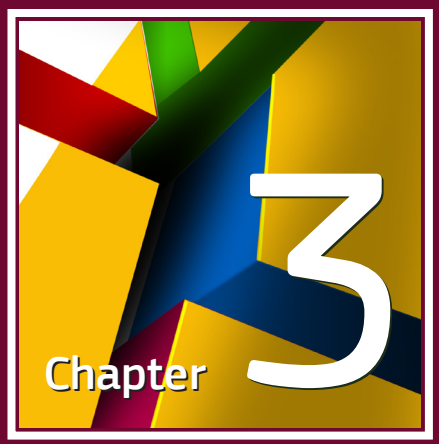


Assets at risk and potential impacts

3.4

Critical infrastructures

Coordinating Lead Authors

John Agius

Georgios Marios Karagiannis

Online Version

Agius, J., Karagiannis, G.M., Pescaroli, G., Galbusera, L., Theocharidou, M., Krausmann, E., Chaudhari, K., 'Critical Infrastructures', 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.

3.4 Critical Infrastructures

CONTENTS

3.4 Critical Infrastructures

Introduction

Critical infrastructure (CI) provides the essential services that underpin modern societies and support national economies. CIs are complex, adaptive, sociotechnical and highly interdependent systems that can fail less predictably than our technological prowess allows for. Moreover, CIs are most often designed in a fragmentary manner, the design of each system considering a mere fraction of its interactions with other systems. Urban populations rely heavily on critical infrastructures, making their protection a major issue, particularly for megacities.

The strategic importance of some assets of the built environment, such as aqueducts and roads, has been known at least since Roman times. As our society evolved and developed an industrial economy including a system of production, our consumption and day-to-day activities are more reliant on technology, long-range supply lines and interconnected networks with the result that our contemporary society, is more vulnerable to the impact of potential disruptions'. Conducted pursuant to a directive by President Franklin Roosevelt, the United States Strategic Bombing Survey estimated that the Second World War air raids would have been more effective if they had targeted electricity-generating plants instead of urban and industrial areas (Air University, 1987). This chapter focuses on CI, construed as 'The physical structures, facilities, networks and other assets which provide services that are essential to the social and economic functioning of a community or society' (UNDRR Glossary, 2017, p. 12).

The national definitions of CI and related sectors have changed over time in response to the complexity of the built environment and society, and changes in strategic needs (Lazari, 2014). The definition of CI has evolved throughout history. For example, power plants were considered in this category during the Cold War, and received more attention in the late 1990s during the Clinton administration, which recognised this trend through Presidential Decision Directive PDD-63 (White House, 1998). Some key events have pushed and pulled practitioners towards a new approach to CI protection. These include the renewed attention to terrorist threats, following the attacks in New York (2001), Madrid (2004) and London (2005), as well as major disasters such as the Indian Ocean tsunami in 2004 and Hurricane Katrina in 2005 (Lazari, 2014). Resilience of CIs includes considerations of their physical, informational, cognitive and social domains, because their technological components cannot be separated from the wider implications of dealing with disruptions (Linkov et al., 2014).

In the EU, in June 2004, the European Council called for the preparation of an overall strategy to protect CIs in Europe. On 20 October 2004, the Commission adopted a communication on critical infrastructure protection (CIP). The communication put forward suggestions on how to enhance European efforts to prevent, prepare for and respond to disruptions to CIs resulting from terrorist attacks. In December 2004, the Council endorsed

the intention of the Commission to propose a European Programme for Critical Infrastructure Protection (EPCIP). In November 2005, the Commission published a Green Paper on the EPCIP. The Green Paper presented a combination of measures intended to be viewed as complementary to CI national efforts at the time. On 12 December 2006, the Commission issued a communication on the EPCIP. In its communication, the Commission set out an overall policy approach and framework, including an action plan for CIP in the EU (European Commission, 2006).
Following the creation of the programme in 2006, the Critical Infrastructure Warning Information System (CIWIN) and the CIP expert group were established. In December 2006, the Commission published a proposal for a directive of the Council on the identification and designation of European CIs and the assessment of the need to improve their protection.

Council Directive 2008/114/EC was adopted on 8 December 2008 (EU, 2008). It establishes a procedure for identifying and designating European critical infrastructures (ECIs) and a common approach for assessing the need to improve their protection. Article 3 of the directive limits its scope to the energy and transport sectors while providing for the eventuality of considering the inclusion of subsequent sectors at a later review stage.

The directive defines a critical infrastructure as 'an asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions' (Article 2).
In simple terms, a CI is an asset, system or part thereof that if disrupted for any reason can bring a Member State to its knees. Hence the importance of protecting CIs. What emerges from the definition of a CI as depicted in the directive is the association of the physical disruption of a CI with the loss of functional assets in society.
Moreover, the directive identifies European critical infrastructures. The definition of an ECI introduces the cross-sectoral elements and cross-border dependencies of disruption associated with those elements whose disruption engenders consequences in two or more EU Member States. (Article 2(b)).

In its EPCIP, the European Commission encourages all Member States to include in their programmes the impact of CI disruptions in terms of scope, severity, population affected, economic losses, environmental effects, political effects, psychological effects and public health consequences (European Commission, 2006, p. 7).

No CI operates in isolation. As a result, a disruption within one CI can trigger cascading effects on related,

associated and other relevant assets and/or systems. Cascading effects can be defined as 'the dynamics present in disasters, in which the impact of a physical event or the development of an initial technological or human failure generates a sequence of events in human subsystems that result in physical, social or economic disruption. Thus, an initial impact can trigger other phenomena that lead to consequences with significant magnitudes'.
Cascading effects can result in 'cascading disasters', whereby secondary emergencies can be caused by existing vulnerabilities (Pescaroli and Alexander, 2015, p. 64). These can quickly become the centre of a crisis and can challenge the coordination of emergency relief and long-term recovery. Cascading effects raise issues of interdependencies whereby 'new and emerging threats faced by critical infrastructure assets and systems, in conjunction with the interdependencies among them at national and European level, makes it virtually impossible to keep addressing critical infrastructure safety in the traditional, hazard-based way (Agius et al., 2017, p. 387).

Experience from recent disasters, together with the scientific literature, has provided evidence of the dependencies among critical infrastructures, highlighting pathways of cross-sectoral and cross-border failures. The next sections analyse how critical infrastructures shape the disaster risk environment of communities and nations. The focus is on the vulnerabilities generated by the increasing reliance of modern economies on critical infrastructure, the challenges of interdependent systems, the options for building resilience into the design of such systems, and the need to pay particular attention to infrastructure in comprehensive emergency management, including mitigation, preparedness, response and recovery. The ultimate goal of this subchapter is to broaden the understanding of current and future risks related to critical infrastructure, thus contributing towards a more resilient and sustainable Europe.

Section 3.4.1 provides an analysis of the essential concepts and the challenges associated with organisational resilience and continuity management for emergency facilities. Emergency services are complex sociotechnical systems spanning all levels of government and include a wide range of facilities, personnel, plans, equipment and organisational arrangements. The role of emergency facilities in the disaster cycle is elaborated through their operational obligations in a European context while they also need to ensure the sustainability of mitigation and response. The procedures and practices that create operational resilience are then defined, explaining how cascading effects can affect the resilience at the organisational level and the level of individual operators. The section concludes by providing a set of examples and lessons learned, integrating them into practical advice and guidelines for continuity management and policies formulated in order to reduce vulnerability and increase flexibility during worst-case scenarios.

Section 3.4.2 discusses networked infrastructures, that is, those systems made up of interconnected assets distributed over a large geographical area, or those with numerous interacting components and functions. The centrality of these networks provides some degree of resilience by design. However, it is due to this network centrality that fragilities are not only intrinsic to each technological layer but can manifest at the boundaries among systems. Therefore, networked infrastructure systems can be channels for the propagation of disasters' consequences, mediators of mitigation actions or both. Considerations from cases in which natural hazards or human acts caused significant impacts are used to illustrate these attributes. Situations in which intrinsic network failures resulted in unprecedented consequences are also considered.

Among all critical infrastructure sectors, electric power is a cornerstone of modern economies. Electricity is ubiquitous in the daily lives of European citizens and spans all sectors of the European economy. In addition,

all critical infrastructure systems depend, to a greater or lesser extent, on the reliable delivery of electricity. Long-term power outages can slow down disaster recovery efforts and severely disrupt the economy of affected communities (Karagiannis et al., 2017). On a similar note, transport networks are expansive, open, accessible and interconnected systems, the sheer size and capacity of which move, distribute and deliver billions of passengers and millions of tonnes of goods each year across Europe. Transportation becomes a critical issue when aid and resources need to be channelled quickly and efficiently in disaster-affected areas. Yet these systems are exposed and vulnerable to all types of human-made and natural hazards. The authors of Section 3.4.2 focus on exposure mitigation, with the objective of identifying gaps and describing lessons learned, which lessons may be relevant to risk analysis and the management of future crisis scenarios.

Section 3.4.3 addresses risks to society and the environment from damage to core industrial and energy facilities due to human-made and natural hazards and how these impacts can be prevented or reduced in the future. Using case studies, the authors highlight how communities can be affected by such incidents, including via cascading (also referred to as 'ripple') effects due to interdependencies between systems and sectors. Examples of solutions for improved risk and impact mitigation based on lessons learned from past events are then provided. Practices and actions for the different stakeholder groups (policymakers, practitioners and scientists) are proposed, and how the citizens can better understand and be involved in related risk reduction is also discussed.

Lastly, Section 3.4.4 discusses the role of communication systems and their varying degrees of responsibility for the transfer of information of differing levels of criticality. Establishing and sustaining interoperable communications is a critical prerequisite for emergency response. Failures in communications systems have often been blamed for several challenges in emergency response. Also discussed are considerations of information and communication systems as critical infrastructures themselves. Rapid advances in technology are noted in the context of the rapidly developing communication systems and services and the advent of fifth-generation mobile technology. Because of the potential for information isolation, the dependency of European societies on information and communication systems is an essential element of the societal impact of the digital divide. In addition, cybercrime and cyberterrorism are opening up new disaster scenarios, which could range from local to global and from minor to catastrophic. The potential failure of communication systems can easily have cascading impacts on other critical infrastructures. Two case studies are featured, with concluding remarks on what measures are essential for the appropriate operation and use of communication systems in building resilience with a view to protecting CIs.

3.4.1 Emergency infrastructure and facilities

Lead Author:

Gianluca Pescaroli *University College London, United Kingdom*

Contributing Authors:

David Alexander *University College London, United Kingdom*

Virginia Murray *Public Health England, United Kingdom*

Pescaroli, G., Alexander, D., Murray, V., 'Emergency infrastructure and facilities', 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.

1 Introduction

Emergency facilities and infrastructure are essential assets for society, but they need to maintain their resilience and operational continuity.

Emergency facilities and infrastructure (EMFIs) are essential components of society's mechanism, as they can make the difference in addressing crises. For example, fire engines, police cars or ambulances deploy from a backbone of stations and coordination centres that have the duty to respond to adverse conditions that could disrupt the functions of a community. EMFIs are part of the vital networks and assets that allow the delivery of emergency services, which are defined by the United Nations Office for Disaster Risk Reduction as 'a critical set of specialised agencies with specific responsibilities and objectives in serving and protecting people and property in emergency situations' (UNISDR, 2017). They include first responders, such as fire service personnel, police, primary healthcare operatives, civil protection responders and local authority workers.

Their structures, jurisdictions and organisation depend on national legislations and regional contexts. EMFIs are intended to be highly resilient, and they can often be seen as strongholds designed to withstand all levels of external (operational) and internal (organisational) pressure. They should have reliable emergency and operational continuity plans to help them avoid failures that could potentially compromise the delivery of relief (Lindell et al., 2007; Alexander, 2016). However, this is far from being the whole truth. If there are gaps in their preparation strategy and if some threat has been underestimated, they can be disrupted and the whole emergency sector may be affected, leading to hiccups in emergency support.

At the international level, emergency facilities have been mentioned in some major global agreements that provide guidance for policies and practices, such as the Sendai framework for disaster risk reduction (SFDRR). This has been adopted by UN Member States as a follow-up to the Hyogo framework for action, and it includes seven targets and four priorities areas intended to 'prevent new and reduce existing disaster risk' (UNISDR, 2015). The SFDRR identifies key actions on emergency facilities to be taken within multiple priority areas.

The reality in which EMFIs operate has evolved as technology has developed, and this chapter provides a basic understanding of the new challenges to their operational continuity and organisational resilience. The next subsections will identify possible guidelines for management designed to ensure that lifelines can respond to complex events. First, they introduce the operational role of lifelines in the disaster cycle. Secondly, they explain some key challenges to organisational resilience. These are clarified using case studies and examples. In conclusion, the chapter defines how to adopt practical steps to increase operational continuity and organisational resilience. For feasibility, the focus is on those facilities and infrastructure involved directly in the management of events and does not include those that can be used for emergency evacuation or shelter, such as education facilities (Lindell et al., 2007; Alexander, 2016).

2 Role in the disaster cycle

Emergency facilities and infrastructure are essential in all phases of the disaster cycle, but their operational context changes and needs to be understood.

According to both scholars and practitioners, there are phases in the process of dealing with disasters (Coetzee and Van Niekerk, 2012). These are usually considered to be mitigation, preparedness, emergency response, recovery and, in some approaches, reconstruction. The cycle has considerable utility in both planning and teaching or training. However, not all scholars and practitioners accept it.

For example, Neal (1997) observed that the phases might not be fully consecutive. Kates and Pijawka (1977) also noted the overlap between parts of the cycle. Historically, there has been an emphasis on the emergency response phase, but it is not the only element to consider in crisis management.

EMFIs are not only the hub of response activities, but they are also the natural home of various forms of planning, including those that pertain to hazard and risk mitigation, and to recovery of basic assets and infrastructures. The natural hub of operations varies from one country to another, depending on which is the lead agency and how interagency relations are organised in the national system (Alexander, 2007).

For example, in the United Kingdom the lead agency is often the police force, as emergencies have traditionally been considered to be a matter of public order. In Germany and Italy, it is the fire service, as technical rescue and scene management dominate the early stages of emergency intervention. Dynamic forces such as globalisation, urbanisation and just-in-time economics have helped change the landscape in which EMFIs operate and are maintained (Helbing, 2013; Linkov et al., 2014; Alexander, 2016).

For example, tools such as the Global Positioning System (GPS) and other global navigation satellite systems have been used intensively to improve the coordination and deployment of resources, but they have also created a network of hidden interdependencies that could compromise operation capacities if they are not mitigated (Pescaroli et al., 2018). Similarly, budget cuts have created the conditions for the development of more effective procedures but have also compromised the redundancies and buffering options that are essential safeguards in this sector.

Wherever a nation's emergency response system is placed on the continuum from command and control to cooperation and collaboration, the functionality and sustainability of the system depend on how it performs under pressure. Planning and redundancy are two of the possible solutions, but both are expensive, and EMFIs easily become a target for cuts in times of austerity.

3 Challenges for operational continuity and organisational resilience

Cascading effects and compounding dynamics can challenge the organisational resilience and operational continuity of emergency facilities.

The capacity of EMFIs to maintain the continuity of operations presents multidimensional challenges in contemporary disaster management, which is distinguished by the presence of complex scenarios (UNISDR, 2017). Indeed, organisational resilience goes beyond the functionality of buildings hosting vital assets or services, including also the interrelation between technological and societal drivers (Hellstrom, 2007; Sommer and Brown, 2011). Three main dynamics have to be considered as key emerging challenges to be integrated into policies and planning strategies in the future.

(a) Direct involvement of EMFIs at the 'epicentre' of a crisis. Increased urbanisation, diffusion of vulnerability in the urban environment and climate change make it likely that buildings are in areas that are at risk from primary threats such as flooding or heatwaves (Birkmann et al., 2014). The high degree of reliability required of structural mitigation measures and safety practices, and the changing patterns of urban vulnerabilities may lead risk to be underestimated. For example, this may be the case for command centres located in floodplains or near sites that become possible terrorism targets when the security environment changes, as happened in 2017 to the London Fire Brigade, whose headquarters are located near the site of the London Bridge attacks of that year.

(b) Impact on EMFIs of cross-sectoral cascading effects. Instead of being stabilised by the mobilisation of emergency resources, the crisis escalates as time progresses, and spreads because of the innate vulnerability of society and the disruption of interconnected infrastructure nodes (Pescaroli and Alexander, 2018).

(c) Complex scenarios and compound and interacting drivers, such as the concurrence of natural hazards. This refers to the concurrence of two or more events that are extreme either from a statistical perspective or by being associated with a specific threshold (Field et al., 2012). For example, demand on EMFIs may increase because of wildfires during a heatwave or drought. Other elements of complexity can be referred to interactions between hazards, for extreme heat triggering an avalanche, or earthquake triggering a tsunami (Pescaroli and Alexander, 2018).

