use plans) and in emergency plans to support civil protection and service providers in the response and recovery. However, at European level, local authorities and aid organizations are currently insufficient to cope with the black-out disaster requiring the mobilization of interregional resources to anticipate and withstand the effects of future major disasters and emergencies. It's evident that successful risk and crisis management cannot be realized by one organization alone; cooperation is key. Moreover, the different phases of risk and crisis management – Prevention, Preparedness, Response, and Recovery – pose different challenges that become more complex considering risk management in cross-border territories, spanning state and national boundaries (Bruch et al., 2011; OSCE, 2016; Alhelou et al., 2019; Mahdavian et al., 2020). In order to respond to the problem, the provided list of measures (see **Table 6**) could be considered as starting point to better characterize technical recommendations in cross-border territories of EU Member States investigating the state of the art about existing methods and tools for producing, sharing and communicating knowledge on the topic among all the stakeholders involved at the different territorial scale. This experience has constituted not only a step forward in the cross-sectoral collaboration among actors that are needed for critical infrastructures resilience but also because it was explicitly addressing all phases of a black out event, from prevention/preparedness to response and recovery, thus showing in practice the complementarity of risk and resilience management. In case of cross-border collaboration on this specific aspect specific challenges will have to be tackled. For example, considering the spatial requirements of allocating specific areas for siting generators in case of need, different land use planning and management regimes in the two bordering countries will have to be considered; in case of resources, such as generators to be shared among communities across the border, permits and technical specifications must be agreed upon and harmonized beforehand.

Table 6. List of measures to mitigate electrical black-out risk

Event phase	Category of action	Main actions	
Ex-ante	Preparation	Identification of at risk areas in case of electrical black-out	• Mapping and monitoring of hazardous areas • Mapping and monitoring of key components of the electricity grid • Identification and mapping of strategic and vulnerable assets and users to be supplied as a priority • Maps updating • Sharing information about past hazardous events
		Alarm system definition	• Definition of an updated list of available contacts
		Definition of collaborative procedures and relationships among the involved stakeholders	• Updated and shared knowledge systems • Definition of protocols, agreements among local authorities, electricity grid operators and citizens to manage hazardous territories (i.e. Public-Private Partnerships)
	Prevention	Structural preventive works	• Maintenance of the vegetation areas close to the power lines and electrical infrastructure • Protection to hydro geological phenomena (i.e. landslides, flash floods) • Landfill of overhead lines (wherever possible and convenient)
Ex-post	Response and recovery	Fast activation of resources available on territory	• Identification and mapping of available areas for generators storage • Installation of special signboards • Mapping of fuel stations to guarantee the supply • Identification of equipment, suppliers and resources to be activated • Definition of an updated list of available contacts
		Reorganization of road and transport system	• Mapping of strategic road infrastructure for the recovery of the electricity and to provide generators where mostly needed • Definition of an updated list of available contacts
		Network and information systems system operability	• Definition of an updated list of available contacts • Providing several redundant network and information systems among local authorities and electricity grid operators • Providing an appropriate information system to citizens by radio messages and press

Source: Authors' elaboration

3.3. Good practices of cross-border cooperation

In the following some good practices of cross-border cooperation for networks are briefly illustrated. There are probably more cases and instances of such type of collaboration, however few are formalized and established since enough long time to be traced in literature. The following constitutes therefore the result of a rather extensive search in internet using different combinations of keywords such as: "transboundary collaboration, framework, arrangements for critical infrastructures protection, resilience, safety". Also searches restricted to specific networks such as power and transport have been attempted. The relatively scarce number of results may be explained on the one hand as the difficulty to report, trace such efforts in publicly available document, but also, on the other, as a signal of the scarce interest of the scientific community in assessing and studying cross-border collaboration with some exceptions (Boin and Rhinard, 2008; Adrot et al., 2022).

3.3.1. An international case: the USA and Canada collaboration

The USA and Canada signed an action plan to coordinate efforts for the protection of critical infrastructures in 2010[19], given the large number of businesses, energy and other plants close to the border and of the interconnected nature of cross border infrastructures. Three main aspects are at the core of the plan, namely: i.) building trusted partnerships; ii) improving information sharing, and iii) implementing an all-hazards risk management approach. A number of more operational actions were foreseen by the plan, such as a virtual Canada-U.S. Infrastructure Risk Analysis Cell to develop and share risk management tools and information, improved information sharing in case of incidents, work through private-public partnership to develop better analytical tools, mechanisms, and protocols for sharing sensitive information. In their national plan 2014-2017[20], the Canadian part was claiming that "The Canada-U.S. Action Plan promotes awareness of shared critical infrastructure issues, and encourages cooperation among State, Provincial, and Territorial authorities". Among the accomplished tasks under this act, annex D to the Report highlights the meetings that have been carried out on an ordinary basis between organisations managing critical infrastructures from the two countries. In the 2018-2020 Plan[21], this collaboration has been apparently extended to other countries, UK, Australia and New Zealand, that is among what are considered as trusted allies. An interesting initiative that is international refers to the EU-US-Canada annual expert meetings on risks to CI that have been running already for more than a decade, being the 11th meeting the one held in June 2022 in Paris, France. In the latter a Joint Statement was agreed upon, explicitly mentioning natural disasters and climate change as key areas of intervention for the protection of CI within other geopolitical challenges.

3.3.2. The Nordic collaboration model

Pursianen (2018) suggested that the collaboration between some Nordic countries could develop into a truly comprehensive Nordic model focusing on resilience rather than on the protection of assets. The article reviews the agreements and the tradition of collaboration that exists since long time among civil protection authorities. In this regard the relevant report by Bailes and Sandö (2014) examines in detail the process that led to the first Haga Declaration in April 2009 among ministries of different offices of the countries of Sweden, Norway, Denmark, Finland, Iceland regarding the cooperation on civil defence and the management of emergencies. Some of the constraints discussed in the latter study were overcome by the second declaration signed in Vaxholm, Sweden in June 2013. This new declaration puts much more emphasis on CI: "The Nordic countries share to a high degree the threats, risks and vulnerabilities that are the starting point for efforts to develop an effective crisis management system. An interconnected infrastructure in many spheres adds to the potential but also increase the interdependence between the countries"[22]. In a recent report on the "Nordic resilience. Strengthening cooperation on security of supply and crisis preparedness", Wigell et al. (2022) write that "The Nordic countries are all dependent on international flows of critical goods, products and services. Alone, none of them can be self-sufficient in many critical sectors, but together they have many complementarities" and "Without a joint Nordic approach, the disruptive consequences of future crises and supply disturbances risk cascading throughout the whole region. In interconnected and interdependent systems, the source of resilience lies in cooperation".