The next two subsections will develop points (b) and (c) further, as their implications for organisational resilience are more complex to understand.

3.1 Impacts on EMFIs of cascading effects

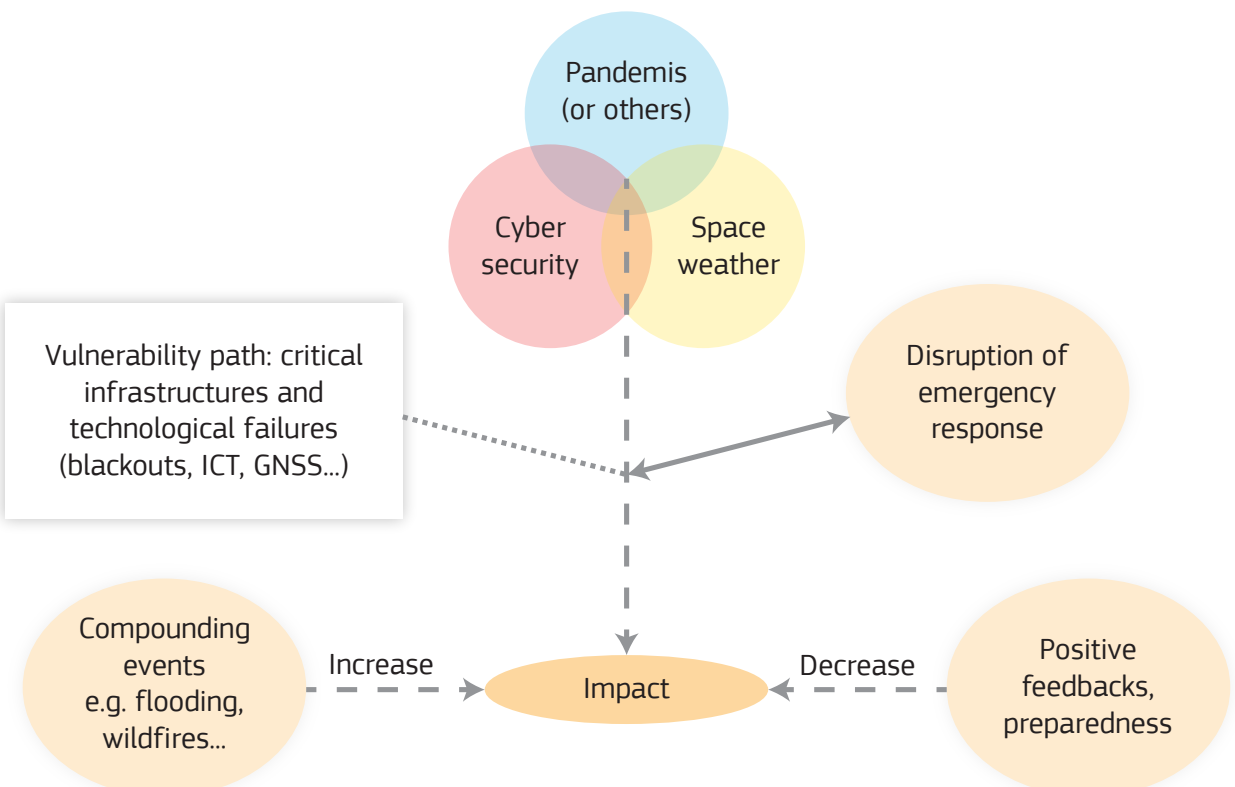
In general, when disasters and crises are triggered, increased pressure on EMFIs can be always be observed. However, their organisational resilience and operational continuity can be challenged by cascading effects that originate in other infrastructure sectors. This can arise as a result of multiple shortfalls of vital supplies, such as electricity, petrol, food, water, hygiene, drugs and personal communication systems. For example, power failures can reduce the energy available for operations, creating both communication disruptions that compromise the internet and transport disruption affecting logistics (Petermann et al., 2011; Van Eeten et al., 2011).

Preparedness for multiple failures can be underestimated or neglected owing to the complexity of the interrelationships that need to be taken into account in planning (Alexander, 2016). For example, changes in the working environment associated with flexible hours, and the evolution of the urban landscape due to inequality or gentrification, may lead to understaffing of command centres in scenarios of public transport failures. In other words, when there are extended disruptions of public transport and communication, it has to be assumed that some personnel will not be available. Therefore, emergency procedures need to be in place to ensure the presence of essential staff, and lifelines have to be reassessed. Operational continuity needs to be made sustainable and resources need to be maximised. Awareness of possible interdependencies needs to be increased by adopting new scenario-building processes that aim to understand common vulnerabilities to multiple threats (Pescaroli et al., 2018).

3.2 Complex scenarios and compound and interacting drivers

In the future, climate extremes will make it possible for cascading effects to recombine with compound drivers. This could lead to scenarios in which initial events of variable intensity, such as a local or regional flood, may coincide with a technologically driven escalation, as shown in Figure 1 (Pescaroli et al., 2018).

Figure 1. *Disruption of operations scenario associated with technological failures and compounding events.*
Source*: Adapted from Pescaroli et al., 2018.*



Primary triggers could originate in the natural domain, as when storm-force winds cause a blackout during a cold wave, or they could potentially be associated with malicious intents, as when cyberattacks aim to disrupt emergency operations. In other words, emergency management could require action to contain primary threats while at the same time being challenged in scaling up processes that are highly reliant on technological resources. Knock-out scenarios are far from implausible. In September 2017 the strongest solar flare in 12 years caused radio and GPS communications to deteriorate while, in the wake of Hurricane Harvey, Hurricane Irma was challenging emergency services on Atlantic coastlines (Crane, 2017).

While there is no evidence that the solar flare complicated the provision of relief, it affected the same hemisphere. Moreover, it has been suggested that shocks to the cyberdomain could be triggered by attacks on critical infrastructures during some other type of crisis, which could limit the capacity of technicians to activate protection measures (Sommer and Brown, 2011). An additional example can be considered by analysing the 2020 coronavirus (COVID-19) global pandemic. Just in the first half year since the emergency declarations in Europe, it become evident that the cascading effects of the primary trigger (COVID 19) could re-combine and compound with events such as heatwaves, wildfires, flooding, earthquakes, hurricanes, chemical accidents and targeted cyber-attacks (York 2020, Clark-Ginsberg et al. 2020).

4 Examples and case studies

There are different examples of how cascading effects and compounding dynamics can directly and indirectly disrupt emergency facilities, and provide complementary lessons learned.

The following subsections propose three case studies that have been chosen for their capacity to support the understanding of the points explained above. The triggering events included two cases of flooding in small to medium-sized urban areas, representing high-frequency hazards of the most common kind. Each of the case studies refers to an area of well-known risk, in which other events followed the main impact, and also involves a recent event with few precursors and active lessons to be learned. One case involves extended technological failure during hot weather. This has been chosen because of growing concerns about ageing infrastructure in Europe, and the possible concurrence with climate extremes such as the heatwaves of 2017–2019. The cases are reported in chronological order, first describing the background and then identifying the lessons learned. The principles that have been discussed apply to most of the other human-made or natural threats, such as earthquakes, forest fires, volcanic eruptions or cyberattacks. In other words, the section uses an all-hazards approach by proposing an analysis of the effects that could be common to different triggers. Practical suggestions about organisational resilience for decision-makers are given subsequently.

4.1 Power outage in Auckland, February–March 1998

With a 2018 population of approximately of 1.6 million inhabitants, Auckland is the largest city in New Zealand. It is the major economic and financial centre of the nation. It is located on North Island on a volcanic field that is potentially disruptive. During the southern hemisphere summer of 1998, the city experienced an extended power outage of 10 consecutive weeks. This directly affected the central business district, where the economic

activities were concentrated. An analysis of the event and its implications for emergency management was conducted by Stern et al. (2003). The crisis was triggered by the failure of four major cables that delivered energy to the city, but it was rooted in unaddressed vulnerabilities, such as lack of adequate maintenance of the grid. In the first instance, emergency services had to deal with demands that are common to wide-area power failures (Petermann et al., 2011; Royal Academy of Engineering, 2016) such as people trapped in elevators, activation of automatic alarms, and pressure on healthcare associated with carbon monoxide poisoning, rotten food and contaminated water. Afterwards, issues of the continuity management of EMFIs came into play. Owing to the failure of telephones and computers, communication between the organisations became harder. The concurrence of the event with summer reduced the working capacity of personnel (Stern et al., 2003). Indeed, many of the buildings suffered public heath issues and failure of ventilation systems. The temperature in offices exceeded 30 °C, which required personnel to be relocated precisely when there was the maximum strain upon their operational capacity. This was particularly true of the facilities located in high-rise buildings, such as the City Council itself.

Lessons learned

Although this case study is now quite dated, it offers various kinds of lesson to learn. First, it shows that, despite high reliability, worst-case scenarios have to be taken seriously. Second, it required workers to balance short- and long-term decision-making as the crisis dragged on and resources and international logistics had to be used sparingly. Finally, it showed that crisis managers themselves can be victims of disruption. Although the event is quite long ago and society has changed since 1998, technological failures concurrent with climate extremes have to be taken seriously and integrated in actual continuity management. For example, the 2018 power network overload in Cascais, outside Lisbon, happened during one of the most severe heatwaves of the decade. In the United Kingdom, summer 2019 was marked by rail transport disruptions in July due to extreme heat, and then a month later a blackout in southern England, where Ipswich Hospital was disrupted during an extended period of severe heat. Moreover, this case study illustrates that multiple levels of cascading effects originating in the energy sector can create cross-sectoral challenges to operational capacity and organisational resilience (Petermann et al., 2011;

Royal Academy of Engineering, 2016). Emergency tools such as generators or stored fuel may be inadequate, while high reliance on contractors could imply loss of lifelines where the crisis implies competition for the same resources, for example when demand for the services of the same contractor is higher than its capacity. The loss of pressure in water mains or heating could compromise the safety of buildings, while reduced telephone capacity during periods of increased demand may overload landlines. Finally, the disruption of technological assets such as servers and data centres could imply shifting to paper-based procedures, as well as requiring tools for individual resilience such as hand-cranked battery chargers. In both cases, underestimation of risks or cuts in budgets may limit the redundancy of resources. In areas where cashless transactions are common, scenario building should consider the impacts of cross-sectoral failures on emergency personnel independently from the triggering events. Electricity failures may make simple activities, such as grocery shopping, impossibly difficult (Royal Academy of Engineering, 2016). EMFIs are operated by personnel that rely daily on the effective functioning of the same systems as everyone else.

4.2 Flooding in Carlisle, January 2005

Carlisle is an industrial town in Cumbria, northern England. It has a population of approximately 74 000 and it is known to tourists for historic heritage such as the nearby Hadrian's Wall and the Lake District National Park.

The city has several areas at risk of flooding, which happened in 1771, 1822, 1856, 1925 and 1968. In January 2005 approximately 1 600 properties were inundated in the city and three people died. Critical infrastructure disruptions were widespread, which affected emergency relief and rescue. The UK Environment Agency (2006) noted that more than 250 000 homes and business in Cumbria and north Lancashire were affected by power failures, with restoration costs of approximately GBP 4.5 million in Carlisle alone. Moreover, as a consequence of the power outage the mobile phone network was disrupted, as was part of the landline telephone system, further burdening the emergency services. Some of the key personnel were prevented by road closures from reporting for duty. Police stations in Carlisle, Penrith and Appleby were heavily damaged, as were council offices and schools. The official report (Environment Agency, 2006) emphasised that the shutting down of the police station in Carlisle was the first closure of a major station in peacetime.

The closure of the civic centre led to the relocation of the strategic ('gold') command centre, which was directly affected by the flooding. It lost its communication room but managed to remain operational despite heavy challenges. The county Fire and Rescue Service was also disrupted, as a fire station was flooded to a depth of approximately 2.5 metres. The emergency situation required the support of fire and rescue crews from across the United Kingdom.

Lessons learned

According to the UK Environment Agency and Cumbria County Council (2016), the 2005 flooding led to the development of a new flood defence scheme and presented an opportunity to define new flood-warning areas and practices. However, in December 2015, as a consequence of Storm Desmond, the city suffered another major event, with 2 128 proprieties flooded in Carlisle and approximately 60 000 homes subject to power outages across northern England. Although the lessons learned at the emergency coordination centre were implemented, further lessons were derived from critical infrastructure failures in the 2015 flood (Environment Agency and Cumbria County Council, 2016; Royal Academy of Engineering, 2016). First, household preparedness and emergency response were inadequate to face extended blackouts, as noted in the previous example in Auckland. Second, it has been shown that, during the flood, power disruption affected the whole area and a pumping station started to rely on an emergency generator until it ran out of fuel and stopped (Environment Agency and Cumbria County Council, 2016; Royal Academy of Engineering, 2016). The exact time was not recorded, but it had an impact on emergency services, as it led to flood overtopping in some affected areas. In conclusion, it can be noted that the wired telephone system continued to hold up, but mobile phone systems did fail. The need for reliable communications was highlighted as a cross-cutting issue in considering the needs of the public (Royal Academy of Engineering, 2016). To sum up, this case study highlights the need to plan carefully the location of EMFIs, and, if they lie in areas at risk, some alternatives should be identified in the preparedness phase (UNISDR, 2015). Moreover, their resilience to multiple infrastructure failures should be assessed, giving priority to increasing redundancies and buffering (UNISDR, 2015).

The last element to consider in this case study is that complex events may require the development of improved cross-border coordination for fast deployment of emergency teams under mutual aid agreements. Since 2005, the evolution of the EU civil protection machinery has provided a concrete answer to that challenge. However, further work may be needed to prepare for the cascading effects of multiple infrastructure losses, in particular to define the logistics of fast deployment during technological failures and loss of lifelines to emergency facilities.

4.3. Flooding in Parma, October 2014

Parma is a well-known centre of high-quality food production in northern Italy. In 2018 the city had approximately 200 000 inhabitants. Over the period 10–13 October 2014 three of its neighbourhoods were partially flooded, causing EUR 26.5 million of direct economic damage but no loss of life (Protezione Civile Emilia-Romagna, 2015). The majority of the economic damage was associated with the disruption of two pieces of critical infrastructure.

(a) The flooding of the Piccole Figlie hospital (Figure 2), a nearby nursing home and a health care centre for non-self-sufficient elderly people necessitated the emergency evacuation of 96 patients. Although the principal clinic of the hospital was located less than 20 metres from the riverbank, all its functions were still operational until river water entered the building. In a few minutes, flooding reached 1.5 metres and staff had to help the patients, many of whom were elderly, climb onto tables to reach safety. Moreover, the building had an oncology centre, from which 16 patients, some with terminal cancer, had to be evacuated using rudimentary methods (Petri and Ciocci, 2014). The hospital was inoperative for 2 months, which placed a burden on other health services in the city.

(b) Flooding of a telecommunications hub led to the total interruption of both landline and mobile telephone coverage supplied by Telecom Italia in the western portion of Emilia-Romagna for days, and it directly affected the operational capacity of the emergency services (Protezione Civile Emilia-Romagna, 2015). In the affected area, situational awareness was reduced because citizens were unable to communicate with the emergency services. The offices of the city hall had communications disrupted, and the personnel were only able to deliver official communications using the Facebook profile of the mayor. Similarly, general practitioners were unable to communicate with vulnerable patients in the flooded areas. Some calls to the 118 emergency medical number had to be rerouted through the regional emergency network using diverse repeaters.

Figure 2. *Parma during the flooding: the Piccole Figlie hospital*
Source*: Wikicommons, author Comune di Parma (2014), CC BY-SA 2.0*

Lessons learned

The event shows the impact on EMFIs associated with both the direct effects of primary triggers, such as flooding, and the cascading effects of disruption in other critical infrastructure sectors, such as telecommunication. There are different lessons to be learned and gaps to be addressed in the future. First, this case study highlights how hazard and critical infrastructure maps still do not connect with each other. In Parma, the location of the telecommunications hub was known only to the provider. They need to be better integrated with the development of processes, practices and scenarios (Nones and Pescaroli, 2016). As happened in the previous case study, these elements should naturally be considered in continuity management, but this is far from always being the case. The location of emergency facilities may be well known, but their vulnerability may be not be understood because changes in the urban landscape have increased the risk. Moreover, this case study points out the need to assess critical infrastructure interdependencies, and the location of nodes and hubs, but also to integrate cross-sectoral failures and cascading effects with measures to ensure the organisational resilience of the emergency services (Pescaroli and Alexander, 2018).

Coordination issues may become primary challenges to address. At the time of the disruption, the contingency plan needed further work. If information is not shared enough, communication challenges may arise within the emergency services, and between the emergency services and the public. For example, the impacts on the continuity of data of hospitals and healthcare facilities has proven to be particularly critical, affecting both routine operations and emergency management (Klinger et al., 2014). Moreover, a growing tendency for disaster management to be over-reliant on internet services has been noted (Royal Academy of Engineering, 2016; Aldea-Borruel et al., 2019). In Parma, the key factor to contain the crisis was low-tech radio capacity, which was vital to operations when more sophisticated technological solutions failed (Perri, 2014).

Practical solutions to those challenges include the development of alternative procedures and redundancies, such as increasing the sphere of operation of radios in case of extended emergencies, and constructing scenarios of emergency needs with respect to the population of vulnerable people. Finally, warning and preparedness strategies are clearly relevant to emergency facilities, as lack of action can compromise their operational capacity and exacerbate the risks for their beneficiaries. There must be further integration and standardisation across functional sectors (Birkmann et al., 2014).

5 A discussion of guidelines for operational continuity and resilience

The resilience of emergency facilities and infrastructure can be improved by considering both primary threats and cascading effects in checklists and operational standards.

The increased complexity of society requires a shift in emergency planning and management (Helbing, 2013; Linkov et al., 2014; Pescaroli and Alexander, 2018; Pescaroli et al., 2018). Indeed, despite the relatively high reliability of critical infrastructure networks that support lifelines in emergencies, the future is one of complex scenarios of reduced operational capacity. The case studies presented above represent a starting point for further discussion. There are some main elements that can be discussed in considering an all-hazards approach, to support scenario building, exercises, risk assessment and horizon scanning.

- Emergency facilities can be affected by primary threats, and consideration needs to be given to addressing investments in retrofitting and mitigation. The literature shows that emergency facilities such as healthcare facilities are dependent on physical resilience, and non-structural and organisational components such as evacuation planning, staff rotas, time of day at which the event happens and accessibility by road (Birkmann et al., 2014). The online technical guidelines of the World Health Organization (2019) have reported some specific considerations that can be used to understand the impacts of some other recurrent hazards in Europe.

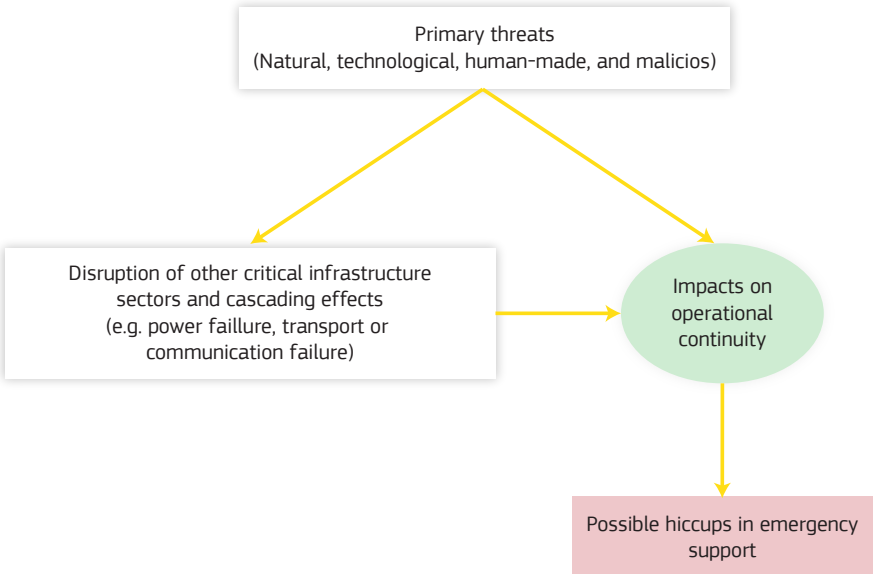
  For example, the effects of earthquakes on hospitals and healthcare facilities can be described in terms of both direct impacts, such as physical damage, and stressors associated with infrastructure failures, such as absence of workforce caused by transport disruption, or the loss of medical supply and procurement. EMFIs can represent a potential target for malicious attacks. The WannaCry ransomware attack in 2017 disrupted one third of hospital trusts, and 603 primary care and other organisations in England (Smart, 2018). The electronic flow of clinical information was compromised, causing the lack of availability of records and test results. Appointments were rescheduled, including visits for cancer patients, while ambulances were diverted and emergency departments became unable to treat patients (Smart, 2018).

- Emergency facilities are vulnerable to cascading effects, technological failures and compound dynamics. Researchers agree that emergency facilities can be widely affected by dependency on infrastructure such as energy supply or telecommunications. However, lessons have not always been adequately incorporated into effective preparedness and training. Helsloot and Beerens (2009) investigated the response to power outages in 2007 in the Netherlands that lasted approximately 3 days and coincided with particularly cold December weather. More than half of the participants in the study highlighted that local governments' response was inadequate. Other exercises highlighted that events such as power failures could hamper backup systems used by EMFIs such as satellite phones, and 'a mechanism to support widely distributed emergency communication is a fundamental need that must be addressed' (Aldea-Borruel et al., 2019, p. 25). Finally, climate extremes and technology could interact in new ways to increase pressure on EMFIs. For example, the heatwave affecting California in 2019 meant that power had to be shut down for safety, to 'prevent equipment from starting wildfires during hot, dry, and windy periods' (Jackson, 2019, p. 1). These shutdowns affected approximately 3 million people.

Figure 3 reports a synthetic overview of possible dynamics that could be exacerbated by lack of preparation. It can be noted that operational continuity can be directly affected by a primary threat, such as floodwaters, earthquakes or malicious attacks. This is the case, in particular, if emergency facilities and infrastructure lie in areas at risk or are exposed to new risks that were not assessed before, such as terrorist attacks, and find themselves at the epicentre of a crisis. However, there could be new stressors and cascading effects associated with critical infrastructure disruptions originating in other sectors during ongoing events, and they could be concurrent with the primary threat.

When the resilience of the EMFIs is not sufficient to stand the impact of a primary threat or the stressors caused by the disruptions, the capacity of emergency support may be reduced or compromised. Unfortunately, with current knowledge it is not easy to produce worst-case scenarios for the escalation of secondary emergencies such as blackouts, telecommunication failures and transport breakdowns. It is often assumed that emergency facilities are safe from primary triggers without committing to regular assessments that evaluate both technological failures and concurrent dynamics. The process could find common escalation paths and thus seek to maximise resource usage and the effectiveness of emergency responses (Pescaroli et al., 2018).

***Figure 3**. Factors affecting operational continuity of EMFIs **Source**: Authors*



5.1 Operational standards and checklist

Some frameworks are already available to improve operational continuity and resilience at the strategic and political levels. They will be described in the next subsections. The first element to consider is the development of international standards that can be used as reference for operational continuity and organisational resilience.

The International Organization for Standardization (ISO) and British Standards Institutions (BSI) standards on continuity management (ISO 22301:2019) and organisational resilience (BSI 65000:2014, ISO 22316:2017) provide the framework for defining a consistent process to identify potential threats, adapting and integrating the operational use of existing guidelines, and increasing flexibility to deal with unanticipated threats. These include support for assessing the integration of cascading effects and interdependencies (ISO 22301:2019) and resilience 'maturity levels' in an organisation or facility (BS 65000:2014, ISO 22316:2017).

Moreover, the US National Fire Protection Association (2019) highlights further the need to evaluate the possible cascading impacts of 'regional, national or international incidents', considering the potential combinations of frequency, severity and cascading impacts for different categories of threats. Continuity management could then inform some key questions for self-assessment derived from the existing guidelines on the subject (UNISDR, 2012; Pescaroli et al., 2017). Using that as a basis, the following checklist may be considered by practitioners and strategic trainers.

- How much has the planning and construction of the EMFIs taken into account current and future disaster risk in the area? Are there any critical nodes for command and control, or emergency relief logistics, that lie in high-risk areas?
- Is vulnerability assessment of the facility conducted and updated, and have mitigation measures been implemented considering the possibility of an escalating crisis? Has planning integrated forward-

looking tools and wider impact assessment methods that are suitable for defining cascading effects and multiple infrastructure failures? What training tools could need implementation?

- Has a gap analysis or resilience assessment been conducted in order to consider the ability of the EMFIs to remain operational during an extended energy, transportation or telecommunications failure? Is it updated and considered to be a realistic worst-case scenario with compounding dynamics (e.g. a power failure during cold weather)? Does the organisation have provisions for emergency power and communication?
- What are the technological lifelines that the organisation has to ensure to remain operational? Is there a 'plan B' for short-, medium- and long-term disruptions? Have backup solutions for essential information and communication technology tools been arranged and alternative procedures been developed?

5.2 Documentation in the European Union

Given the emphasis on Europe in this report, a short overview of the key documentation produced by the European Commission is warranted. Scenario building can be facilitated using the documents that explain and list the expected impacts of extreme climate change on critical infrastructure, and the concomitant implications for society (European Commission, 2013a). Although this approach has limitations, it can provide a practical overview of compounding dynamics upon which to develop scenarios and understand cross-sectoral disruptions. Similarly, in 2013 the European Commission (2013b) provided a roadmap for the implementation of the European programme on critical infrastructure protection, with the inclusion of cross-sectoral interdependencies that could be used as a basis for understanding cascading effects.

Although this documentation needs better integration between the legislative tools, for example between the European Floods Directive (EU, 2007) and the Council Directive 2008/114/EC (EU, 2008) — identification and designation of European critical infrastructures and assessment of the need to improve their protection (Nones and Pescaroli, 2016), the process is constantly evolving. With respect to cascading events, the capacity to communicate and coordinate efforts needs to be increased, while new strategies for vulnerability assessment need to be put in place. At the EU level it can be assumed that there are contextual differences between national capacities, local realities and organisations present in the same jurisdiction. These differences must be recognised and considered at the strategic level.

5.3. United Nations guidelines and checklists

A wider spectrum of actions can be derived from the documentation produced by international bodies. The SFDRR contains some specific references to emergency facilities. It recommends increasing the resilience of critical infrastructure such as hospitals, and introducing practices of safe design, standardisation, periodic maintenance and sociotechnological impact assessment (UNISDR, 2015). The SFDRR stems from the evolution of multidisciplinary and practice-oriented research that integrates climate change adaptation into planning and policy design, and promotes emergency planning oriented towards prevention (Aitsi- Selmi et al., 2016).

It can be noted that some of the observations on emergency facilities were based upon other practices, such as those developed by the World Health Organization and Public Health England (2013). These recommendations underline the need to build safe hospitals and to ensure that health facilities remain operational in emergencies. Planning, training, exercising and developing a surge capacity are essential activities. They highlight the need to plan for multisectoral disruption in order to assure the continuity of health services (World Health Organization

and Public Health England 2013). Some complementary guidelines have been developed under the Words into Action initiative, which has been promoted by UNISDR in order to support the national implementation of the SFDRR. These provide information on the underlying drivers of risk including the different types of disasters that could occur (UNISDR, 2017). An essential asset to consider is national disaster risk assessments, which provide the means by which the vulnerability of emergency facilities is understood, and standards of preparedness are created by means of investment and exercises (UNISDR, 2017).

For example, if the risk register defines a possible event as having moderate likelihood but major impact, contingency planning will have to consider realistically possible disruption over a broad scale. At the local level, local disaster risk reduction and resilience strategies have to identify the essential aspects of risk scenarios. They must update information on critical infrastructure, the potential impacts of hazards, and possible cascading effects that could reduce local capacity (UNDRR, 2019). Further consideration has to be given to the strategic dimension of interagency coordination and protocols, which in many cases can lead to the fragmentation of preparedness and organisational standards. For example, there may be gaps in the process of informing the public and deciding what information to provide in case of technological disruption, such as power failure, and how this provision of information can be extended to other urban and rural areas.

The case studies reported in this chapter illustrate the need to plan for operational continuity and organisational resilience in order to assure that lifelines can be restored as fast as possible. Further guidance can be found in practical handbooks for local government and professional practice (UNISDR, 2012; Linkov and Fox-Lent, 2016; Pescaroli et al., 2017).

Future impacts of climate change should be considered in order to establish early warning and monitoring systems, defining, ex ante, the decision thresholds that could influence crisis management agencies and coping strategies (UNISDR, 2012, UNDRR, 2019). Finally, the location of emergency facilities should be reassessed in relation to changing vulnerability and hazards. Minimum standards of resilience should ensure that supply routes and lifelines are identified in order to prioritise the maintenance of emergency facilities and the delivery of emergency relief, for both events triggered by natural hazards and those triggered by technological scenarios (UNISDR, 2012; Pescaroli et al., 2018).

6 Conclusions and key messages

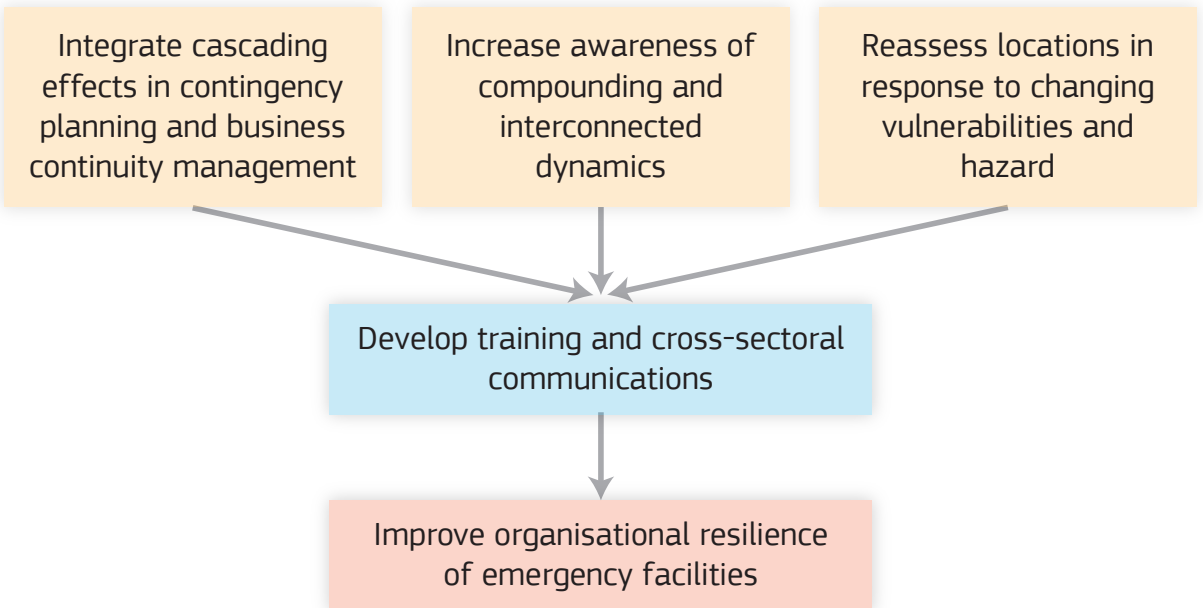
The next steps for improving the resilience and operational continuity of emergency facilities and infrastructure include efforts to improve multi-stakeholder coordination and impact assessment.

Maintaining the operational capacity of emergency facilities and infrastructure is at the centre of this subchapter. The adoption and implementation of the SFDRR and the Words into Action guidelines are essential measures designed to increase the resilience of emergency facilities while at the same time reducing future disaster risk (UNISDR, 2015, 2017;UNDRR 2019). However, the theory and the case studies provided here highlighted that many challenges for the application of these concepts still exist in practice.

First, there may be a structural issue of coordination, communication and information sharing in the management of EMFIs, and this could undermine the improvement of training and exercising for complex scenarios.

This is particularly true in the case of cross-sectoral failures, in which emergency facilities are disrupted by the cascading effects triggered in other sectors, such as electricity. The recent global crises associated with COVID-19 highlighted even further the need to see EMFIs as the nerve centre of our social functions, developing a collaborative and inclusive process to assure their operational capacity.

Figure 4. *Steps for improving organisational resilience of emergency facilities* ***Source****: Authors*



Cross-cutting challenges

Differences in the language used by academics, policymakers and practitioners could cause problems. It is realistic to believe that they could be overcome by collaboration in the medium term, so that counterparts learn to know each other's point of view, creating both trust and knowledge exchange. The existence of different timelines for policymaking, utility management and research may need the development of a focused research project and impact-oriented studies. In conclusion, it is evident that dynamics (such as budget cuts) affect both academics and practitioners by limiting the resources available.

This element can potentially disrupt emergency services and represents a situation in which positive changes, in terms of proactive collaboration, may be less limited by institutional and administrative barriers. New steps to assure the organisational resilience of emergency facilities are essential to prevent the escalation of future crises, and the collaboration of all the actors involved in emergency planning and management is necessary to mitigate complex scenarios.