Considering the research commissioned by the Finnish National Emergency Supply Agency, the Norwegian Ministry of Trade, Industry and Fisheries and the Swedish Civil Contingencies Agency (Amundsen et al 2020), Finland, Norway and Sweden constitute a trilateral cooperation on the themes of security of supply and CI protection to prepare for potential disruptions to cross-border flows of critical goods and services. In working together to address cross-border dependencies, the countries benefit from pursuing cross-sectoral combinations of measures. In particular, the cooperation between these countries benefits from strengthening of the common information base through a mapping and analysis of cross-border interdependencies and of flows of strategic goods and products in the Nordic region. Gaining a better understanding of the current dependencies between and shared by the Nordic countries is a step towards ensuring that crucial connections are hard to exploit, disrupt or sever, either by intention, by accident, or by chance. Important issues for future

---

19 https://www.cisa.gov/sites/default/files/publications/ip-canada-us-action-plan-2010-508.pdf (last accessed May 2023)

20 https://www.securitepublique.gc.ca/cnt/rsrcs/pblctns/archive-pln-crtcl-nfrstrctr-2014-17/pln-crtcl-nfrstrctr-2014-17-eng.pdf (last accessed May 2023)

21 https://www.publicsafety.qc.ca/cnt/rsrcs/pblctns/archive-pln-crtcl-nfrstrctr-2018-20/pln-crtcl-nfrstrctr-2018-20-en.pdf (last accessed May 2023)

22 See the Haga Declaratin II at the following website: https://www.msb.se/en/about-msb/international-co-operation/nordic-co-operations/ (last accessed April 2023).

collaboration include the use of cooperative platforms for cyber security, shared contingency solutions, shared fuels during power shortages. In this regard, it's recognized that the involvement of key actors and organisations (public and private) defining the different national approaches becomes fundamental to strengthen the coherence and durability of the arrangements built together.

3.3.3. Cross-border police collaboration in Europe

Bi-lateral or multi-lateral cooperation among border police has been certainly a positive factor easing the management of crucial problems such as attempts to import goods not conforming to EU regulations into countries of the Union, in case of terrorism and illegal migration. In case of terrorism, a clear challenge has been that some attacks were planned in one country but then perpetrated in others. Transboundary effective collaboration implied therefore more than border police cooperation and required a much more transversal sharing of information also between national police forces. Border police cooperation has been certainly helpful on the occasion of incidents that were cross border as the hazards or the incidents occurred in bordering areas. Such cooperation eased the sharing of information, the mutual aid with respect to needed means, resources and specialized personnel.

3.3.4. The Euregio Meuse-Rhine Incident Control and Crisis Management interservice collaboration

The Meuse-Rhine Euroregion Incident Control and Crisis Management (EMRIC) is a collaboration of public services responsible for public safety throughout the border between France, Germany and the Netherlands. The network includes fire services, technical assistance and emergency medical care, and was established in 2006 to (i) provide local citizens with the quickest available assistance independently from the country where health care or firefighting resources could be found; (ii) ensure scaling up of capacity and resources in case of large incidents; (iii) exchange knowledge, expertise and technical know-how. It provides an excellent example of an Interreg project that was continued after its completion as a fully operational and selfsustained initiative between the three MS. It also proved its added value during the COVID 19 pandemic, when patients from Denmark were hospitalized in Germany better equipped with intensive care units.

The Euregio Meuse-Rhine still invests in projects on cross-border coordination, such as the IKIC project aiming at developing an International Knowledge and Information Centre bringing together five universities and research centres and stakeholders from the public sector in emergency management and education and training. As a response to the 2021 floods, the Meuse-Rhine Euregio launched a call for Interreg projects dealing with crisis management triggered by floods. In a presentation to the Marhetak project kick off meeting in November 2022, lack of uniform knowledge of the situation and forecast on the occasion of the July 2021 event as well as differing crisis communication towards citizens were identified as important pitfalls in the cross-border region. The evaluation of the event led to the articulation of the work packages, such as those related to joint cross-border risk assessment and coordinated management.

3.3.5. The cross-border collaboration between Italy and Switzerland

Cross-border collaboration between the Lombardy Region, Italy and the Canton Ticino, Switzerland to make possible joint coordinated intervention in case of natural disasters and incidents on the transport system goes back to more than twenty years. In 2005 an Interreg project permitted to assess the geological and hydrogeological hazards that could affect the Alpine bordering region, with impacts on both cultural heritage and CI. In the context of that Interreg project a first joint assessment and table top exercise on an incident in the second track of the railway connecting the two countries, in the tunnel Monte Olimpino 2, was simulated. In 2016 a first joint full exercise was run, called the Odescalchi exercise. A first accident in the same Monte Olimpino 2 simulating an accident to a passenger train was followed by an accident in the Chiasso station, in Switzerland, triggering a fire in the neighbouring woods propagating along the mountain slopes.

A more recent Interreg project, SICt (acronym of Safety of transboundary Critical Infrastructures)[23] has been concluded in 2022 (Borghetti et al 2020). The project was aimed at developing a platform for information sharing between Italy and Switzerland on transboundary incidents with a focus on the transportation system. It was aimed at developing shared monitoring of natural hazards and traffic conditions and on developing further

[23] https://www.progetti.interreg-italiasvizzera.eu/it/b/78/sictproject

collaboration in terms of resources and coordinated response in case of an incident or a disaster with transboundary implications. The platform that has been developed relies on advanced Geospatial techniques for visualizing in almost real time the impact of a disruption. In the context of the project a number of joint training on the developed platform were developed both online and in presence in both countries.

In 2022 a second Odescalchi exercise was set up and run, simulating a train incident at the Maccagno station in Italy. The repercussions of the incident were modelled and the intervention on both sides of the border simulated and coordinated. Despite of sharing the same language, differences in organisation, the impossibility to develop joint army or police intervention, limits the development of joint emergency plans (Borghetti et al 2020). The Interreg experience with the joint training has created therefore room for learning each other's procedures and intervention schemes, facilitating in the future coordinated emergency management.

Similarly to the example of the Meuse-Rhine Euroregion also in the case of the cross-border Alpine region between Italy and France the Roya event in October 2020 triggered research related activities. The Alcotra Interreg Programme has supported activities for gathering evidence on damage and losses suffered by the population with a questionnaire online in the context of the Concert-Eaux project on the impacts of climate change in the Roya Valley (Adrot et al., 2018).

4. Expected future developments

In this section pathways for future studies and governance frameworks are proposed, grounding on both the analysis of past cross-border incidents and of the tools and methods available for transboundary risk and resilience assessment and management.

4.1. Future developments from a conceptual/technical perspective

As for risk assessment methods, the chapter of the Recommendations for National Risk Assessments (2019) devoted to Critical Infrastructures (Theocharidou et al., 2021) addresses the challenges that are still ahead for governments in not only listing their critical infrastructures but also in developing appropriate forms of data collection and management, and in better assessing vulnerabilities due to increased interconnection and interdependencies.

The case studies in **Table 5** show that often impacts are due to a combination of hazards rather than to individual occurrences. This is because some hazards such as volcanic eruptions or storms entail a number of rather different phenomena that may affect exposed elements in many diverse ways. However, as shown by an in depth analysis conducted by Theocharidou and Giannopoulos (2015) of the methodologies, codes and tools have been developed insofar by a number of national agencies, in EU funded projects, none is fully multi-hazard and multi-sector, as would be needed.