Policymakers

Account must be taken of the need for further development of conventions on multi-stakeholder collaborations to support a systematic exchange of information, expertise and results. The identification of internal and external interdependencies suggested in new continuity management standards such as ISO 22301:2019 and NFPA 2019/1600 could be the first step in this process. However, new steps are needed in terms of legislation and policies to support the development of a holistic collaborative framework and introduce better accountability and compliance requirements. Some open questions remain, associated with the quantification of cascading impacts triggered by the disruptions of EMFIs. At the time of writing, it is not possible to access any quantitative information on losses and damages that could have been avoided if EMFIs had been completely efficient. These data could be used to develop some better cost–benefit analyses to support decision-makers. Clearly, this approach is merely a first step in a longer process of improvement and evolution that should involve EU legislation and policies.

Practitioners

Possible mitigation for this issue includes the adoption of standardised practices for creating organisational resilience and understand internal vulnerabilities (ISO 22316:2017, 22301:2019; NFPA 2019/1600), while increasing the adoption of measures in line with the scenarios proposed in the updated versions of national risk registers (UNDRR, 2019). Figure 4 shows the main steps needed to improve the organisational resilience of EMFIs in the near future by actively involving training and cross-sectoral communication between stakeholders. In the assessment process the functionality of vital services must involve multiple dimensions, such as operations, structure, planning and resources. These have different potentials to become useful tools in practice. They have been extensively evaluated, for example in the Intergovernmental Risk Governance Council's Resource Guide on Resilience (Linkov and Fox-Lent, 2016). Furthermore, scenario building should integrate cascading effects and interconnected dynamics in order to understand the carrying capacity of EMFIs during technological failures and complex events (NFPA 2019/1600). The integration of these aspects in practice requires the development of further collaborations with academia.

Scientists

Many aspects of this assessment process represent a fine opportunity for an active role of scientists in supporting practitioners and decision makers. For example, new collaborations can be developed in order to understand gaps in preparedness for cascading events, as well as to analyse structural and non-structural vulnerabilities to multiple threats. Moreover, scientists could actively support the development of new scenarios and strategic foresight to be used in training activities, as has already been done in the field (e.g. Alexander, 2016; Pescaroli et al., 2017).

Citizens

The role of individual citizens is another element that can be explored to improve the status quo. For example, the literature recommends defining what to communicate and how to do it (Alexander, 2016; Lindell et al., 2007), but there is a lack of understanding of what procedures would be most useful if emergency facilities were disrupted. In line with the SFDRR (UNISDR, 2015), it could be useful to develop better involvement with local communities and stakeholders. Indeed, civil society could represent an essential asset for coordinating emergency efforts, and developing basic training for the population on cascading scenarios could be one of the tools for improving societal resilience (Royal Academy of Engineering, 2016).

3.4.2 Network infrastructures

Lead Authors:

Luca Galbusera — *European Commission, Joint Research Centre*

Marianthi Theocharidou — *European Commission, Joint Research Centre*

Contributing Authors:

Oriol Monserrat — *Centre Tecnològic de Telecomunicacions de Catalunya, Spain*

Petr Novotny — *Technical University of Ostrava, Czechia*

Giovanni Sansavini — *ETH Zürich, Switzerland*

Bozidar Stojadinovic — *ETH Zürich, Switzerland*

Galbusera, L., Theocharidou, M., Monserrat, O., Novotny, P., Sansavini, G., Stojadinovic, B., 'Network infrastructures', 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.

1 Introduction

Many of today's critical infrastructures (CIs) are commonly described as 'networked' because of their spatial imprint or the many interacting components and functions they are made of. Mutual linkages also come into play, sometimes subtly, when different processes and technologies interact, overlap, compete over resources or intertwine to compose services. Expressions such as 'networks of networks' and 'global supply chains' are highly meaningful in relation to a modern definition of networked CIs, and the scientific community is investigating the subject of interdependencies through several methodologies, chiefly relying on network science and related disciplines (Rinaldi, Peerenboom, and Kelly 2001; Barabási 2002; Barthélemy 2011; Ouyang 2014).

In the EU policy framework, networked critical infrastructures (NCIs) and their interconnections take on a major role in both the 2004 Communication from the Commission to the Council and the European Parliament – Critical Infrastructure Protection in the fight against terrorism (European Commission, 2004) and Council Directive 2008/114/EC on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection (Council, 2008)([1]). The energy and transport sectors, central to the latter policy instrument, are particularly relevant to the present section.

Key enablers for modern economies, NCIs require special consideration from the standpoint of risk and disaster management. Indeed, failures can be rooted in both exogenous (e.g. natural or human-made hazards) and endogenous (e.g. ageing) factors.

Moreover, interconnections can give rise to various failure propagation patterns, often hardly predictable; see for instance the categories of cascading, escalating and common cause failures from Rinaldi et al. (2001). As a result, assessing NCI risks solely as the sum of the risks associated with the individual parts may be grossly misleading and, conversely, the broader picture of risks ought to be investigated. Moving from the standard definition of risk as 'effect of uncertainty in objectives' (ISO, 2018, p. 1), Helbing (2013) discusses the concepts of systemic risk ('the risk of having not just statistically independent failures, but interdependent') and hyper-risk ('implied by networks of networks').

The same author also points out some key failings of current risk-assessment methods. These include poor estimates of probability distributions and parameters for rare events, underestimation of likelihoods of coincidence of multiple rare events, shortage of accounting for feedback loops in fault/event tree analysis, insufficient consideration of joint probabilistic analysis and complex dynamics analysis, human/social factors, lack of questioning about established ways of thinking on economic/political/personal incentives.

The spectrum of consequences can be vast, and recent studies emphasise how, for instance, a local disruption to infrastructure can result in considerable macroeconomic impacts, e.g. see Hallegatte et al. (2019). Awareness of similar aspects and the non-conventional nature of risks in NCIs is rising among researchers, practitioners, policymakers and stakeholders at large.

This can be observed, for instance, in the Sendai framework for action on disaster risk reduction 2015–2030 (UNDRR, 2015). Therein, in particular, Global Target D ('substantially reduce disaster damage to critical infrastructure and disruption of basic services, among them health and educational facilities, including through developing their resilience by 2030') sets objectives in terms of both 'damage to critical infrastructures attributed to disasters' and 'number of disruptions to basic services attributed to disasters'.

(1) See Theocharidou et al. (2018) for a more extensive discussion of the EU policy framework on CIs.

Interdependencies and direct/indirect effects are also central to standard ISO 31000 (ISO, 2018); see for instance the comprehensive interpretation given of the term 'consequences'.

These examples and many more found in several policy documents manifest the need for a refined approach to disaster risk management, especially as far as NCIs are concerned. Broadening the landscape even further, what has been mentioned so far is only one facet of the topic from a disaster risk management perspective.

These systems are also vital and integral to the deployment of response actions during crises, providing relief to the population, channelling recovery resources and ultimately softening the consequences of adverse events. Accordingly, they should be better interpreted today as socio-technical systems, wherein different technological layers are interoperating at the boundaries between those environmental, social and organisational contexts that shape their design, operations and development (Masys, 2014). From this perspective, Vespignani (2009) observes how 'the major roadblock in defining the fundamental predictability limits for techno-social systems is their sensitivity and dependence on social adaptive behaviour'.

Social consensus is needed to ensure resilience of those assets and services that NCIs provide to society. Our discussion, therefore, has implications for the engagement of civil society, volunteers, community-based organisations, public institutions, academia, scientific and research entities, business, professional associations, the private sector and the media.

2 Case studies

In European power grids and transport systems, significant cascading consequences have been observed in the past.
The structure of networks can greatly influence direct and indirect impacts, relief and recovery from disasters.

Lessons on disaster risk management related to NCIs can be drawn from memorable failures from the recent past. As mentioned above, next we focus on some case studies from the energy and transport sectors, which are mentioned in Council Directive 2008/114/EC.

2.1. European power outages

The European Transmission System (ETS) is an evolving, highly meshed network, which entails five synchronous large area networks. According to the European Network of Transmission System Operators for Electricity (ENTSO-E, 2019a), it includes about 489 381 km of high-voltage lines and is operated by 43 transmission system operators (TSOs) from 36 countries, serving 534 million citizens with an annual electricity consumption of about 3 329 TWh (in 2017) and a peak load of 542 GW (cold wave on 18 January 2017). To ensure security of supply and reliable operation, the ETS needs protection against cascade tripping, voltage/frequency collapse and loss of synchronism. ENTSO-E (2019b) observes that 'Europe enjoys one of the world's most reliable power grid'. Kröger (2017) observes the following trends and challenges for the ETS:

- unbundled market structure replacing monopolies, with the responsibility for power supply security shifting from single industries to national authorities;
- operation modes pushed closer to limits, even beyond initial design parameters;
- fast-rising share of intermittent asynchronous renewable energy sources, which are highly dispersed,

usually abundant in sparsely populated areas and often available during low-demand periods; this requires massive power transfers over long distances, as well as peak-smoothing strategies;

- increasing volumes of cross-border power exchange and of short-term trading;
- increasing smartness and user involvement due to information and communication technology pervasiveness, self-sustaining areas and transfer of control functions from central units to decentralised private users while at the same time the coexistence of novel and legacy technologies must be managed;
- broadening spectrum of threats and hazards related to cyber- and physical attacks and extreme weather, with both frequency and severity increasing, ageing of systems and components, lack of adequate investment and decreasing redundancy/reserves.

The most serious challenges that the ETS faces are blackouts, which are increasingly rare but can have devastating consequences for people and the economy. In 2006 an incident on the north German transmission grid led to its being cut off from the interconnected power system of continental Europe, with 15 million households across 20 countries experiencing power supply disruption (UCTE, 2007).

Another example that shows how electricity supply, and the lack of it, can affect society is the Italian electric power blackout on 28 September 2003 (Sunday morning to Monday night) (UCTE, 2004; Kröger and Zio, 2011). At 03.01, one of the main north–south transit lines through Switzerland – the Lukmanier transmission line – shut down because of a tree flashover.

This resulted in the redistribution of the electricity, and another north–south transit line, namely the San Bernardino transmission line, was overloaded. The Swiss and Italian transmission operators communicated in order to relieve the overloads in Switzerland and return the system to a secure state.

Thus, Italy reduced its imports; however, this reduction was insufficient to relieve the overloads. At 03.25, the San Bernardino line tripped after another tree flashover. With two important lines down, cascading failures occurred on the remaining lines. This resulted in the Italian system becoming isolated from the European network, and several generation plants in Italy failed. A total blackout followed at 03.27 throughout Italy, with the exception of Sardinia and some load islands.

In Italy, the restoration process started immediately after the blackout. After 3 hours, energy had been restored in some regions connected to France (such as Liguria). Nine hours later, in the afternoon of 28 September, electricity was restored gradually in most places, including Turin, Milan, Venice and Rome. Rolling blackouts continued to affect about 5 % of the population over the next 2 days (29–30 September). In Italy alone, the estimated total energy not supplied amounted to 177 GWh, and it took 18 hours to complete the restoration.

According to the analysis proposed in (Kröger and Zio, 2011, p. 14), the impact on the population was strong (‘about 56 million people have been affected, five elderly persons died’; ‘hundreds of people have been trapped in elevators’), economic losses moderate (including those related to spoiled foodstuff and the interruption to continuously working industries) and the impact on dependent critical infrastructures varying.

Among the critical infrastructure sectors affected were transportation (trains and subways stopped, flights delayed or cancelled, outages of traffic lights), water supply (`in some southern regions interruptions of water supply for up to 12 h’) and ICT (`telephone and mobile networks in a critical state but operable; Internet providers shut down their servers’). Less severe was, for instance, the impact on hospitals (`due to the use of emergency power generators’).

2.2 Transport-related failures

According to the 2018 OECD Survey on Critical Infrastructure Resilience and Security, transport is very consistently designated as a CI sector by the countries surveyed (OECD, 2019). It branches into many segments; for instance, the list of European CI sectors in Council Directive 2008/114/EC includes road, rail, air and inland waterway transport, as well as ocean and short-sea shipping and ports.

A conspicuous effort has been put into determining the key stressors for each transportation category and providing quantitative indicators. For instance, Koks et al. (2019) estimate that approximately 27 % of the global road and railway assets are exposed to at least one natural hazard, while about 7.5 % of all assets are exposed to a 100-year flood event.

Common categories of transport disturbance causes include natural events, accidents, social events and malicious attacks (Khademi et al., 2015). The sensitivity of different means of transport to different kinds of events can be quite variable. Notably, the scientific community has inquired into their risk and resilience qualities as a function of specific network features (Barthélemy, 2011; Rodrigue et al., 2016). The latter reference, for instance, characterises a given transport network in terms of topology (expressing its 'arrangement and connectivity') and typology (which 'relates to its geographical setting as well as its modal and structural characteristics').

According to various studies, road infrastructures often exemplify the concept of hierarchical mesh, spanning multiple geographical scales ([2]). Setting apart large-scale events, a peculiar vulnerability is related to the failure of strategic connectors such as some bridges or tunnels. In this sense, a major event occurred in Europe on 24 March 1999, when the fire that spread from a truck severely affected the Mont Blanc tunnel (France–Italy) and led to the deaths of 39 people. Despite the triggering of security mechanisms, a critical issue was the lack of oxygen due to toxic smokes, while high temperatures were reached and cooling took days. Three years of closure followed, leading to economic losses estimated in excess of EUR 300 million. After damage assessment and evaluation of restoration and modernisation options, the French–Italian commission of investigation issued a list of recommendations including improved tunnel configuration, vehicle regulations and training aspects (Duffé et al., 1999). Further events followed soon, such as the 1999 fire in the Tauern tunnel (Austria) and the 2001 fire in the Gotthard road tunnel (Switzerland). Fires have also affected the Channel Tunnel (France–UK) more than once since its construction (Lewis et al., 2013), as well as the Alpine pass of Fréjus (France–Italy) in 2005. Bridge disasters in Europe in recent decades include the Entre-os-Rios (Portugal) tragedy in 2001, when the collapse of the Hintze Ribeiro bridge caused 59 deaths, and the 2018 collapse of the Morandi bridge in Genoa, which resulted in 43 victims.

Observing the historical evolution of air transport routing, Rodrigue et al. (2016) observe how 'geographically, a key outcome of airline deregulation has been the emergence of hub-and-spoke networks centered on a major airport where a single carrier is often dominant' ([3]). Air transport networks can be highly vulnerable to disruptions at such hubs.

A seminal paper by Guimerà et al. (2005) describes the worldwide air transport network as a scale-free small-world network with centrality anomalies due to the community structure resulting from both geographical constraints and geopolitical aspects. Among its implications, for instance, the authors observe how 'cities that connect

([2]) See also Rodrigue et al. (2016) for a discussion of the case of rail networks and their specific network layout.
([3]) According to ICAO (2004), a hub and spoke system is 'an operational system in which flights from numerous points (the spokes) arrive at and then depart from a common point (the hub) within a short time frame, so that traffic arriving from any given point can connect to flights departing to numerous other points'.

different communities play a disproportionate role in important dynamic processes such as the propagation of infections such as severe acute respiratory syndrome'. See also Colizza et al. (2006) for correlations between the properties of the air transport network and epidemic spread.

According to Eurocontrol ([4]), flight delays cost the European economy close to EUR 18 billion in 2018 (Sullivan, 2019). A recent report by the International Air Transport Association estimates that 'the terrorist attacks in Western Europe in late-2015 and early-2016 reduced European airlines' international passenger traffic by around 1.6 % in the following year, compared to what would otherwise have happened. [...] This reduced European airlines' 2016 revenues by around US$2.5 billion' (Oxley, 2017). The same report also highlights that, 'as was the case during the SARS [severe acute respiratory syndrome] pandemic in 2003 and the Icelandic ash cloud in 2010, the impact on European international passenger traffic has been only temporary. This underlines the resilience of air passenger demand to short-lived shock events'.

By contrast, events such as the terrorist attacks of 11 September 2001 and the global financial crisis had a more lasting impact. Another example of disruption to airport services can result from problems with fuel supplies, such as in a recent (April 2019) case related to the Portuguese air transport system, when strikes by drivers of hazardous materials had consequences on fuel provisioning.

The vulnerability of maritime networks and sea lanes involves different considerations depending on whether the node is a hub or a gateway (Rodrigue et al., 2016). Disruptions at a hub will mostly affect maritime shipping networks, whereas disruptions at a gateway will mostly affect the hinterland. See the latter reference for case studies, including cases of global maritime routes and chokepoints. When considering transport disruptions, tolls in terms of human lives are often accompanied by significant outbound and inbound cascading effects on and from other sectors. As an example, studies mentioned by Rozenberg et al. (2019) estimate that the total yearly costs due to extreme events on the transport system in the European Union are in the order of EUR 2.5 billion, predominantly road costs, with predicted rises for the years to come. Reliance on other sectors is critical, with energy and information and communication technology often topping the list of sources of delays and disruptions. Modes of transport, when disrupted, can severely affect each other, owing to the transfer of demand and the fact that they are often interconnected. Modern cities aim for transport intermodality, making these dependencies increasingly important. An event with major consequences from this viewpoint was the ash cloud resulting from the Eyjafjallajökull eruption of April–May 2010 (see Super Case Study 3 on the Eyjafjallajökull eruption), which resulted in the 'closure of Europe's airports and airspace which lasted for a period of over seven days with cancellation of up to 100,000 flights affecting 10 million passenger journeys. [...] The airline industry faced high costs of up to $400 million per day' (OECD 2019, p. 33). 'Stranded passengers looked for other transport modes, notably trains, the cross-channel Eurostar and ferries which were neither equipped nor flexible for such an increase in demand' (OECD 2019, p. 33).

Finally, transport nodes are key for managing disasters, as they are essential for the deployment of equipment and humanitarian goods in order to help and provide relief to victims. An efficient response helps to reduce the social, economic and environmental impacts. As an example, some recovery actions implemented during the 2016 earthquakes in Amatrice (Italy) were related to restoring access to the village, which required over-river access, after the collapse of bridges. A joint group formed by the National Civil Protection and the Italian army built two temporary bridges within 10 days of the 24 August 2016 main shock (Durante et al., 2018).

([4]) Note that Eurocontrol (jointly with Galileo, the electricity transmission grid and the gas transmission network) is one of the CIs selected to pilot the approach to CI protection and resilience proposed in (European Commission, 2013).

3 Gaps and challenges

Past events affecting network infrastructures pushed forward our awareness and response to critical events, for instance through updated legislation, technologies and crisis management solutions. Many challenges remain, due for instance to complexity and hyperconnectivity, evolving market conditions, climate change and infrastructure ageing.

A recent study in German cities (Monstadt and Schmidt, 2019) observes that the governance of critical infrastructures 'overarches different, often fragmented, policy domains and territories and institutionally unbundled utility (sub-)domains'. The authors also observe that risk mitigation and preparedness are based on catastrophic scenarios as opposed to past events, and involve considerable uncertainty. While national policies or regulations may be needed, this is often not translated to local vulnerabilities, needs and gaps. The discussion proposed so far in this section can help to shed light into some of the gaps and challenges to addressed, as far as NCIs are concerned.

In power networks, the analysis of recent major blackouts and disturbances led to the identification of some underlying causes, factors and considerations for future developments (Kundur and Taylor, 2007; Kröger and Zio, 2011), as illustrated below.

- Technical failures, external impacts and adverse behaviour of protective devices are important triggering events, when not protected by the N-1 security criterion ([5]) and/or manifesting in combination with high-load conditions. These triggering events can lead to cascading outages of lines or other equipment and, eventually, to the collapse of the entire system.

- Organisational aspects and factors, such as market liberalisation and short-term contracting, can cause the system to operate beyond its original design parameters. Stressing operating conditions such as weakening maintenance work and/or inadequate integration of intermittent power generation have proven to be outstanding causes of critical situations.

- The TSOs play a decisive role in contingency management; lack of situational awareness and short-term preparedness, as well as limited real-time monitoring beyond control areas and poorly timed cross-border coordination, can accumulate as aggravating factors.

- The inadequacy of the N-1 security criterion and, even more importantly, of its evaluation/implementation in various cases has prompted attempts to make it more stringent and legally binding.

- Power systems are increasingly being pushed harder, with higher levels of power transfers over longer distances. Transmission protection operations in the absence of any faults have played a major role in cascaded outages. This is because, as the equipment is more stressed, the boundary between functioning and faulty equipment becomes blurred, making it more difficult for the protection to discriminate.

([5]) The N-1 criterion is 'the rule according to which the elements remaining in operation within a TSO's control area after occurrence of a contingency are capable of accommodating the new operational situation without violating operational security limits' (European Commission, 2017).

Recent critical situations, not necessarily leading to continent-wide blackouts, have highlighted additional areas for improvement in the ETS. In particular, the cold spell of January 2017 (ENTSO-E, 2017) underlined the need for (1) close cooperation among energy sector operators, i.e. electric power and gas TSOs, (2) increased fidelity in the models used for system security and adequacy assessment, and (3) the conduction of stress tests at the pan-European level, also accounting for climatic trends. This becomes even more important as today's electricity systems integrate, requiring efficient interaction between the different stakeholders and levels of responsibility (ENTSO-E, 2019c).

Moreover, Europe's energy sector is shifting from a supply-centric model dominated by fossil fuel to a consumer-centric system with many distributed resources (ENTSO-E, 2019c). Such systems can operate in islanded mode. They can offer options to cope with critical conditions or emergencies in the rest of the power network and to increase the resilience of the overall system, by providing redundancy in energy paths and quick recovery options. In addition, flexibility in terms of long-term and short-term energy storage systems is a key element for enhancing the resilience of the grid and the ability to withstand unforeseen occurrences. Flexibility, however, adds operational complexity to the grid, which has to be appropriately assessed and managed.

In the case of transportation networks too, recent events have led to the identification of gaps to be filled at various levels, including the technological and policy layers. Lessons learned from the aftermath of tunnel disasters, for instance, have highlighted shortcomings in regulation and led to Directive 2004/54/EC (EU, 2004) on minimum safety requirements for road tunnels in the trans-European road network. This expresses a fundamental effort in formulating compliance requirements for tunnel infrastructure safety, and its implementation has been closely monitored throughout the years since it came into force; see for example Krausmann and Mushtaq (2010); Durante et al. (2018); ICF (2015). As a complement, the research community is also addressing tunnel safety and providing suggestions, for instance in the areas of uncertainty treatment and behavioural analysis (e.g. during evacuation); see Ntzeremes and Kirytopoulos (2019).

Transnational transport networks and corridors are increasingly central in emerging disaster risk management strategies. Notably, Directive 2008/96/EC (EU, 2008), complementing the abovementioned Directive 2004/54/EC, laid down key principles for road infrastructure safety management at the level of trans-European road transport systems. Procedures put in place include road impact safety assessments, road safety audits, road safety inspections and network safety management. The implementation of the directive led to a series of successive implementation appraisals (Schrefler and Dinu, 2018). Similar initiatives are in place to cover, more broadly, the Trans-European Transport Networks, a set of strategic land, air and water transport networks currently in the works and representing a key constituent of the EU Trans-European Networks.

A posteriori analyses of events involving aviation have produced a rich set of recommendations. Alexander (2013), discussing the case of the 2010 Icelandic ash cloud, points out criticalities such as some arbitrariness in air restriction decision-making, risk aversion, gaps in procedures and planning, and a lack of modal integration in the European transport system.

The Single European Sky (SES) initiative by the European Commission is an example of the evolving approach to the management of air transportation networks and infrastructures. In particular, the Single European Sky ATM

Research (SESAR) initiative represents the technological pillar of SES, and aims to deliver ATM innovation. The rich SESAR solutions catalogue (SESAR, 2019) includes, for instance, the notion of trajectory-based operations, 'to enable the ATM system to know and, where appropriate, modify the flight's planned and actual trajectory, before or during flight, based on accurate information that has been shared by all stakeholders.

Prospective advantages include efficiency gains both for individual aircrafts and for the network as a whole. Further solutions described therein at the network level include collaborative decision-making and performance management, demand- and capacity-balancing mechanisms, and free routing in high-complexity environments.

In general, assessing the cascade impact of disruptions such as those described above (e.g. major air transport disruptions) remains a challenge due to the complexity of these NCIs. Many approaches exist. Examples include: the cascading impact assessment methodology from (Rehak et al. 2018); the framework for modelling the robustness of the critical infrastructure network proposed in (Pinnaka, Yarlagadda, and Cetinkaya 2015); the integrated framework for hazard estimation, network estimation and infrastructure failure assessment presented in (Pant et al. 2018); the multi-agent system framework for conceptualising, modelling and analysing interdependent critical infrastructure from (Pereyra, He, and Mostafavi 2016); the approach for the analysis of geographic hotspots of critical infrastructure illustrated in (Thacker et al. 2017); various other interdependency models focusing on critical infrastructure networks, such as the ones in (Duan et al. 2016; Lin et al. 2016; Johansen and Tien 2018). While similar models can assist a policymaker in assessing the complex relationships between infrastructures and potential cascade effects, often there is a lack of the resources or expertise needed to apply such models in real-life situations or to scale their application to nationwide assessments.

Network infrastructures face changes in demand and usage due to urbanisation and population growth. The concentration of the population implies a concentration of some risks. Thus, the impacts of any disaster affecting an urban area will be compounded proportionally to the population and infrastructure density. For example, road networks may be used at the maximum of their capacity due to changes in traffic or the development of the city. Another challenge is looking for cost-efficient alternatives.

At the same time, operators of infrastructures have to deal with the ageing of their networks. Maintaining, retrofitting or updating components of infrastructures is a significant annual cost for most operators and poses challenges, as in many cases it may reduce service uptime. In many cases, there may be a lack of alternatives in terms of service provision, or another infrastructure or sector may be affected. In some types of networked infrastructures, such as water distribution systems, ageing may pose problems both to business continuity and to the health of consumers (Allen et al. 2018).

Climate change can affect NCIs, such as energy, transport or water infrastructures. Temperature changes, sea level rise, changing patterns of precipitation and storms may affect demand, reduce efficiency, cause inundation of coastal infrastructure or damage assets, such as bridges, ports and airports (OECD, 2018). Moreover, interdependencies between sectors should be taken into account when planning for climate-resilient and sustainable infrastructures. For instance, Beheshtian et al. (2019) analyse the interdependency between transport and motor fuel supply chains, and investigate how vulnerability to climatic extremes in a fuelling infrastructure hampers the resilience of a transport system.

4 Conclusions and key messsages

In this section, we have addressed NCIs from the disaster risk management perspective. Taking stock of case studies related to the power and transport sectors, we have made observations on the gaps and challenges that systems of this kind pose to our community. Enabling a fuller operationalisation of the scientific contributions still requires substantial effort, which this report contributes to. Next, we provide some conclusions and recommendations.

4.1 Risk and resilience policies

Recent policies stress the importance of resilience for better disaster risk management. For instance, many recommendations issued in recent years are about infrastructural climate resilience, which has the potential to improve the reliability of service provision, increase asset life and protect asset returns. 'Building climate resilience can involve a package of management measures (such as changing maintenance schedules and including adaptive management to account for uncertainty in the future) and structural measures (e.g. raising the height of bridges to account for sea-level rise or using natural infrastructure such as protecting or enhancing natural drainage systems)' (OECD, 2018, p. 2).

Predominantly, the CI resilience issue is faced by resorting to a comprehensive, all-hazards approach. In recent EU policies related to CIs, resilience has gained more and more importance and is connected to a number of strategic directions (Theocharidou, Galbusera, and Giannopoulos 2018). The Sendai framework considers four priority areas related to disaster risk management: (1) understanding disaster risk; (2) strengthening disaster risk governance to manage disaster risk; (3) investing in disaster risk reduction for resilience; (4) enhancing disaster preparedness for effective response and to 'build back better' in recovery, rehabilitation and reconstruction. As mentioned above in this section, the dual aspect of damages to facilities and services, as well as the links to the economic dimension, are also considered.

A key challenge for regulators and governments is to encourage investments by private companies in risk reduction and resilience, especially within the current economic and environmental context. Operators have varying technical, financial, political, reputational and legal priorities and constraints, which the policymakers need to bear continually in mind. To this end, stakeholder engagement and information sharing can be enhanced through participation in public–private partnerships and other networks (Theocharidou, Galbusera, and Giannopoulos 2018). As the OECD (2019) discusses, 'it is important for governments to find the right balance between mandatory and voluntary frameworks to enhance stakeholder engagement in the process and ensure that investments in resilience are effectively made'.

The recent OECD survey mentioned therein identified an articulated set of policy tools for this purpose; see Table 1. The same reference also contains a proposal for a structured approach to CI resilience policies, including the transboundary aspects.

Table 1. *Policy tools to foster critical infrastructure resilience.* ***Source****: © OECD, 2019.*

1. Provision of hazards and threats information	12. Inspections and performance assessments
2. Voluntary information-sharing mechanisms or platforms	13. Fines for non-compliance with resilience requirements
3. Mandatory information-sharing mechanisms or platforms	14. Other types of penalties for non-compliance
4. Awareness-raising activities and training	15. Ranking based on inspection / performance results
5. Resilience guidelines for critical infrastructure operators	16. Reporting on operators' resilience
6. Fostering the development/use of professional standards	17. Sharing best practices
7. Incentive mechanism to assess risks and vulnerabilities	18. Public investments in infrastructure resilience
8. Incentive mechanisms for investing in resilience	19. Guidance for subnational levels of government
9. Sectoral prescriptive regulations dedicated to Critical Infrastructure Protection	20. Mandatory insurance for critical infrastructure
10. Performance-based regulations on business continuity	21. Peer reviews, monitoring and evaluation
11. Mandatory business continuity plans	22. Sectoral mutual aid agreements

4.2. Modelling and simulation

Throughout this section, we have made reference to the role of scientific disciplines such as network science in NCI applications; see also Galbusera and Giannopoulos (2019) for further discussion. The study of NCIs still requires important modelling efforts, ranging from topological aspects to dynamical processes and multi-layer networks. From the disaster risk management perspective, interesting insights can come, for instance, from network perturbation studies. Key aspects covered by the literature include the compromise between error tolerance and attack tolerance (Albert et al., 2000; Crucitti et al. 2004) and the representation of failure propagation processes (Newman et al. 2005). Eusgeld et al. (2009) provides further insights on the role of both network theory and object-oriented modelling in vulnerability analysis of CIs. As far as the research on cascading disasters is concerned, Alexander (2018) observes that 'some of the work covers the propagation of failures through networks, but this is largely restricted to individual categories of critical infrastructure'.

Aspects to cover in the development of modelling and simulation tools include reliability and dependability assessment, optimisation, large-scale simulation and the treatment of uncertainty. Examples of tools or approaches for NCI applications include Bayes networks (Schaberreiter et al., 2013), Boolean networks (Galbusera et al., 2018), probabilistic models for cascading failures (Newman et al., 2005), agent-based approaches (Panzieri et al., 2005; Kröger, 2008), hierarchical holographic modelling (Haimes et al., 2002), input–output modelling (Galbusera and Giannopoulos, 2018), risk analysis-based models (Ezell et al., 2000), Monte Carlo simulation (Pant et al. 2016), Petri nets (Ghasemieh et al., 2013) and Unified Modeling Language-based approaches (Bagheri and Ghorbani, 2010). In the literature, surveys are also available to provide a broader picture of the emerging modelling approaches; see for instance (Bagheri and Ghorbani, 2008; Satumtira and Dueñas-Osorio, 2010; Ouyang, 2014) ([6]).

From the community perspective, the development of models should also be accompanied by initiatives to facilitate their exchange, validation and use even beyond the boundaries of particular specialisms. Knowledge management initiatives such as the creation of inventories of models, methods and tools may serve this purpose.

([8]) Further examples of resources that could be used for cascade effect analysis can be found at Poljanšek et al. (2019, pp. 115–118).

Work is also needed to facilitate the interoperability of models and to relate them to disaster risk management practices. The necessity for extended paradigms for the analysis and modelling of CIs is addressed in more detail by Zio (2016).

Finally, the development of modelling and simulation approaches with relevance to NCIs is coupled with the ongoing scientific discussion on conceptual aspects such as the definition of the technical, organisational, social and economic dimensions of resilience; see Theocharidou et al. (2018) and related references for further analysis. See also Alderson and Doyle (2010) for a discussion on complexity in network-centric infrastructures, as well as Florin and Linkov (2016); Trump et al. (2018) for resources on resilience aspects.

4.3 New technologies

Emerging technologies have the potential to radically transform aspects of CI management, such as monitoring. For instance, the increased availability of data from satellite Earth observation is becoming important for damage prevention and restoration monitoring. Recent literature shows how such data, with different temporal and spatial resolution characteristics, can be used as a tool to evaluate the state of health of various CIs (Milillo et al., 2016; Chang et al., 2017; Huang et al., 2018), as well as to sample the surrounding environment, detect potential hazards and help to prevent potential damages (Peduto et al., 2017; Dai et al., 2018; Solari et al., 2018). However, there are still challenging issues to be addressed in order to provide fully operative tools for this purpose.