Multi-hazardous events are increasingly considered as not only possible but potentially on the increase both because of the potential impact of climate change on different hazards and because of the increased exposure and vulnerability of assets (Menoni et al., 2017). Following the classification by Gill and Malamud (2014), there are different types of multi-hazardous events, triggered by one another or independent. Multi-hazardous events cause multi-risk conditions as damage due to one hazardous event will sum up and combine potentially with cascading effects to the impact provoked by another event occurrence. However multi-risk conditions are created also by systemic vulnerabilities and by chains of impacts in interconnected systems (Menoni and Boni, 2020), even in case only one extreme natural phenomenon has occurred. In fact, parts of CI are not only exposed and vulnerable but may also turn into hazards themselves as is the case with gas conducts or sewerage water. Due to the rising societies' dependencies on complex systems, and due to the emerging challenges posed by climate change, focusing only on the interaction between hazards (multi-hazard approach) might lead to an underestimation of risks. As the consequences of hazardous events often propagate, and especially in the field of CI multiple interconnected vulnerabilities vary and interact, a multi-risk approach would be more appropriate to handle current Ci risk assessments. Multi-risk, intended as the consideration of risk in a multi-hazard framework together with vulnerabilities interaction and dynamics (Zschau 2017) would allow to better address current and future risks for safeguarding networks providing essential services.

As an example, **Box 3** illustrates a methodology that has been developed recently in a collaboration between researchers and technical experts of a private company to assess the vulnerability and resilience to multiple hazards of datacentres (Gazzola et al 2023. Data centres must be considered nowadays as a key component of network and information systems, given the advance of cloud computing and services. Bank transactions, health care data of hospitals, data of public administrations among many others are stored and processed in data centres, that have been defined for the first time in the NIS2 Directive as assets to be protected.

Another area in which improvement should be achieved regards tools for gathering damage and loss data to CIs, possibly harmonized across Europe.

Developing **Table 5** the lack of reliable damage and loss data related to cross-border impacts on networks and essential services was a significant obstacle. Only those events for which publicly available reports or media sources such as newspapers and journals could be actually used. This situation is not different at the national level in most cases, with some exceptions as the Netherlands already discussed. However also when such data exist, their accessibility is very limited. The data problem is in fact twofold. On the one hand there is the need to allow some data sharing, at least between relevant stakeholders for crisis coordination, preparedness, and lessons learnt purposes. For example, data collected by insurance companies on insured assets should be made available at least to states and governmental agencies.

On the other hand, data is simply missing or extremely fragmented. Some data might not be available considering the rarity of some events; also, it is important to highlight that CI have undergone and keep going into a rapid process of changes and modification in the past decades, therefore the lack of data can be partially attributed to this. In the last ten years or so the DRMKC has been promoting reflection on how to improve disaster loss data collection and analysis for all sectors, including CI (De Groeve et al. 2013, 2014, 2015). As

reported by De Groeve et al (2013), data on failure of critical infrastructures is rarely collected by authorities that need later to carry out regional or national risk assessment. Post damage surveys are not coordinated among the different agencies nor between lifelines managing companies. Historical data of rare or extreme event impacts, together with base-data, would provide instead the basis to delineate better strategies, preparedness plans, test and validate models useful for a variety of other applications aimed at ensuring safe, reliable, and continuous operations.

This becomes an even larger challenge in the case of transboundary failures and impacts on CIs, as not only databases are often missing or not sufficiently populated with key information, but there is also a problem of inconsistencies, lack of harmonization in the ways damage surveys are conducted. For example, it is sometime challenging even attributing damage across border to the same storm, when the latter is named differently between MS (see the example of the storm that ravaged the Alps in 2018, named Vaia in Italy whilst Adriaan in Austria).

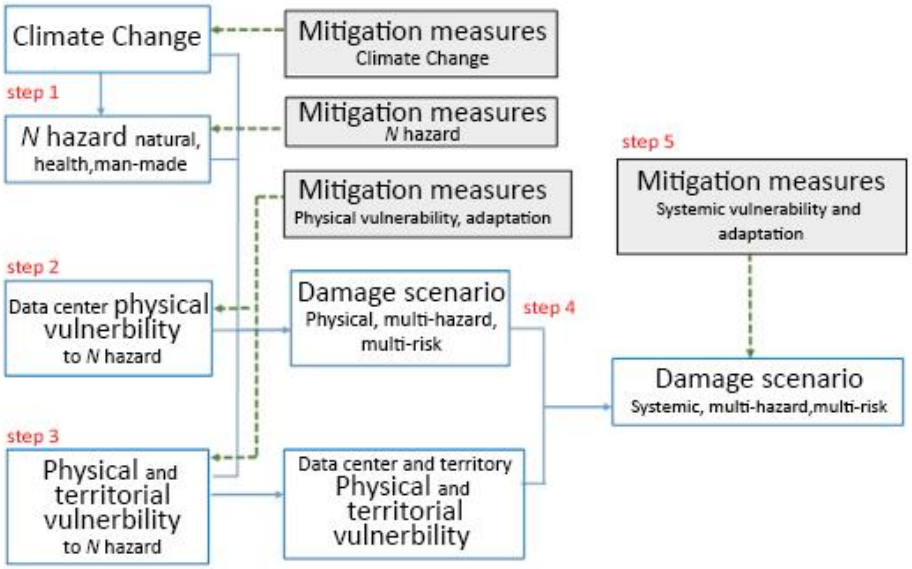
Such a context, together with the related lack of empirical data regarding the frequency and length of disruptions to end-users or connected critical infrastructures, i.e. detailed information about the loss of service experienced, its causes and propagation mechanisms, create a condition in which it becomes hard to quantify potential impacts, understand failure mechanisms, delineate efficient and effective crisis management plans. Empirical damage and loss data would instead provide the necessary base to develop more reliable models and simulations of how operational mechanisms and functioning of CI is actually disrupted by stresses provoked by natural hazards.

Box 3. Data centres: new vulnerable assets requiring attention

Over the last few decades and even more during the recent pandemic crisis, the dependence of economic activities and services on network and information systems system has increased exponentially highlighting firstly the unavoidability of digital technologies for a large amount of operations and business, educational and recreational sectors, then the need to have well-equipped reliable networks. Data centres are relatively new point shaped assets, variable in size, hosting servers, mainframes and cables necessary for storing and processing data. Not only malicious attacks but also environmental and natural risk factors could be identified as cause of various "vertical" failures involving data centres as relevant nodes in the network and information systems sector that is increasingly demanded for the type of services it can provide in terms of data storage and processing (Sandhu and Raja, 2018). Moreover, data centres are intrinsically transboundary services as evidenced by the large fire that damaged an OVHcloud data centre in Strasbourg in 2021 hampering operations of several French governmental bureaus, Vehicle Licensing Agency, and the European Space Agency. In general, the strong dependence of the network and information systems system on power, water and transport networks represents an evident element of systemic vulnerability, especially for the possible knock-on effects that could occur during a calamitous event, even in case the facilities themselves are not physically damaged. As Critical Infrastructure (CI) potentially exposed and vulnerable to the impact of different types of phenomena, data centres have to guarantee higher levels of security (physical, logical and operational), reliability and efficiency in provision of services. According to the upcoming DORA legislation on the financial sector, IT risk management framework shall include strategies, policies, procedures, instruments and protocols necessary to adequately and effectively protect all relevant infrastructures and physical components (including hardware and servers) as well as data centres and susceptible areas (art. 5). Moreover, institutions shall pursue a risk-based approach (art. 8), identifying threats and their own ability to restore ensuring business continuity (art. 9, 10). Even in their relatively short lifetime, the data centre sector has shifted from a "bunker" like type of mindset towards a clearer recognition of the many interdependencies with the external environment in which they are located.