In parallel to satellite Earth observation, the development of short-range non-destructive techniques has grown significantly over the last 10 years. The appearance of drones has introduced great innovation in CI monitoring (Colomina and Molina, 2014), allowing damage inspection even in a number of difficult-access areas. In addition, the technological development of terrestrial sensors, such as radars and laser-based sensors, has provided a set of instruments to check both structural health and potential damage without interfering with the CI in question (Teza et al., 2009; Pieraccini, 2013; Luzi et al., 2014; Monserrat et al., 2014; Ham and Lee, 2018; Zhang et al., 2018). The use of these techniques, too, is still limited by various aspects such as costs or lack of awareness, or regulatory restrictions (e.g. in the case of drones).

Clearly, many other aspects of information technology are relevant to NCI disaster risk management. An example is the development of data-gathering and analysis platforms (Galbusera and Giannopoulos, 2017). Application-specific studies have highlighted the relevance of such kinds of data-backed initiatives. A recent study on bridge failures in the United States, for instance, points out the relevance of data collection on historical bridge failures to improving bridge specifications (Lee et al., 2013).

In recent times, the development of some apps and other information-sharing tools represents an excellent example of the use of technologies to foster citizen awareness and engagement. For instance, two-way alerting mechanisms may prove beneficial in reducing reaction time to critical events affecting network infrastructures, and may mitigate impacts on end-users.

4.4. Exercises and stress tests

Finally, an identified gap remains the need to perform joint exercises to better comprehend dependencies between CIs, thus generating more accurate risk assessments, and to jointly test risk treatment options. Such exercises may need to be designed with a different mentality with respect to the case of civil protection exercises, which

focus mainly on the operational capabilities of emergency responders. Crisis scenarios that involve both public authorities and infrastructure operators are not widely analysed, but they can be a valuable tool to test risk and resilience strategies and plans, as well as to enhance collaboration (Poljanšek et al., 2019). An interesting example of an exercise initiative relevant to NCIs is the Homeland Security Exercise and Evaluation Program (HSEEP) by the US Federal Emergency Management Agency (FEMA, 2020). The HSEEP provides guiding principles for exercise projects and programmes, including aspects related to their design, development, conduct, evaluation and improvement planning.

A related concept is that of stress tests (Galbusera et al., 2014; Galbusera and Giannopoulos, 2019). A stress test is a systematic method of crisis scenario analysis and of evaluating measures taken to reduce the societal risk exposure stemming from networked CIs. It involves the owners, the users and other stakeholders of CIs. Following the use of stress tests in the banking sector after the 2007–2008 financial crisis and in the nuclear power sector after the 2011 Fukushima disaster, the European Programme for Critical Infrastructure Protection (EPCIP) (European Commission, 2013) recognised that there is a need for stress tests of critical non-nuclear civil infrastructure systems, to verify their risk exposure levels as well as to help increase the disaster resilience of European CIs.

To this end, a harmonised risk-based natural hazard stress test methodology for CIs was recently developed in FP7 project STREST ('Harmonized approach to stress tests for critical infrastructures against natural hazards') (Esposito et al., 2020). The STREST stress test is designed to cover a wide range of critical non-nuclear CIs. It can be conducted at different levels, characterised by different scopes and complexities of risk analysis, to suit the widely different capabilities and resources of different European CIs. The STREST stress test comprises the following phases. First, the goals, scope and risk analysis methods are defined, and the stress test team members are selected and organised. The stress test is then performed at both component (subsystem) and system levels, accounting for network dependencies and cascading effects, using a probabilistic risk analysis approach. A mechanism for an independent review of the stress test findings is built in. Furthermore, risk assessments are harmonised using a penalty system to compensate for the differences between different risk analysis methods, and levels of CI and hazard knowledge. The harmonised risk assessment results are compared with societally accepted risk levels using a STREST grading system. Finally, the STREST CI grade and risk assessment findings are transparently reported to the owners, stakeholders and the public to build public trust.

The STREST grading systems are conceptualised to enable a comparison of different CIs in terms of their own disaster risk exposure and the risk exposure they present to society. This is an essential step towards harmonised systemic risk evaluation of CIs across Europe. The grading systems contain a mechanism for continuous reduction of CI risk and improvement of CI disaster resilience enacted through mandatory repeated stress tests at risk-driven intervals. For example, if the CI system poses a risk that is greater than societally accepted risk exposure levels, the CI owners and stakeholders are obligated to take risk reduction actions by a specific deadline and to verify the achieved risk reduction in a subsequent stress test. The implementation of the STREST stress test was also illustrated using six different CI systems, characterised by different functions and dependencies, network structures, geographical extents and natural hazard exposures (Argyroudis et al., 2019).

In conclusion, it is important to observe that a comprehensive treatment of disaster risk management for NCIs extends well beyond the electricity and transport realms, which have been scrutinised in this section. The mosaic of contributions on this subject is made of many pieces, including insightful studies on finance (Gai and Kapadia, 2010; Glasserman and Young, 2015), gas (Cimellaro et al., 2015) and telecommunications (Sterbenz et al., 2013).

O'Rourke (2007) suggests that 'thinking about critical infrastructure through the subset of lifelines helps clarify features that are common to essential support systems and provides insights into the engineering challenges to improving the performance of large networks'. A scientific attitude to NCI analysis and assessment able to compare sectors and learn from disciplines can, therefore, be crucial to building resilient communities.

Policymakers

Policymakers should focus on stakeholder engagement and information sharing, including public–private partnerships with operators and citizen involvement initiatives. Existing constraints affecting the private sector should be taken into account, striking the right balance between mandatory and voluntary frameworks to ensure effectiveness in investments in risk reduction and resilience.

Practitioners

Practitioners face varying technical, financial, political, reputational, legal priorities and constraints. For better disaster preparedness and response by network infrastructure operators, the use of new technologies such as monitoring tools or information-sharing platforms can be valuable. Initiatives such as training and exercises or stress tests represent an opportunity to identify gaps and coordinate for better resilience.

Scientists

Scientists have a key role in the development of innovative modelling and simulation tools for network infrastructures. These can assist policymakers, operators and responders to better understand failure propagation through networks, identify mitigation actions and optimise response plans. Scientific effort should be devoted to tool interoperability, large-scale simulation, the treatment of uncertainty, reliability and dependability assessment, as well as resilience aspects.

Citizens

Citizens rely heavily on the use of network infrastructures. They can benefit greatly from new technologies, for instance as a way to get alerts about service disruptions and also to report promptly on the failures they observe.

3.4.3 Core industrial and energy facilities

Lead Author:

Elisabeth Krausmann *European Commission, Joint Research Centre*

Contributing Authors:

Athanasios Fourtounas *Joint Logistics Support Group NATO, Greece*

Serkan Girgin *University of Twente, Netherlands*

Miguel Angel Hernandez Ceballos *European Commission, Joint Research Centre*

Daniel Jung *European Commission, Joint Research Centre*

Ernesto Salzano *University of Bologna, Italy*

Zdenko Šimić *European Commission, Joint Research Centre*

Krausmann, E., Fourtounas, A., Girgin, S., Hernandez Ceballos, M.A., Jung, D., Salzano, E., Šimić, Z., 2020, 'Core industrial and energy facilities', 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.

1 Introduction

Industrial installations and energy facilities are susceptible to a variety of hazards, which can be natural, technological or intentional in nature. Some of these facilities pose a secondary hazard if they store, handle or transport hazardous materials. In case of spills, fires or explosions after natural-hazard impact, the associated risk is referred to as natural-hazard-triggered technological accident (Natech) risk (Krausmann et al., 2017a). Failure or disruption of these facilities can cause impacts on society, the environment or the local, national or global economy. Impacts can also occur as a result of business or service disruptions, such as power outages or a loss of production (Küfeoğlu, 2015). They can be exacerbated by cascading effects and (inter)dependencies between systems. In some cases, cascading effects across sectors can reach global proportions, resulting in a shortage of raw materials and finished products (Lohr, 2011).

There are many examples of incidents involving core industrial and energy facilities. In 2005, leaking fuel caused a major explosion and fire at an oil storage and transfer depot in Buncefield, United Kingdom, which engulfed 23 storage tanks (MIIB, 2008). The incident also revealed the complexity of supply chains conditioned by the just-in-time supply approach (Airmic, 2011). In the same year, Hurricanes Katrina and Rita destroyed or damaged 276 offshore platforms, 24 rigs and 457 underwater pipelines, and resulted in global price hikes for oil and gas (Pan, 2005; Cruz and Krausmann, 2008). A technical problem caused an explosion and fire at an Austrian natural-gas distribution and reception hub in 2017, causing Italy to declare a state of emergency due to a lack of gas supplies (Oltermann, 2017).

This section provides an overview of the risks to and impacts from selected industrial and energy facilities that are critical for the European Union (EU), such as chemical facilities, the pharmaceutical industry, refineries, oil and gas pipelines, and offshore facilities. It exemplifies the diversity of incident triggers, risk receptors and impacts by using three iconic case studies. It then discusses the gaps and challenges associated with reducing the risks and their impacts. The section ends with a summary of recommendations for the different stakeholder groups. Some of the discussions are equally valid for types of critical industry and infrastructure other than the ones mentioned above

2 Case studies

Numerous past events are testimony to the potential for major consequences of incidents at core industrial and energy facilities.

In the following, three detailed case studies demonstrate the different types of incident triggers, impacted infrastructure and consequences. The incidents not only affected the countries they originated in, but also had international impacts and influenced risk-management regulations and practices across countries and continents.

2.1 Spolana chemical accident, Czechia, 2002

In August 2002, heavy and long-lasting rainfall in central Europe led to major flooding of the River Elbe with unprecedented flood heights. On 15 August 2002, the flood hit the Spolana general chemicals facility in Czechia. The facility was protected against a 100-year flood; however, the flood waters exceeded the 100-year water level at the site by 1.3 m (eNATECH, 2018).

The anti-flooding measures implemented at the plant were inadequate for the magnitude of the flood, and the storehouses holding chlorine, a highly toxic and corrosive substance, were inundated. Several of the pressurised chlorine tanks were lifted by buoyancy and in the process the safety valves of a full chlorine tank were torn off, resulting in a massive leakage of over 80 tonnes of chlorine (Figure 1). On 23 August, a smaller chlorine release occurred (Hudec and Lucš, 2004; eNATECH, 2018).

Although nobody was killed during the accident, it had a significant impact on the environment and agricultural activities in the surroundings of the chemical facility. The chlorine entered the Elbe and the air, where the chlorine gas chemically burned the flora around the facility. Community life was disrupted, as the public had to shelter in place to escape the chlorine cloud. The operator was criticised for not properly warning the population after the chlorine release (Reliefweb, 2002). In addition, significant quantities of other hazardous substances (e.g. dioxins) were released into the Elbe and settled in sediments on its shores. In a village downstream from the damaged chemical facility, dioxin levels were found to be three times higher than safety norms (Gautam and van der Hoek, 2003). The company indicated that the direct costs to property due to flood damage amounted to approximately EUR 29 million (eNATECH, 2018).

Figure 1. *Chlorine release at the flooded Spolana plant.* ***Source****: © Václav Vašků.*

After the accident, on-site protection measures were updated to prevent the recurrence of such an event in case of a flood of the same or higher severity. Among the actions taken, chlorine storage was reduced to 50 % of the capacity before the accident, thereby significantly reducing the risk. The storehouse emergency exhaust system was improved to allow suction of the chlorine from the upper part of the storehouse, which is important if the retention basins are flooded.

From a policy perspective, discussions were launched to better understand how flood impacts of this magnitude could be prevented in the future. As a regulatory follow-up after this and other accidents triggered by natural hazards, the EU Seveso Directive on the control of major accident hazards involving dangerous substances was, inter alia, amended to render the need for protection against this type of risk more explicit (EU, 2012). The directive, which applies to over 10 000 industrial establishments in the EU (Gyenes and Heraty Wood, 2018), now explicitly requires the consideration of natural hazards as a threat to the safe operation of hazardous installations, including the demonstration that the risk is identified and mitigated.

2.2 Deepwater Horizon accident and oil spill, United States, 2010

The Deepwater Horizon oil spill was one of the largest marine oil spills in history. It was caused by an explosion on BP's Deepwater Horizon oil rig located in the Gulf of Mexico in April 2010. A natural gas surge blasted through a concrete core installed to seal the well for later use. The gas travelled up to the platform and ignited a series of explosions and a firestorm causing 11 fatalities and 17 injuries (Figure 2). The rig capsized and sank in 2 days, resulting in an oil spill lasting about 5 months and releasing around 4.9 million barrels of oil (Pallardy, 2018). A massive response with more than 100 000 people, 6 500 vessels and 4 000 km of boom ensued to protect the environment (BP, 2015). Extensive damage was caused to marine and wildlife habitats, and also to the drilling, fishing and tourism industries.

Figure 2. *Left, supply vessels combating the Deepwater Horizon fire; right, skimming oil in the Gulf of Mexico after the oil spill from Deepwater Horizon.* ***Sources****: left, photo courtesy US Coast Guard; right, photo courtesy National Oceanic and Atmospheric Administration (NOAA).*

An offshore drilling moratorium left an estimated 8 000–12 000 people temporarily unemployed (Snow, 2010). About one third of US federal waters in the Gulf was closed to fishing at the peak of a fishing ban (NOAA, 2010). Following the accident, BP's stock value fell by more than 50 %, resulting in a total loss in value of USD 105

billion (Tharp, 2010), and its petrol stations in the United States reported a drop in sales of 10–40 % due to backlash (Weber, 2010). In 2016, a historic USD 18.7 billion District Court settlement was approved, resolving all litigation with the government and the affected states over the economic and environmental claims. Overall, BP spent more than USD 65 billion in relation to the spill (Vaughan, 2018). Multiple companies and individuals were charged with federal crimes, but no charges resulted in prison time (Gill, 2016).

There were many investigations into the accident, addressing technical, organisational and human aspects (DNV GL, 2015). The government report stated that the accident was due to poor risk management, last-minute changes to plans, failure to observe and respond to critical indicators, inadequate well-control response and insufficient emergency response training (BSEE, 2011). A national commission concluded that the accident was avoidable and resulted from clear mistakes by the companies and also by government officials who failed to create and apply proper regulatory oversight (Graham et al., 2011).

The accident was a global wake-up call and caused major changes in the design and operation of offshore equipment, accident prevention measures, planning and management of spill response activities, safety culture and regulations. In the United States, the regulatory body was restructured, new requirements were issued for offshore operations, new standards for drilling and well control were published, the accident-reporting system was improved and research on offshore activities was promoted (DNV GL, 2015).

The European Commission launched an assessment of the offshore activities in EU waters to identify actions needed to maintain safety (European Commission, 2011). Subsequently, a new EU directive was published on the safety of offshore oil and gas operations to prevent accidents and respond promptly and efficiently if they occur (EU, 2013). The directive contains provisions on risk assessment and emergency response planning before exploration or production, to ensure that companies have the necessary technical expertise and are well financed before granting licences; independent verification of technical safety solutions; environmental protection measures; emergency preparedness by the national authorities; full liability of the companies for environmental damage caused in EU waters; and public information on safety and public stakeholder involvement on planning of installations (Moore et al., 2013).

2.3 Florakis naval base explosion and power blackout, Cyprus, 2011

In July 2011, an explosion of ammunition and military explosives at the Evangelos Florakis Naval Base in Cyprus caused the fifth-largest non-nuclear explosion in history, with a yield of about 2–3.2 kilotons TNT equivalent. The explosion led to cascading events causing damage not only to the naval base but also to its surroundings, including the Vasilikos power station (VPS), the largest power facility in Cyprus, and urban areas.

The blast destroyed the firefighting system of the VPS but the 60 000 t of diesel and 84 000 t of fuel oil stored there did not ignite, avoiding a domino effect. At the time of the explosion, 98 containers of highly explosive ammunition seized by the US Navy in 2009 had been stored in the open for over 2 years. Bad decision-making at the naval base, including lack of political willingness, ineffective logistics management and the lack of a viable firefighting plan (Florin et al., 2016), and the high temperatures and humidity of Cyprus caused the accident.

Since military and energy facilities were concentrated in a cluster, the power station was severely damaged in the explosion (Figure 3). It killed 13 people and injured a further 62 but also severely damaged all the buildings in Zygi village, displacing about 150 civilians (Evripidou, 2011; Hajipapas and Hope, 2011). The electricity supply to about half of Cyprus was interrupted, and for 15 days rolling blackouts affected cities, airports, hospitals, tourist areas and industrial facilities, causing outages and economic damage by disrupting business and society.

The Electricity Authority of Cyprus was forced to import generators from Greece and Israel while the damage, estimated at EUR 2 billion (almost 10 % of the country's economy), was repaired, with a recovery cost of EUR 900 million for the VPS alone (Hajipapas and Hope, 2011). Eight years after the accident, Cyprus reimbursed over EUR 4.5 million to citizens, and lawsuits by private companies claiming a total of EUR 8.5 million are still ongoing.