In data centre risk assessment, it's fundamental to consider the various hazardous factors insisting on the area where data centres are located, the territorial relationships (with particular regard to electricity, network and information systems and water networks, and transport system) and the mitigation measures that can be implemented (both internally and externally) to limit the incidental events (ex-ante) and/or to prevent the consequent damage in terms of loss of data (ex-post). Taking inspiration from the Dow's Safety and Loss Prevention guidelines (1966) designed for chemical-industrial plants subject to accident risks with external releases (mainly in case of fires and explosions), the assessment of territorial risks and protection factors for the business continuity of data centres must combine the analysis of hazardous factors that could have an impact (direct, indirect or systemic) on data centres themselves and/or on their territory with the identification of prevention and protection factors that can reduce the likelihood of the accidents and mitigate their potential impact. More specifically, some evaluation steps (**Figure 11**) are essential to assess incidental scenarios with their impact assuming both the probability of hazardous conditions in the area where data centre is located and the loss of functionality of the networks serving the plant and the possible repercussions on its functionality. Then, in response to results emerged from the hazard, exposure and vulnerability evaluations, mitigation measures are defined. As a data centre could be affected by n hazards that could be multiple, co-concurrent or capable of triggering cascading phenomena, some of them influenced by Climate Change in a positive or negative way, in multi-risk conditions it's important to take into account that some mitigation measures could be used to mitigate impacts of several hazards simultaneously, some others might generate some situations of conflict, reducing vulnerability to one type of hazard (i.e. elevation to reduce flood impacts) and increasing vulnerability to another (i.e. pilotis or columns could increase the seismic vulnerability). The need for a multi-risk assessment considering the effects of interaction between events triggered by natural or mixed phenomena (Na-tech) is required by the increasing complexity of urban settlements. Moreover, the pandemic crisis has highlighted even more the need for a multi-risk approach since several operators (i.e. civil protection agencies) have had to adapt their procedures of intervention in different scenarios to the simultaneous risk of infection with Covid-19.

Figure 11. Analytical methodology for data centres multi-hazard and multi-risk assessment



Source: Authors' elaboration

4.2. Needed changes from a risk governance perspective

In the OECD report 2019[24], a toolkit has been proposed to enhance the capacity to govern critical infrastructure resilience. The seven steps that structure the framework are discussed here below with reference to the situation within the EU.

4.2.1. Setting up a multi-sector governance structure for critical infrastructure resilience

Setting up a multi-sector governance structure for CI resilience is already difficult to achieve at a country level, though coordination committees have been established both at national and regional level in many states. The OECD Report[24] lists a number of good practices of cross sectoral collaboration. For example, in Finland the National Emergency Supply Agency "has established a network of thematic clusters where key stakeholders of critical sectors, such as: food supply, energy, transportation, health or industry, develop partnerships in order to assess vulnerability and performance and plan for resilience". Láng and Mäkelä (2021) describe how such public private partnership has worked within national and European funded projects. The challenge is to transfer those initiatives across borders. Collaboration and cross border management already exists but is restricted to individual sectors, in which either the same company is managing both sides of the frontier (as in the case of energy networks) or when agreements and protocols have been signed to reinforce coping capacity and joint management (as in the case of transport routes).

4.2.2. Understanding complex (inter-)dependencies and vulnerabilities across critical infrastructure systems to prioritise resilience efforts

Understanding complex interdependencies and vulnerabilities across transboundary infrastructure systems to prioritise resilience efforts requires mutual trust and high-level political commitment that will loosen the burdens that hamper collaboration between technical bodies. This can be achieved for example through joint exercises so as to become more aware of interdependencies across sectors and by doing this improving risk assessments not only from the individual agencies or operators' perspective, but considering instead the problems that may arise in complex disasters and involve the interaction between public agencies and private companies across borders (Cedergren et al 2018).

[24] https://www.oecd.org/gov/good-governance-for-critical-infrastructure-resilience-02f0e5a0-en.htm

4.2.3. Establishing trust between governments and operators and securing information sharing on risks and vulnerabilities

A study of De Bruijne and Van Eeten (2007) defines the CI environment as "technically interconnected but institutionally fragmented". A multi-actor setting characterizes the monitoring and management of CI, in which many private and public stakeholders are involved. Private stakeholders who produce essential supplies and services, alongside public institutions which are responsible for protection and logistic of delivery, share the responsibility to prevent disruptions through joint actions, information sharing and coordination. Multiple actors with diverse roles and mandates involved in the operations and procedures, acting on different borders, together with institutional fragmentation become an obstacle for shaping resilience and protection of CI.

There is a general lack of information sharing from the private sector and government, in addition there are some other issues such as privacy regulation and classified national security information that create relevant obstacles. Most importantly damage and loss data are not always collected through appropriate procedures nor stored or managed in a systematic fashion to allow proper sharing between designated stakeholders and private or public organizations (UNDP and UNDRR, 2022).

Availability of accurate base-data and impact-related data represent an issue to overcome in order to enhance the current approaches towards CI protection and resilience building. A proper information system, designed to collect, store and manage data regarding not only the basic data of the infrastructures itself such as components and services delivered with details about the served spatial scale, but also the physical damage and cascading effects and loss of service details, would allow to move forward the current CI status.

4.2.4. Building partnerships to agree on a common vision and achievable resilience objectives

According to Crichton et al. (2009) "drifting into failure is not so much about breaking downs or malfunctioning of components, but about an organization not adapting effectively to the complexity of its structure and environment". In the case of transboundary incidents, though, the compound of cross-border organizations would need to adapt through joint structures and mechanisms that need to be in place before the incident and rely on already established practice. The introduction of resilience somehow calls for stronger cooperation and finding secure ways for information sharing for the advantage of all parties.

4.2.5. Defining the policy mix to prioritise cost-effective resilience measures across the life-cycle

This very relevant step aims at introducing resilience concerns not only around existing infrastructures, that is ex-post, but considering the entire life, starting from the design to the actual deployment and usage of the infrastructure, including its maintenance and end-of life to substitution. From a cross border perspective this implies having in place coordination teams that attend such entire life-cycle, similarly to what is envisaged in the U.S.-Canadian Agreement that encompasses all phases from prevention to recovery.

4.2.6. Ensuring accountability and monitoring implementation of critical infrastructure resilience policies

In order to enhance cross border partnership and cooperation there would be the need of a stronger impulse given by the European Commission, even though aware of the risks implied also in larger cooperation and sharing of information. In this regard the recommendation 2 on governance in the Scientific Opinion on Strategic Crisis Management in the EU can be recalled. It proposes in fact a network arrangement based on a dynamic core-periphery configuration to counteract the too loose structure of fully decentralized organisations hard to coordinate and too rigid hierarchical centralized systems. Such structure should be flexible enough to allow the entrance of new kay partners anytime their need is acknowledged given the type or evolution of a crisis. This fits very well with the environment of CI because they are partly privately run and because themselves are dynamically changing to meet new technical or geopolitical challenges. An interesting development of this idea can be foreseen considering Adrot et al (2022) who consider "the capacity to 'layer' and 'switch' between different decentralised and centralised modes of governance as a particularly significant capacity within the network".

4.2.7. Addressing the transboundary dimension of infrastructure systems

An additional step that could be added relates to the capacity of organizations individually and collectively whenever pertinent, to learn lessons from failures, exercises and incident. As correctly put by Crichton et al. (2009), cross-sectors learning is also important when events have affected systems characterized by high levels of interdependency, complexity, having components and systems tightly coupled to each other etc. Furthermore, as stated by several Authors (Crichton et al., 2009; Lagadec, 1995; Roux Dufort, 2000) learning lesson is not easy and it is even more difficult to make changes on the basis of what has been proved to be wrong and leading to vulnerabilities. Only prepared organizations are able to learn from failure, however here such learning implies the development of enough trust across the border to share the evidence of mistakes, errors, or simply malfunction of one or more components of the infrastructure.