Figure 3. *Vasilikos power station after the Florakis Naval Base explosion, Cyprus.* ***Source****: photo courtesy IDE Technologies Ltd.*

The accident investigation report found that Cyprus had not applied the Seveso II Directive (EU, 1997), an omission that exacerbated the accident (Polyviou, 2011). Following the accident, the government took action to improve risk management. In 2013, the ZENON basic national plan on the management of risks from human-made or natural origin in critical infrastructure was issued (Cyprus, Ministry of Defence, 2013).

Exercises were organised to test the plan's effectiveness, train the personnel and inform the public. In the same year, the VPS issued a new handbook on the proactive identification of human-made and natural hazards, according to Seveso II criteria (Electricity Authority of Cyprus, 2018).

The handbook is reassessed periodically considering feedback from all stakeholders. In 2016, oil and gas companies located near the power plant were obliged to engage in continuous communication with each other to coordinate planning for security issues, as well as response to disasters (Cyprus, Ministry of the Interior, 2016). In 2017, the ZENON Coordination Center was inaugurated. It is the main executor and coordinator of the ZENON plan in case

of man-made or natural disasters, declares alert states and is in contact with the relevant EU agencies. Since it may take time for help to arrive by air or sea, the aim of this centre is to respond promptly during the initiation of an event to avoid an escalation to catastrophic proportions, as well as to increase the risk awareness of society.

3 Reducing impacts – gaps and challenges

The factors that create risk to industry and energy facilities can be natural, technical or organisational in nature. Some underlying causes are linked to risk-governance challenges and socioeconomic context. Other factors, such as climate change, the ageing of infrastructure or the greening of production facilities, may introduce additional risks. The subsections below provide examples of risk drivers that directly or indirectly influence the impacts resulting from an incident.

3.1 Risk governance

Risk governance should be approached from a territorial perspective to capture the potential interactions of industry, infrastructure and communities.

Governance' refers to the actions, processes, traditions and institutions by which authority is exercised and decisions are taken and implemented. Risk governance applies the principles of good governance to the identification, assessment, management and communication of risks (IRGC, 2020). Gill and Ritchie (2018) emphasise that the occurrence of technological incidents highlights conceptual and theoretical gaps in disaster science, which has been focusing on sudden-onset natural hazards since the 1970s.

In addition, the risk management of a critical facility is often viewed in isolation from its surroundings rather than considering the potential interactions with other industry, lifelines and nearby communities. In the EU, land use planning around high-risk chemical facilities aims to protect the surroundings of the plant (EU, 2012); however, this is not always the case in other parts of the world or for other critical sectors. This means that the potential for cascading events and the impact on infrastructure resilience are not captured. Since natural hazards often affect large areas at the same time, this is even more relevant to Natech risks. Suarez-Paba et al. (2020) contend that a systemic view is required for the effective management of Natech risks, requiring a territorial approach to risk governance and incorporating physical (e.g. industrial facilities, lifelines, building stock), organisational and socioeconomic factors into the analysis. Decommissioned or mothballed facilities constitute a particular risk-governance problem.

Efforts to improve risk governance exist in all domains where modern government tries to reduce costs and ensure benefits. Some aspects of risk governance from different industry or infrastructure domains could be applicable universally (i.e. improved legislation, enforcement, inspections and experience feedback practice). However, systematic research into the applicability and effectiveness of different governance types for a variety of problems and under different conditions is lacking (NASEM, 2018). International organisations, such as the European Commission or the Organisation for Economic Co-operation and Development (OECD) facilitate risk-governance experience exchange in different domains (e.g. Tomic et al., 2008; NEA, 2018; OECD, 2003, 2014, 2015).

3.2 Data availability, collection and analysis

The availability of accurate, reliable and complete data affects the quality of risk analysis and all risk-reduction decisions based on it.

DData are the basis for gaining knowledge on the dynamics of incidents, through incident analysis and learning lessons. Data required for risk assessment must be accurate, reliable and complete, and must consider, e.g. in the case of Natech risk assessment, all natural hazards that an industrial plant can be subject to in a certain area, the likelihood of these hazards, their possible impact, the equipment's vulnerability to each natural hazard identified and the consequences of impact (Girgin et al., 2017; Krausmann et al., 2019). However, industry and infrastructure data or information on incidents is often not collected in a systematic way or voluntarily disclosed, owing to confidentiality issues. The availability of relevant and reliable data conditions the quality of risk assessment and all risk-reduction decisions that are based on it. Several studies have pointed out (e.g. De Almeida et al., 2015; Sengupta et al., 2016) the scarce availability of industrial data and associated databases, which can hamper the definition of a strategy for risk reduction. A recent study by Heraty Wood and Fabbri (2019) concludes that databases for chemical incidents are incomplete and fragmented. They add that an official international database for analysing global chemical accident trends does not exist and that only relatively few countries and industry organisations around the world maintain dedicated chemical accident databases.

Data mining and standards, i.e. harmonisation of data according to standardised procedures, are relevant to improve the feasibility and rapidity of analysis (OECD, 2012). The proper compilation and aggregation of data in well-structured databases allows experts to systematically assess risks to industry and energy infrastructure, and supports lesson-learning studies for better preparedness and loss prevention (Chakraborty et al., 2018).

3.3 Risk assessment

Methodologies, tools and guidance for Natech risk assessment are scarce.

Risk analysis identifies threats at industrial and energy facilities both during normal operation and in incident situations. It evaluates the risk based on the likelihood of occurrence of an event and its consequences. The analysis can be qualitative, semi-quantitative or quantitative. Quantitative risk analysis uses sophisticated models to simulate and analyse a high number of scenarios and requires significant time and expertise (Cox, 1998; Uijt de Haag and Ale, 1999; CCPS, 2000).

All approaches are subject to data and model uncertainties, whose magnitude needs to be quantified before risk-analysis results should be used for decision-making. Once the risk has been analysed, it needs to be compared with prescribed numerical acceptability criteria to determine if risk-reduction measures have to be implemented. In the EU, these criteria are not uniform among Member States, which hampers comparability between countries. The criteria can range from fully quantitative (occurrence probabilities) to deterministic (maximum permissible levels of overpressure, toxic concentration, etc.). Countries can also have different thresholds.

Certain identified risk scenarios are commonly removed from the assessment process when their likelihood is considered below a limit probability defined according to acceptability criteria. While this approach helps to save time and resources by screening out seemingly less important scenarios, this can only work if assumptions are sound and subject to low uncertainty. This approach also creates immediate problems for high-impact, low-probability risks, as they could be lost from the risk-management process (Nafday, 2009).

Natech risk analysis has been hampered by its multi-hazard risk nature and a lack of damage models and Natech scenarios, resulting in a lack of Natech risk-analysis methodologies and tools. Guidance on Natech risk assessment at industry and community levels is also scarce. Therefore, this risk source is not adequately taken into account in the industrial risk-assessment process, and preparedness levels are low, even in countries generally well prepared for natural hazards (Krausmann et al., 2019). Steps have been taken to address Natech risk analysis in a qualitative and (semi-)quantitative way at facility level or in national risk assessment (Cruz and Okada, 2008; Cozzani and Salzano, 2017; Krausmann, 2017; Krausmann et al., 2017b; Girgin et al., 2019). However, no assessment tool exists that captures all external hazard factors (Girgin et al., 2017).

3.4 Cascading effects

The risk of cascading effects is high for core industrial and energy facilities.

Today's industry and energy infrastructures are highly interconnected and mutually dependent in many respects: physically, spatially, logically and through the information infrastructure (Rinaldi et al., 2001; Petit et al., 2015). A dependency exists if one infrastructure relies (depends) on the service provided by another infrastructure in order to carry out its function (Bloomfeld et al., 2009; see also Section 3.4.2 of the present report). These dependencies (unidirectional) and interdependencies (bidirectional) can give rise to a percolation of failures, as a failure in one system can produce a failure in another. The spreading of failures can take place in a cascading (non-linear) manner, which can exacerbate the impact of the initial disruption. On the other hand, interdependencies do not per se give rise to risks, but can in some cases also be a source of redundancy and fault tolerance (Bloomfeld et al., 2009), which underlines the need to understand them clearly.

Energy production facilities are rich in interfaces between different infrastructures (e.g. energy, transport, communication). Industrial production processes usually require the transportation of raw materials and fuel, and the distribution of a product to consumers or to secondary industry, and thus depend on various infrastructures. Nearly all facilities depend on supervisory control and data acquisition systems required to control or monitor the system (cyberdependency). Furthermore, logical dependencies on the financial sector and governance exist. Disruptions to one of these essential services might not only result in economic losses, but also endanger the security of supply, with possible impacts on society if products are of vital importance to public security, societal well-being or economic prosperity. If at the end of the chain stands a service or (physical) supply of critical importance, dependencies along the chain could also be identified as critical.

In addition, industrial plants are often concentrated in clusters (as are transport networks), and an accident in one facility can cascade to multiple units in the same facility or to neighbouring plants, thereby increasing the severity and likelihood of negative impacts, which are called domino effects. This risk is significantly increased in cases of natural-hazard impacts on industry (Cozzani et al., 2013; Necci et al., 2015). Unfortunately, this domino risk is not systematically captured in industry because of the complexity of the analysis and the large number of data needed (Reniers and Cozzani, 2013). Novel modelling techniques have been proposed to address this problem (e.g. Khakzad, 2015; Kamil et al., 2019).

The risk of propagation of failures among different interacting infrastructures, e.g. between electrical transmission and natural gas systems (EU, 2008), has reached the attention of policymakers in recent years, partly because of the increased significance of gas-fired power plants as backup generators in the transition towards renewable energy sources. Many regions of the EU rely heavily on foreign natural-gas imports. The need to identify 'critical gas-fired power plants' has also been noted by policymakers at the European level (EU, 2017, Art. 11). In order to contain the risk, the relevant (inter)dependencies between infrastructures must be well understood.

It is usually impossible to fully analyse or understand the behaviour of a given infrastructure in isolation from its environment or connected infrastructures. The methodology to analyse interdependencies between infrastructures should match the needs of each specific problem and be based on a solid theoretical foundation, as are for example the well-developed theories of complex adaptive systems and of dependable systems (Avižienis et al., 2000; Laprie, 2008). A systematic approach is needed to describe the mechanisms, exposing a clear chain of causality, and to quantify the impact of dependencies and interdependencies between different systems and sectors.

3.5 Emergency management

Interfaces and procedures for multi-agency cooperation and communication are key for successful emergency management.

Emergency planning is at the interface between incident prevention and consequence mitigation, and ensures adequate preparedness in case of an event. The EU's Seveso Directive requires the preparation of internal and external emergency plans and the establishment of procedures to ensure that these plans are tested and revised as necessary (EU, 2012). The internal emergency plan is under the responsibility of the operator and aims to protect potential targets within a facility. Public authorities are in charge of the external emergency plan, which mitigates the risk to off-site targets. Similarly, other pieces of legislation for offshore operations or natural-gas supply include provisions to prepare for emergency situations (EU, 2013, 2017). It is vital that the various actors involved in emergency management cooperate effectively. The risk of transboundary impacts should also be taken into account for facilities close to borders (UNECE, 2015).

Although legislation and regulations are necessary to ensure the safe operation of industrial and energy facilities, they may not be sufficient to prevent or adequately prepare for incidents. Gyenes and Heraty Wood (2018) found a number of patterns related to failures in emergency management:

- lack of clear emergency response procedures with well-defined roles and responsibilities, and deficiencies in the emergency plan,
- lack of accident scenarios in the emergency plan due to their low frequency of occurrence,
- inadequate training of emergency managers and lack of emergency exercises,
- inadequate evacuation plans,
- inadequate public warning systems,
- inadequate communication and coordination between on- and off-site response services,
- unavailability of emergency power supply for safety-critical parts of a facility.

Additional problems arise because emergency planning usually does not acknowledge dependencies between critical infrastructures, possibly leading to deficiencies in crisis response and indirect impacts on the population. Moreover, multiple critical installations can fail at the same time because of common-mode failure or cascading effects (which are common occurrences during disasters of natural origin).

However, preparedness measures taken by operators, as well as by emergency responders, usually take into account only single failures (Boin and McConnell, 2007; Luijf and Klaver, 2009). For example, owing to its multi-hazard nature, Natech risk needs special treatment because of the complications generated by the natural-hazard trigger. The possibility of multiple and simultaneous accidents over large areas, the increased likelihood of cascading events and the accompanying challenges in managing the emergency might overwhelm on- and off-site response capacities alike.

4 Conclusions and key messages

Collaboration between the different stakeholder groups is essential for effectively reducing risks.

Industrialisation, urbanisation and climate change are increasing the risks from natural and man-made hazards. Damage or disruption of industry and energy facilities may severely affect society either by the consequences of technological accidents or through effects on the supply chain. Management of these risks is essential for reducing losses but also for sustainable industrial growth. This requires a concerted effort by policymakers, scientists and practitioners with the involvement of citizens.

In the following, recommendations for addressing existing gaps for each stakeholder group are proposed ([1]). The need for open and effective communication to share relevant information applies to all stakeholders.
The adequate handling of potential data sensitivities must also be ensured.

Policymakers

- Base policy development on experience and science with transparent justification and independent verification.
- Approach risk governance from a territorial perspective that views the safety and security of critical facilities in conjunction with their surroundings.
- Encourage corporate and government leadership at all levels, and promote new governance models fostering the sharing of responsibility for a risk.
- Exploit risk governance insights from different sectors, and especially from high-hazard activities, as they are universally applicable. International organisations such as the European Commission, OECD, the United Nations Economic Commission for Europe (UNECE) or IAEA could help support arrangements to identify and disseminate risk-governance experience across different regulatory domains.
- Mandate that all risks to industry and energy facilities be analysed, including cascading risks, starting from a national level, and provide a framework for emergency management to clarify responsibilities. Potential transboundary risks should also be taken into account in this context.
- Ensure (with the help of practitioners) that the results of research projects, e.g. new or improved risk-analysis methodologies, are disseminated and applied.
- Encourage knowledge transfer and experience sharing between (inter)dependent sectors to guarantee a more efficient use of resources.
- Promote public–private partnerships to provide solutions linking science, practice and policy-making. For the sake of societal resilience, these partnerships should not be driven by market forces.
- Incentivise private bodies to invest in risk-management structures that help to prevent, prepare for and respond to infrastructure failures and their societal repercussions.

([1]) Please note that policymakers include governmental authorities and that practitioners include operators, emergency responders and insurance.

Practitioners

- Collect data and make them accessible (including to scientists) to enable risk analysis and to prepare for emergencies. New technologies, e.g. artificial intelligence, can support the data collection.
- Explain the results of risk analyses, with their underlying assumptions, completeness and level of uncertainty, to facilitate communication with policymakers and citizens.
- Verify the validity of design criteria, construction standards, and prevention or mitigation measures considering industry-specific conditions (e.g. ageing) and hazard-specific conditions (e.g. climate change affecting natural hazards' frequencies and intensities).
- Promote the use of good practices in risk management, including cross-fertilisation between sectors.
- Develop business continuity plans to facilitate recovery after infrastructure failure. For example, facilities could stockpile spare parts to ensure that service recovery is fast after an incident.
- For Natech accidents, assume in on-site emergency plans that off-site response resources and lifelines might be unavailable.
- Assess physical emergency-response capacity, including protective equipment, and the capacity needed in case of cascading events, when competition for scarce resources will manifest.
- Review and test emergency plans periodically to ensure they are up to date. Also outline actions to take if assumptions are exceeded (e.g. if a natural hazard exceeds design criteria). For industry in natural-hazard areas, assume that the natural event will render the response more complex (e.g. no possibility of shelter in place or evacuation).
- Train emergency responders and security personnel on how to handle releases of hazardous materials when providing assistance to citizens affected by a natural hazard.
- Make medical services aware of the risks at industry and energy facilities to ensure that they have sufficient and suitable resources for treating the victims of hazardous materials releases.
- Emergency planning and response should exploit new technologies, such as new communication systems, 3D photography, robots and drones.
- Evaluate investments to ensure they are risk sensitive and do not aggravate existing risks.
- Use financial incentives (e.g. lower insurance premiums) to increase resilience by rewarding risk-averse behaviour.

Scientists

Make existing data, models and tools for the analysis of impact risks available to practitioners, including guidance on their use and limitations, and recommend best practices for risk analysis.