5. Conclusions

This report constitutes a first attempt to define cross border impacts to networks providing essential services as a consequence of natural hazards.

Cross border has been intended as implying inherently a spatial aspect intertwined with the administrative, cultural, organisational factors that must be taken into consideration whenever two (or more) countries are involved. Not only direct damage to networks has been considered, but also functional, due to the systemic interconnections between the latter and the essential services they provide. Therefore, cross-sectoral, cascading, domino, escalating failures have been considered as they often characterize the second and higher order impacts that can be suffered cross-border and may actually make governance arrangements more difficult to establish.

The main objective of this report is to analyse what is available on this specific topic from case studies to methods for assessing risks and resilience that can be applied and adapted to a transboundary context. The study actually highlights that there are specific challenges to not only deal with cross border impact but even to enumerate case studies and provide satisfactory descriptions and explanation on what has actually occurred and how the cross border dimension has made a difference with respect to a disruption that is confined in one country.

Given the difficulties of finding reliable and good quality information on case studies of past impacts on networks and the limitations of currently available methodologies for assessing and manage risks and resilience across borders, in section 4 future directions of work have been foreseen. The latter have been distinguished between technical, methodological advancement and governance frameworks. Both are important to enhance the understanding and the capacity to intervene on cross border impacts on networks due to natural hazards. Some challenges have to be acknowledged and tackled, some others can be overcome in pursuing such future research and practice pathway.

As for governance, a first level of difficulty that has been encountered relates to finding good practices of cross border cooperation. There may be probably more than we were able to identify. However, in order to be able to use them as a reference for MS, they should be more investigated and better reported. Projects should be developed to search intentionally for different forms of cooperation cross-border focusing on CI through for example Interreg projects, large scale surveys among organisations in charge of CIs and civil protection, safety organisations.

A second level of difficulty relates to the fragmentation and large number of actors delivering essential services. Once the provision of the latter in Europe was a fully public concern, but following the liberalization of the energy and communication markets in the Eighties and Nineties the regime of management has been growing in complexity. Many CI have become private or semi-private and the management of the physical assets has been detached from the management of the service itself thus creating more layers that are concerned whenever a failure occurs. Along with privatization more emphasis has been put on cost-benefits concerns, that, as already mentioned, do not get along well with resilience which is more about redundancy and flexibility rather than efficiency and cost effectiveness (Perrow, 2007).

Regarding the Nordic good practice, Pursiainen (2018) highlighted the aspect of legal and structural differences that even between countries that share significant cultural and societal features exist and constitute a barrier to extensive cooperation and joint emergencies management. According to him, Europe could play an important role “If some kind of guidelines for CI resilience could be agreed upon at the EU level, this would probably make the concept more widespread for operative use, not only in the Nordic countries but also in Europe at large”.

As for technical and methodological aspects, a significant challenge for assessing risks and resilience stems from the fact that networks have become so complex and patchy that only managers inside each organization actually hold the expertise and knowledge necessary to run them properly and foresee potential problems and failures. Cross border cooperation and cooperation among sectors would require those managers to meet and cooperate in ad hoc arrangements.

From the point of view of methods and models, more research and practice should be devoted to further develop methods and models to assess and manage transboundary risk and resilience of networks providing essential services. Adrot et al (2022) call for example for more work to be done on the concept of transboundary resilience they have tried to frame. Also Sonesson (2021) argues that the application of the resilience approach to CI is still too theoretical and would require further development of criteria and indicators for measuring the extent to which resilience has improved not only within individual infrastructural systems but considering interdependencies between them.

References

Abele-Wigert I. (2006). Challenges Governments Face in the Field of Critical Information Infrastructure Protection (CIIP): Stakeholders and Perspective, in Dunn M., Mauer V. (ed.), International CIIP Handbook 2006. Vol. II. Analyzing Issues, Challenges, and Prospects. ETH Eidgenössische Technische Hochschule Zürich Swiss Federal Institute of Technology Zurich.

Adrot, A., Buscher, M., Fiedrich, F., Klein, M., Rigaud, E. et al. (2022) Transboundary Resilience. [Research Report] Université Paris Dauphine-PSL. 2022, pp.29. ffhal-03958067.

Al-Kuwaiti M., N. Kyriakopoulos, S. Hussein, (2006) Network dependability, fault-tolerance, reliability, survivability,: a framework for comprative analysis, in "Proc. The 2006 International Conference on Computer Engineering and Systems (ICCES'86)", 5 – 7 November 2006, Cairo, Egypt.

Alexander, D. (2018). A magnitude scale for cascading disasters. International Journal of Disaster Risk Reduction, 30, 180-185.

Alhelou H.H., Hamedani-Golshan M.E., Takawira Cuthbert Njenda, Siano P. (2019). A Survey on Power System Blackout and Cascading Events: Research Motivations and Challenges. Energies 2019, 12: 682.

Amundsen R., Buvarp P., Harrami O., Lindgren J., Sahlén V., Wedebrand C. (2020), Critical Nordic Flows. Collaboration between Finland, Norway and Sweden on Security of Supply and Critical Infrastructure Protection. National Emergency Supply Agency, Helsinki.

Arvidsson, B.; Johansson, J.; Guldåker, N. (2021). Critical infrastructure, geographical information science and risk governance: A systematic cross-field review. Reliability Engineering & System Safety, 213, 107741.

Bailes, A., Sandö, C. (2014).Nordic cooperation on civil security: the "Haga" process 2009-2014. Institute of International Affairs, Centre for Small States Studies, Swedish Defense Research Agency.

Boin, A., Rhinard, M. (2008). Managing transboundary crises: What role for the European Union?. International studies review, 10(1), 1-26.

Borghetti, F., Marchionni, G., Gugiatti, E., Ambrosi, C., Czerski, D., Melzi, C. (2020). Cross border critical infrastructure: a new approach for the protection evaluation, Baraldi, P., Di Maio, F., Zio, E. (Eds) Proceedings of the 30th European Safety and reliability Conference and the 15th Probabilistic Safety Assessment and Management Conference.

Bruch M., Schmid K., Kuhn M. (2011). Power Blackout Risks. Risk Management Options. Emerging Risk Initiative – Position Paper by CRO Forum. Available at: www.preventionweb.net/files/24128_powerblackoutrisks1.pdf

Bruneau, M., Chang, S. E., Eguchi, R. T., Lee, G. C., O'Rourke, T. D., Reinhorn, A. M., Shinozuka, M., Tierney, K., Wallace, W. A., & von Winterfeldt, D. (2003). A Framework to Quantitatively Assess and Enhance the Seismic Resilience of Communities. Earthquake Spectra, 19(4), 733–752 https://doi.org/10.1193/1.1623497

Carvalhaes, T., Markolf, S., Helmrich, A., Kim, Y., Li, R., Natarajan, M., Chester, M. (2020). COVID-19 as a harbinger of transforming infrastructure resilience. Frontiers in Built Environment, 6, 148.

Cedergren, A.; Johansson, J.; Hassel, H. (2018). Challenges to critical infrastructure resilience in an institutionally fragmented setting. Safety science, 110, 51-58.

Collier, S; Andrew, L. (2020). The vulnerability of vital systems: how 'critical infrastructure' became a security problem. In Dunn, MA.; Søby Kristensen K. Securing 'the Homeland' Routledge, pp. 11-39.

Crichton, M. T., Ramsay, C. G., & Kelly, T. (2009). Enhancing organizational resilience through emergency planning: learnings from cross-sectoral lessons. Journal of Contingencies and Crisis Management, 17(1), 24-37.

Curt, C., & Tacnet, J. M. (2018). Resilience of critical infrastructures: Review and analysis of current approaches. Risk Analysis, 38(11), 2441-2458.

De Bruijne, M., & Van Eeten, M. (2007). Systems that should have failed: critical infrastructure protection in an institutionally fragmented environment. Journal of contingencies and crisis management, 15(1), 18-29.Kapucu N (2009) Interorganisational coordination in complex environ- ments of disasters: the evolution of intergovernmental disaster response systems. J Homel Secur Emerg Manage. https://doi.org/ 10.2202/1547-7355.1498

De Groeve, T., Corbane, C., Ehlrich, D. (2015). Guidance for Recording and Sharing Disaster Damage and Loss Data. Report by Joint Research Centre of the European Commission, doi:10.2788/186107, available at http://drr.jrc.ec.europa.eu/Portals/0/Loss/JRC_guidelines_loss_data_recording_v10.pdf

De Groeve, T., Poljansek, K., Ehlrich, D., (2013). Recording Disaster Losses: Recommendations for a European approach. Report by the Joint Research Centre of the European Commission 10/2013; doi: 10.2788/98653.

De Groeve, T., Poljansek, K., Ehlrich, D., Corbane, C. (2014). Current Status and Best Practices for Disaster Loss Data recording in EU Member States: A comprehensive overview of current practice in the EU Member States. Report by Joint Research Centre of the European Commission, JRC92290, doi: 10.2788/18330, available at http://drr.jrc.ec.europa.eu/Portals/0/Loss/JRC%20SOTA%20Loss%20Report_11182014.pdf

Dominguez, L., Bonadonna, C., Frischknecht, C., Menoni, S., & Garcia, A. (2021). Integrative Post-event Impact Assessment Framework for Volcanic Eruptions: A Disaster Forensic Investigation of the 2011–2012 Eruption of the Cordón Caulle Volcano (Chile). *Frontiers in Earth Science*, *9*, 645945.

Dora - Proposal for a Regulation of The European Parliament and of 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 COM/2020/595 Final. Available online: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0595

Egan M. (2007). Anticipating future vulnerability: defining characteristics of increasingly critical infrastructure-like systems, Journal of Contingencies and Crisis Management, 15:1.

ENTSO, Final Report System Disturbance on 4 November 2006 union for the co-ordination of transmission of electricity. https://eepublicdownloads.entsoe.eu/clean-documents/pre2015/publications/ce/otherreports/Final-Report-20070130.pdf (last accessed April 2023).

Fekete, A., Sandholz, S. (2021). Here comes the flood, but not failure? Lessons to learn after the heavy rain and pluvial floods in Germany 2021. Water, 13(21), 3016.

Forzieri, G., Bianchi, A., e Silva, F. B., Herrera, M. A. M., Leblois, A., Lavalle, C., Aerts, J., Feyen, L. (2018). Escalating impacts of climate extremes on critical infrastructures in Europe. Global environmental change, 48, 97-107.

Galbusera, L., Cardarilli, M. and Giannopoulos, G. (2021) 'The ERNCIP Survey on COVID-19: Emergency & business continuity for fostering resilience in critical infrastructures,' Safety Science, 105161, 139, doi: 10.1016/j.ssci.2021.105161.

Garschagen M., Sandholz s. (2018). The role of minimum supply and social vulnerability assessment for governing critical infrastructure failure: current gaps and future agenda. NHESS, 18: 1233–1246.

Gazzola V., Menoni S., Ghignatti P., Marini A., Mauri R., Oldani G. (2023). Analysis of Territorial Risks and Protection Factors for the Business Continuity of Data Centers. Sustainability, 15, 6005.

GCSA - Group of Chief Scientific Advisors, Scientific Opinion No.13, November 2022. Strategic Crisis Management in the Scientific. Improving EU crisis prevention, preparedness, response and resilience (2022). European Commission, Directorate-General for Research and Innovation. doi:10.2777/517560 ISBN 978-92-76-53947-6

Gheibdoust, H. ; Gilaninia, S. ; Taleghani, M. (2023). The impact of the Ukraine war on the global food supply chain security: a literature review. International Journal of Logistics Economics and Globalisation, 10(2), 186-208.

Giannopoulos, G., Dorneanu, B., & Jonkeren, O. (2013). Risk assessment methodology for critical infrastructure protection. JRC–Scientific and Policy Report; JRC: Ispra, Italy.

Gill, J.C., Malamud, B.D. (2014). Reviewing and visualising the interactions of natural hazards. Reviews of Geophysics 52, 680.

Grøtan, T. O. (2014). Hunting high and low for resilience: Sensitization from the contextual shadows of compliance, Steenbergen et al. (Eds) Safety, Reliability and Risk Analysis: Beyond the Horizon, Taylor & Francis Group, London, 327-334.

Heri, S., Rajabifard, A., Bishop, I.D. (2010). Integrating spatial planning and disaster risk reduction at the local level in the context of spatially enabled government. Spatially enabling society: Research, emerging trends and critical assessment 1.

Hollnagel E, Woods D, Leveson N (eds) (2006) Resilience Engineering: Concepts and Precepts. Aldershot, UK: Ashgate Publishing Limited

Horrocks L., Beckford J., Hodgson N., Downing C., Davey R., O'Sullivan A. (2010). "Adapting the ICT Sector to the Impacts of Climate Change – AEA Final Report", ED 49926, no. 5.

Horton, R., Kiker, G. A., Trump, B. D., & Linkov, I. (2022). International airports as agents of resilience. Journal of Contingencies and Crisis Management, 30, 217–221. https://doi.org/10.1111/1468-5973.1240.

Jin, A., Trump, B.D., Golan, M., Hynes, W., Young, M., Linkov, I. (2021). Building resilience will require compromise on efficiency, Commentary in Nature Energy, October 20.

Jungwirth, R., Smith, H., Wilkomm, E., Savolainen, J., Alonso Villota, M., Lebrun, M., Aho, A., Giannopoulos, G. (2022). Hybrid threats: a comprehensive resilience ecosystem, Ispra: European Commission, JRC120097.

Koks, E. E., Van Ginkel, K. C., Van Marle, M. J., & Lemnitzer, A. (2022). Brief communication: Critical infrastructure impacts of the 2021 mid-July western European flood event. Natural Hazards and Earth System Sciences, 22(12), 3831-3838.

Lagadec, P. (1995). Cellules de crise. Les éditions d'organisation, Paris.

Láng, I., & Mäkelä, A. (2021). Lessons learned from working with windstorm-related impact data (No. EGU21-8288). Copernicus Meetings.

Linkov, B.D. Trump, J. Trump, G. Pescaroli, W. Hynes, A. Mavrodieva, A. Panda, Resilience stress testing for critical infrastructure, International Journal of Disaster Risk Reduction (2022), doi: https://doi.org/10.1016/j.ijdrr.2022.103323

Linkov, I., Eisenberg, D. A., Bates, M. E., Chang, D., Convertino, M., Allen, J. H., ... & Seager, T. P. (2013). Measurable resilience for actionable policy.

Luiijf, E., & Klaver, M. (2021). Analysis and lessons identified on critical infrastructures and dependencies from an empirical data set. International Journal of Critical Infrastructure Protection, 35, 100471.

Mahdavian, F., Platt S., Wiens M., Klein M., Schultmann F. (2020). Communication blackouts in power outages: Findings from scenario exercises in Germany and France. International Journal of Disaster Risk Reduction, 46.

Manyena, S. B. (2006). The concept of resilience revisited. Disasters, 30(4), 434-450.

Menashri, H., & Baram, G. (2015). Critical infrastructures and their interdependence in a cyber attack–the case of the US. Military and strategic Affairs, 7(1), 22.

Menoni, S., & Boni, M. P. (2020). A systemic approach for dealing with chained damages triggered by natural hazards in complex human settlements. International Journal of Disaster Risk Reduction, 51, 101751.

Menoni, S., & Margottini, C. (Eds.). (2011). Inside risk: a strategy for sustainable risk mitigation. Springer Science & Business Media.

Menoni, S.; Bondonna, C.; Garcia Fernandez, M.; Schwarze, R. (2017). Recording disaster losses for improving risk modelling capacities. In Poljansek K., M. Martin Ferrer, T. De Groeve, I. Clark (eds.) "Science for disaster risk management 2017. Knowing better and losing less", European Commission, DG-JRC

Menoni, S.; Pergalani, F.; Boni, M.P.; Petrini, V.; (2007). Lifelines earthquake vulnerability assessment: a systemic approach. In: Linkov, Igor, Wenning Richard, Kiker Gregory. Risk Management Tools For Port Security, Critical Infrastructure, and Sustainability. p. 111-132. NATO Series, Springer.

Mukherjee B. (2018). Network Adaptability from Disaster Disruptions and Cascading Failures, Network Adaptability from Weapon of Mass Destruction Disruption and Cascading Failures.

Necci, A. and Krausmann, E. (2022). Introduction to eNATECH, Publications Office of the European Union, Luxembourg, JRC130281.

Nojima N. (1998) Lifeline system malfunction and interaction. Proceedings of the World Urban-Earthquake Conference in Fukui. June.

OSCE (2016). Organization for Security and Co-operation in Europe. Protecting Electricity Networks from Natural Hazards. Available at: https://pure.iiasa.ac.at/id/eprint/13849/1/242651.pdf

Oxford-Economics (2010). The Economic Impacts of Air Travel Restrictions Due to Volcanic Ash, Technical Report for Airbus.

Park J.; Seager, T. P.; Rao, P. S. C.; Convertino, M.; Linkov, I. (2013). Integrating risk and resilience approaches to catastrophe management in engineering systems. Risk analysis, 33(3), 356-367.

Perrow, C. (1984; second edition Princeton University Press 1999) Normal accidents. Living with high risk technologies, Basic Books, New York.

Perrow, C. (2007). The Next Catastrophe: Reducing Our Vulnerabilities to Natural, Industrial, and Terrorist Disasters, Princeton University Press.

Petit, F., Verner, D., Brannegan, D., Buehring, W., Dickinson, D., Guziel, K., ... & Peerenboom, J. (2015). Analysis of critical infrastructure dependencies and interdependencies (No. ANL/GSS-15/4). Argonne National Lab.(ANL), Argonne, IL (United States).

Pitilakis, K., Franchin, P., Khazai, B., & Wenzel, H. (Eds.). (2014). SYNER-G: systemic seismic vulnerability and risk assessment of complex urban, utility, lifeline systems and critical facilities: methodology and applications (Vol. 31). Springer.

Poljansek, K., Casajus Valles, A., Marin Ferrer, M., Artes Vivancos, T., et al (2021) Recommendations for national risk assessment for disaster risk management in EU: where science and policy meet, Version 1, EUR 30596 EN, Publications Office of the European Union, Luxembourg, 2021, ISBN 978-92-76-30256-8, doi:10.2760/80545, JRC123585.

Poljanšek, K., Casajus Valles, A., Marin Ferrer, M., De Jager, A., Dottori, F., Galbusera, L., Garcia Puerta, B., Giannopoulos, G., Girgin, S., Hernandez Ceballos, M., Iurlaro, G., Karlos, V., Krausmann, E., Larcher, M., Lequarre, A., Theocharidou, M., Montero Prieto, M., Naumann, G., Necci, A., Salamon, P., Sangiorgi, M., Sousa, M. L, Trueba Alonso, C., Tsionis, G., Vogt, J., and Wood, M. (2019). Recommendations for National Risk Assessment for Disaster Risk Management in EU , EUR 29557 EN, Publications Office of the European Union, Luxembourg, 2019, ISBN 978-92-79-98366-5 (online), doi:10.2760/084707 (online), JRC114650.

Pursiainen, C. (2018). Critical infrastructure resilience: A Nordic model in the making?. International journal of disaster risk reduction, 27, 632-641.

Rehak, David; Hromada, Martin; Novotny, Petr. (2016). European Critical Infrastructure Risk and Safety Management: Directive Implementation in Practice. 15th international symposium on Loss Prevention and Safety Promotion (LOSS 2016) Book Series: Chemical Engineering Transactions Volume: 48 Pages: 943-948.

Remko, V.H. (2020) 'Research opportunities for a more resilient post-COVID-19 supply chain – Closing the gap between research findings and industry practice', International Journal of Operations and Production Management, 40, pp. 341–355. doi: 10.1108/IJOPM-03-2020-0165.

Rinaldi, S. M. (2004, January). Modeling and simulating critical infrastructures and their interdependencies. In 37th Annual Hawaii International Conference on System Sciences, 2004. Proceedings of the (pp. 8-pp). IEEE.

Rinaldi, S. M., Peerenboom, J. P., & Kelly, T. K. (2001). Identifying, understanding, and analyzing critical infrastructure interdependencies. IEEE control systems magazine, 21(6), 11-25, www.ce.cmu.edu/~hsm/im2004/readings/CII-Rinaldi.pdf.

Rose, A. (2004). Economic principles, issues, and research priorities in hazard loss estimation. Modeling spatial and economic impacts of disasters, 13-36.

Roux-Dufort, C. (2000). La gestion de crise: un enjeu stratégique pour les organisations. De Boeck Supérieur.

Sandhu, H. S., S. Raja. (2018). "No Broken Link: The Vulnerability of Network and information systems Infrastructure to Natural Hazards." Sector note for LIFELINES: The Resilient Infrastructure Opportunity, World Bank, Washington, DC.

Sawalha, I. H. S. (2014). Collaboration in crisis and emergency management: Identifying the gaps in the case of storm 'Alexa'. Journal of Business Continuity & Emergency Planning, 7(4), 312-323.

Scholz C., Latzenhofer M., Schauer S. (2022). The Emergence of New Critical Infrastructures. Is the Covid-19 Pandemic Shifting Our Perspective on What are Critical Infrastructures?. Available at SSRN: https://ssrn.com/abstract=4108980.

Sonesson T.R., Johansson J, Cedergren A. (2021) Governance and interdependencies of critical infrastructures: Exploring mechanisms for cross-sector resilience, Safety Science 142.

Tavares Da Costa, R. and Krausmann, E. (2021). Impacts of Natural Hazards and Climate Change on EU Security and Defence, EUR 30839 EN, Publications Office of the European Union, Luxembourg, ISBN 978-92-76-41947-1, doi:10.2760/244397, JRC126315.

Terna, (2020). Piano di sviluppo 2020. Available at: https://download.terna.it/terna/Piano%20di%20Sviluppo%202020_8d7db1ffa4ca9e7.pdf

Thacker, S.; Adshead, D.; Fay, M.; Hallegatte, S.; Harvey, M.; Meller, H., ... & Hall, J. W. (2019). Infrastructure for sustainable development. Nature Sustainability, 2(4), 324-331.

Theocharidou M., Giannopoulos G. (2015) Risk assessment methodologies for critical infrastructure protection. Part II: A new approach. Report EUR 27332 EN, Luxembourg: European Union — Publications Office.

Theocharidou, M., Galbusera, L., Giannopoulos, G. (2021) Critical infrastructure disruption, Poljanšek, K., Casajus Valles, A., Marín Ferrer, M., Recommendations for National Risk Assessment for Disaster Risk Management in EU. Where Science and Policy meet, JRC Science for Policy Reports, Version 1.

UNDP and UNDRR (2022) Addressing the data gap: analysis of infrastructure damages and service disruption in PDNAs, Report. https://reliefweb.int/report/world/addressing-data-gap-analysis-infrastructure-damages-and-service-disruption-pdnas (last accessed May 2023).

Van Eeten, M., Nieuwenhuijs, A., Luiijf, E., Klaver, M., Cru, E. (2018). The state and the threat of cascading failure across critical infrastructures: the empirical evidence from media incident report, Public Administration, 89: 2, 381–400.

Walters, L., Wade, T., & Suttles, S. (2020). Food and agricultural transportation challenges amid the COVID-19 Pandemic. Choices, 35(3), 1-8.Lagadec P., Cellules de crise. Les conditions d'une conduite efficace. Les Èditions d'Organisations, 1995, Paris.

Wigell, M., Hägglund, M., Fjäder, C., Hakala, E., Ketola, J., Mikkola, H., (2022). Nordic resilience. Strengthening cooperation on security of supply and crisis preparedness, Finnish Institute of International Affairs, Report.

Zio, E. (2016). Challenges in the vulnerability and risk analysis of critical infrastructures. Reliability Engineering & System Safety, 152, 137-150.

Zschau, J. (2017). Where are we with multihazards, multirisks assessment capacities? In: Poljanšek, K., Marín Ferrer, M., De Groeve, T., Clark, I. (Eds.). Science for disaster risk management 2017: knowing better and losing less. EUR 28034 EN, Publications Office of the European Union, Luxembourg, Chapter 2.5, doi: 10.2788/688605.

European projects

CIPRNet (FP7)

Educen (www.educenhandbook.eu)

Lode (Loss Data Enhancement for DRR & CCA Management), DG ECHO, www.lodeproject.polimi.it

Improve (Improved risk evaluation and implementation of resilience concepts to critical infrastructure) project Horizon 2020, 2015-2018, https://cordis.europa.eu/project/rcn/196889/factsheet/en

Intact FP 7 project on the impact of weather-related hazards on CI

List of abbreviations and definitions

CER	Directive on the Resilience of Critical Entities
CI	Critical Infrastructure
CIP	Critical Infrastructure Protection
CSIRT	Computer Security Incident Response Team
ECI	European Critical Infrastructures Directive 2008/114/EC
EFTA	European Free Trade Association
ENISA	European Union Agency for Network and Information Security
EWE	Extreme weather events
MS	Member State
NIS	Security of Network and information systems (Directive)
NIS2	NIS 2 Directive replaces and repeals the NIS Directive
PICRIT	Protecting International Critical Infrastructures
SWD	Staff Working Document
TNO	Netherlands Organisation for Applied Scientific Research
UNECE	United Nations Economic Commission for Europe

List of boxes

Box 1. Natural Phenomena causing long lasting incidents to network and information systems sector (analysis of ENISA reports) 10

Box 2. Electrical black-out: collaborative measures to mitigate risk 35

Box 3. Data centres: new vulnerable assets requiring attention 42

List of figures

Figure 1. Structure of the report 7

Figure 2. Incidents share by cause 11

Figure 3. User hours lost per root cause category – multi-annual 2012-2020 (% of total user hours lost) 12

Figure 4. Cascading impacts framework (Menoni & Boni, 2020**)** 14

Figure 5. Map locating the various cross-border incidents described in **Table 5** 17

Figure 6. A resilience framework for cross-border critical infrastructure risk assessment and management 28

Figure 7. RDH application - Risk assessment for energy transmission lines in Greece due to landslides 30

Figure 8. RDH application – Analysis of risk of landslides on critical services in Slovenia and Austria at NUTS3 31

Figure 9. The data displayed are retrieved from the RDH loss database, specifically the application shows the total economic impacts of coastal, river and flash floods on critical services over the past 25 years in Italy disaggregated at regional level 32

Figure 10. Expected Direct Damage to Road network due to risk of river flooding around the city of Avignon in France 33

Figure 11. Analytical methodology for data centres multi-hazard and multi-risk assessment 43

List of tables

Table 1. Some criteria that supports the identification of CI and essential services 4

Table 2. Criteria to define cross-border impacts 9

Table 3 Comparison between the years in which Natural Phenomena have reached relative peaks 12

Table 4. Types of multiple impacts in Critical Infrastructures 14

Table 5. Case studies of events with significant cross-border impacts on networks providing essential services 18

Table 6. List of measures to mitigate electrical black-out risk 36

GETTING IN TOUCH WITH THE EU

In person

All over the European Union there are hundreds of Europe Direct centres. You can find the address of the centre nearest you online (european-union.europa.eu/contact-eu/meet-us_en).

On the phone or in writing

Europe Direct is a service that answers your questions about the European Union. You can contact this service:

— by freephone: 00 800 6 7 8 9 10 11 (certain operators may charge for these calls),

— at the following standard number: +32 22999696,

— via the following form: european-union.europa.eu/contact-eu/write-us_en.

FINDING INFORMATION ABOUT THE EU

Online

Information about the European Union in all the official languages of the EU is available on the Europa website (european-union.europa.eu).

EU publications

You can view or order EU publications at op.europa.eu/en/publications. Multiple copies of free publications can be obtained by contacting Europe Direct or your local documentation centre (european-union.europa.eu/contact-eu/meet-us_en).

EU law and related documents

For access to legal information from the EU, including all EU law since 1951 in all the official language versions, go to EUR-Lex (eur-lex.europa.eu).

Open data from the EU

The portal data.europa.eu provides access to open datasets from the EU institutions, bodies and agencies. These can be downloaded and reused for free, for both commercial and non-commercial purposes. The portal also provides access to a wealth of datasets from European countries.

Science for policy

The Joint Research Centre (JRC) provides independent, evidence-based knowledge and science, supporting EU policies to positively impact society

EU Science Hub
joint-research-centre.ec.europa.eu

@EU_ScienceHub
EU Science Hub - Joint Research Centre
EU Science, Research and Innovation
EU Science Hub
@eu_science

Publications Office
of the European Union