- Carry out benchmarking exercises for methodologies for risk analysis of critical infrastructures, to understand their reliability and applicability.
- Identify and quantitatively assess (inter)dependencies and propose actions and measures that could be taken to eliminate or mitigate them.
- Develop methodologies for better estimation of environmental damage and economic losses. These methodologies should also consider cascading impacts.
- Engage in studies that measure the relative costs of prevention and preparedness versus response and recovery.
- Carry out systematic research into the applicability and effectiveness of regulatory approaches across different sectors and conditions.

Citizens

- Proactively request information about risks from industry and energy facilities in the neighbourhood, unless already provided by authorities, making use of citizens' rights under the Aarhus Convention (UNECE, 1998). New media and information technologies should be employed to draw citizens' attention to risks.
- Participate in emergency drills to train the correct behaviour during hazardous material releases.
- Request the inclusion of disaster risk management in school curricula, stressing the importance of both natural and technological risks, their possible interaction and the factors that drive risk.

3.4.4 Communication systems

Lead Author:

Kalpana Chaudhari — *Institute for Sustainable Development and Research, India / Shah and Anchor Kutchhi Engineering College, India*

Contributing Authors:

David Lund — *Public Safety Communication Europe Forum, Belgium*

Paruthummootil Jacob Philip — *Institute for Sustainable Development and Research, India*

Pasquale De Toro — *University of Naples Federico II, Italy*

Maria Cerreta — *University of Naples Federico II, Italy*

Jose Luis Marin — *Applications in Advance Computing, Grupo AIA, Spain*

Milenko Halat — *Applications in Advance Computing, Grupo AIA, Spain*

Chaudhari, K., Lund, D., Paruthummootil, J.P., De Toro, P., Cerreta, M., Marin, J.L., Halat, M., 'Communication systems', 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.

1 Introduction

Humans and other life forms have communicated for millions of years, interacting to coexist, co-create and develop our societies to where we are today. Only the last 140 years have seen the mainstream use of electronic communication, marked by the award of the telephone patent to Alexander Graham Bell in 1876.

However, within the last 20 years we have witnessed an information revolution. Communication capabilities have moved rapidly, from 'text messages' and voice only, to highly rich media allowing simultaneous communication of live video, audio and large amounts of information, which are vital for speeding up and improving economic activities. The coming 5–10 years will see use of immersive, augmented and mixed reality, whereby communicated information will become even more pervasive within our physical world augmented by new artificial intelligence capabilities.

Legislation gives varying degrees of support to classifying communication systems as critical infrastructures. The information that is carried by these systems should define the level of criticality. For example, a tweet may not be considered as critical information as a medical record. However, our distinct social and business reliance on the internet and mobile communication systems must consider the most critical information flows as the common baseline to determine that a communication system must be classified as a critical infrastructure.

In this section we discuss:

- the role of communication systems and their varying degrees of responsibility regarding the transfer of information of varying critical natures;
- information and communication systems as critical infrastructures;
- rapid advances in technology – fast-changing communication infrastructure and services;
- the dependency of EU society on information and communication systems;
- cybercrime as an emerging challenge – new modalities of disaster;
- the cascading impact of compromised communication systems on other critical infrastructures;
- social impact and isolation when communication systems are not available;
- case studies;
- proposed solutions and key messages.

As we become more and more dependent on our communication systems, we will become more vulnerable and helpless when those services that we depend on are no longer available. When disaster hits, and communication services fail, then we, as citizens, will become blinder than ever.

We must prepare to enable our public safety responders with communication capabilities in the face of disaster. They must be able to collaborate whenever and wherever disaster hits within and outside Europe. Mission-critical communication should not be bounded by geopolitical borders as it is today. New communication capabilities to enable operational mobility for public safety responders are crucial to achieve this. This reflection should encourage commercial mobile communication operators to improve reliability and response action in the face of disaster, hence providing more resilient services for all, and not just for public safety responders.

2 Information and communication systems as a critical infrastructure

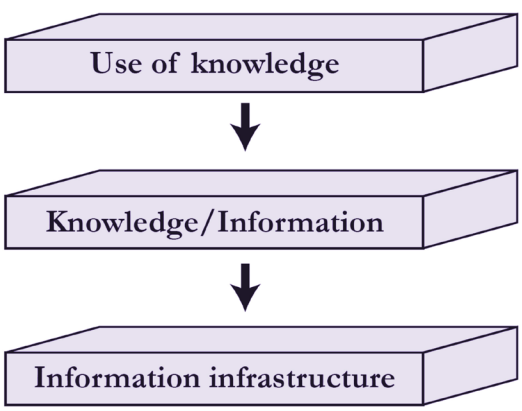
2.1 Critical information infrastructures

Critical information on infrastructure involves three levels: critical service information, business information and consumer information.

The definition of critical infrastructure (CI) is often confused with the definition of a critical information infrastructure (CII). This confusion lies in different perceptions of the definition of a critical asset. When are physical assets that constitute a communication infrastructure considered to be critical? The answer, in fact, is dependent on the information that this physical infrastructure carries, the knowledge that the information represents and the use of that knowledge for motivated reasons.

To aid the understanding of criticality of an information infrastructure throughout the present report, a conceptual framework relating to an information communication system and consisting of three layers, as shown in Figure 1, is considered.

***Figure** 1. Conceptual framework for information and communication. **Source**: Authors*



The use of knowledge differs in criticality depending on the need that drives the use of that knowledge. We give examples here with the aim of differentiating the following three levels of criticality required for knowledge exchange.

Critical. Critical knowledge and/or information is required for the provision of critical services supporting vital societal functions. Such information may even be considered mission critical for some functions, in that the knowledge or information is vital to the functioning of an organisation or the accomplishment of a mission. Examples include public protection and disaster response services, control of utilities (energy generation and distribution, water, etc.), logistics (delivery of food etc.) and transport (cars, buses, trains, aircraft, shipping, etc.).

Business. Business knowledge and/or information is related to the provision of economic development activities requiring high degrees of confidentiality and integrity in information exchange, e.g. development of new products and services (intellectual property), sales and marketing, delivery of products and financial markets.

Citizens/consumers. Such information and/or knowledge is useful for exchanging with friends and family. We expect confidentiality and our privacy must be under our control.

2.2 Rapid advances in technology – fast-changing communication infrastructures and services

Rapid change in technology involves many actors in providing services, which could be a challenge for the security an d quality of the service.

Communication operators will experience increased use of software-defined systems. This is set to fragment the communication system value chain. A transition is expected with the advent of fifth-generation (5G) mobile technology, whose standards allow for new, different and diverse business models. The provision of mobile virtual network operations is likely to change, allowing more agile and dynamic provision of mobile services.

New security challenges will be faced with the increased virtualisation of communication services, whereby they will no longer be physically separated. It is likely that more software components and services will be provided by more actors. This raises new challenges regarding the quality and security assurance of these software components and therefore trust in them.

New challenges will also be faced with the increased dynamics of sharing virtual resources, especially considering the fact that critical, business and citizen communications will probably be hosted on the same physical infrastructure.

2.3 High level of dependency of European society on information and communication systems

With increased use of mobile services, we have more to lose when they become compromised and unavailable.

According to the GSMA (2019), the mobile market is estimated at:

- 5 billion mobile subscribers, constituting 66 % of the world's population, rising to 71 % by 2025;
- 43 % of them using mobile internet, rising to 61 % by 2025.

In Europe there are:

- 465 million mobile subscribers, constituting 85 % of the European population, rising to 88 % by 2025;
- 72 % of them using mobile internet, rising to 82 % by 2025.

There are 3.19 billion users of social media (42 %) globally (Chaffey, 2018), increasing by 13 % year on year. These statistics do not differentiate usage by the three different classifications of criticality described earlier. The majority of users are expected to be citizens communicating with each other, and businesses communicating with each other and with citizens.

As we rapidly move forwards from voice communications to a richer media and immersive environment, we reach an important point to reconsider work carried out in the 1960s by Professor Albert Mehrabian. Mehrabian (1971) studied the role of non-verbal communication, developing the 7–38–55 % rule of personal communication. This

rule shows the importance of non-verbal cues in communication, which extend the effectiveness of communication over and above spoken words. In this rule, 7 % represents spoken words, 38 % voice and tone, and 55 % body language.

This original study related only to feeling and attitudes but gives an important point to consider, now that we can communicate with high-quality voice, which improves tone, and more than just voice, as video calling can also communicate body language (gestures and facial expression). Augmented and virtual reality will extend this. As the use of mobile services increases, we have more to lose when they become compromised and unavailable.

2.4 Cyber-dependent crime as an emerging challenge – new modalities of disaster

It is challenging to identify cybercrime as technology changes quickly and those changes increase complexity.

Cyber-dependent crime (that is, crime that can only be committed using information and communication technology) is an evolving challenge. As vulnerabilities are patched, and new techniques countered, new vulnerabilities and techniques are adopted by criminals.

According to Accenture and Ponemon Institute (2017) the global average cost of cyber-dependent crime was of USD 11.7 million, having increased by 22.7 % in one year. Small companies are also a target, and so suffering losses, but only 14% of small businesses are prepared for cyber-attacks (Accenture and Ponemon Institute, 2019).

Cyber-dependent crime itself can be the root cause of a disaster. Cyber-dependent crime is not just focused on monetary theft or data breaches. It is a primary vector yielding both malicious and non-malicious severe consequences, for example on key utilities that provide our services (electricity, water, etc.). Cyberterrorism must be continually countered to protect these critical infrastructure services.

A report by Europol (2018) focuses on both cyber-dependent crime and many other online threats, such as child sexual exploitation, payment fraud, online criminal markets and Terrorists are becoming increasingly proficient in hiding their traces and activities by using encryption tools and services. Furthermore, the anonymity provided by crypto currencies, and their preferential use in the trades taking place on dark markets, seems to be leading terrorists to invest in this currency. Goods and services offered on Dark net.This ranges from malware, to illegal goods like stolen weapons, to crowd funding sites claiming to support terrorist groups..

The report explains how mobile malware has not yet been reported as a significant issue but is set to become more prominent in the coming years. A major vulnerability and associated mobile malware were discovered in July 2019, affecting WhatsApp (NCSC, 2019), which is used by 1.5 billion users in 180 countries. The deployment of 5G faces some challenges technically and institutionally (Blackman and Forge, 2019). Steadily increasing demand for efficient spectrum utilization as part of the fifth-generation (5G) cellular concept. The rising demands associated with communicating over 5G will make lawful interception and, therefore, investigation and law enforcement more difficult.

Higher degrees of virtualisation in mobile networks will minimise capital expenditure and optimise operating expenditure costs of service delivery. Software components will become smaller and will be delivered by more providers. Security assurance of these virtualised solutions will become even more challenging.

2.5 Vulnerability of physical structures of communication and network systems

The quality and connectivity of communication systems depend upon different service providers, released frequency spectrum and network infrastructure.

Physical aspects of communication systems can be classified in two ways:

1. the crucial physical medium that is required for communication:
   (a) radio spectrum;
   (b) copper and optical fibre;

2. the physical components required to carry out and manage the communication operations, e.g.:
   (a) traditional wired telephone networks – public switched telephone network (PSTN), Integrated Services Digital Network (ISDN), etc.;
   (b) point-to-point high-capacity backhaul:
      i. wired (copper and optical),
      ii. wireless (e.g. microwave, free space optical links, etc.);
   (c) mobile telecoms infrastructures:
      i. mobile base stations, switching facilities, etc.,
      ii. mobile terminals;
   (d) satellite ground stations, and satellites themselves;
   (e) network operation centres.

The radio spectrum is a valuable, yet vulnerable, resource. Any actor can transmit on any frequency. It is easy to listen to transmissions and/or jam radio communications. Jamming, while easy to achieve, is often used in combination with other factors. For example, jamming a 4G mobile connection can be used to force a mobile device to automatically move to 3G or 2G. Attacks such as this are often accompanied by the use of fake base stations to either capture identities or act as a man-in-the-middle.

Spectrum access is heavily regulated, yielding high revenues for governments. Unlicensed spectrum is available but accessed opportunistically. Reliability of unlicensed communication can be questionable, depending on context and circumstance of use. Licensed spectrum often comes with obligations to use a protocol that adopts methods allowing the fair sharing of spectrum resources between users.

Physical components of telecommunication systems require physical security measures to avoid physical compromise. They are often situated in public places requiring strong enclosure which protect 5G equipments or set up to be difficult to reach. At the same time, the whole communication system fails if there is no power.

3 Impacts

3.1 Insights from ENISA reports on incidents

Impacts of natural and human-made disasters on digital services, digital infrastructure and service providers need to be understood to improve services.

As reported by the EU project RAIN (2019), network outages in the telecoms sector are not audited openly or with the same level of public detail as is customary in the power sector, which probably reflects the fact that the telecoms sector is less regulated([1]). It is therefore hard to obtain good, detailed study cases for disaster risk management specialists to analyse. However, incident reporting became mandatory in the EU thanks to Article 13a of Directive 2009/140 EC (the common regulatory framework for electronic communications networks and services).

The European Union Agency for Network and Information Security (ENISA) requires each EU Member State to report incidents affecting the following communication services and networks: fixed telephony (e.g. PSTN, voice over internet protocol over digital subscriber line, cable, fibre), mobile telephony (e.g. Global System for Mobile Communications, Universal Mobile Telecommunications System, Long-Term Evolution), fixed internet access (e.g. digital subscriber line, fibre, cable) and mobile internet access (e.g. General Packet Radio Service/EDGE (IMT Single-Carrier, based on GSM), Universal Mobile Telecommunications System, Long-Term Evolution).

ENISA has collected the data and published annual reports summarising them, starting in 2011. These deal mostly with outages, i.e. disruption in the telecoms service provided by carriers. In the last few years ENISA has supplemented these with additional reports that cover incidents at higher levels of the information infrastructure stack, namely trust providers (which secure electronic transactions, e.g. digital signatures, digital certificates, electronic seals and timestamps) and digital service providers (cloud, online marketplaces and search engines). However, in the following we focus only on incidents related to the core communication services.

One of the first non-trivial insights arising from the data is that the vast majority of incidents are due to system failures (hardware failures and software bugs), followed by human errors and weather events. Incidents caused by malicious intent (i.e. cybersecurity incidents and physical vandalism) represented less than a 10% of the total (Figure 2). We see that, contrary to what all the talk about cybersecurity threats suggests, the actual data tell us that we should be more worried about common equipment failures, human errors and extreme weather events.

Of course, this picture is likely to be different if we consider other, non-telecom, information services, such as trust providers and general cloud service providers, as those are inherently more dependent on internet-exposed information technology systems. Likewise, the severity of the incidents labelled as minor and large are on the rise (Figure 3).

([1]) See *https://ec.europa.eu/digital-single-market/en/policies/telecom-laws*

Figure 2. *Incidents reported by root cause.*
Source: *Authors using the Cybersecurity Incident Report and Analysis System – Visual Analysis Tool (ENISA, n.d.).*

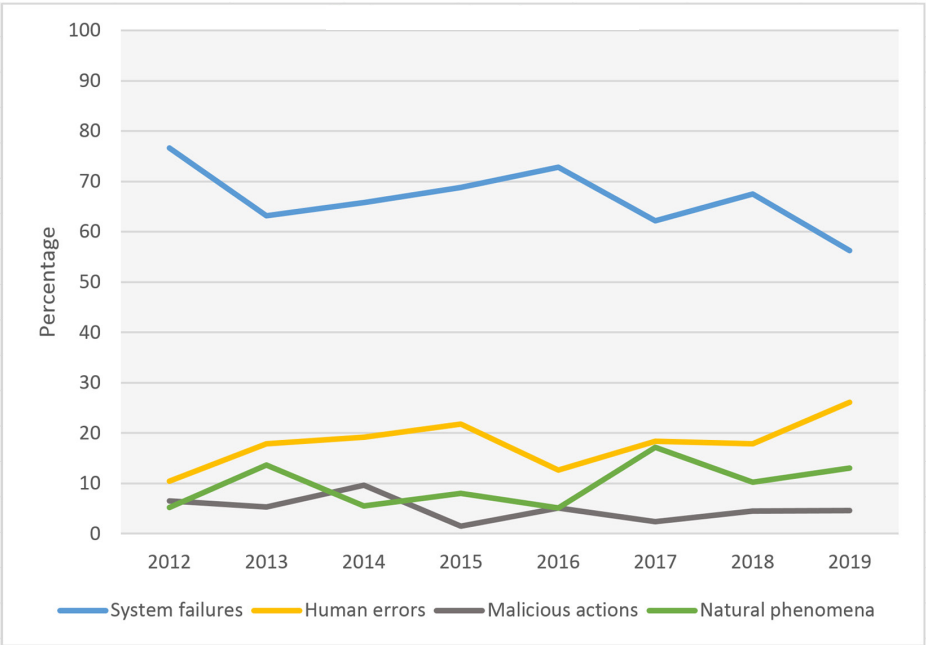
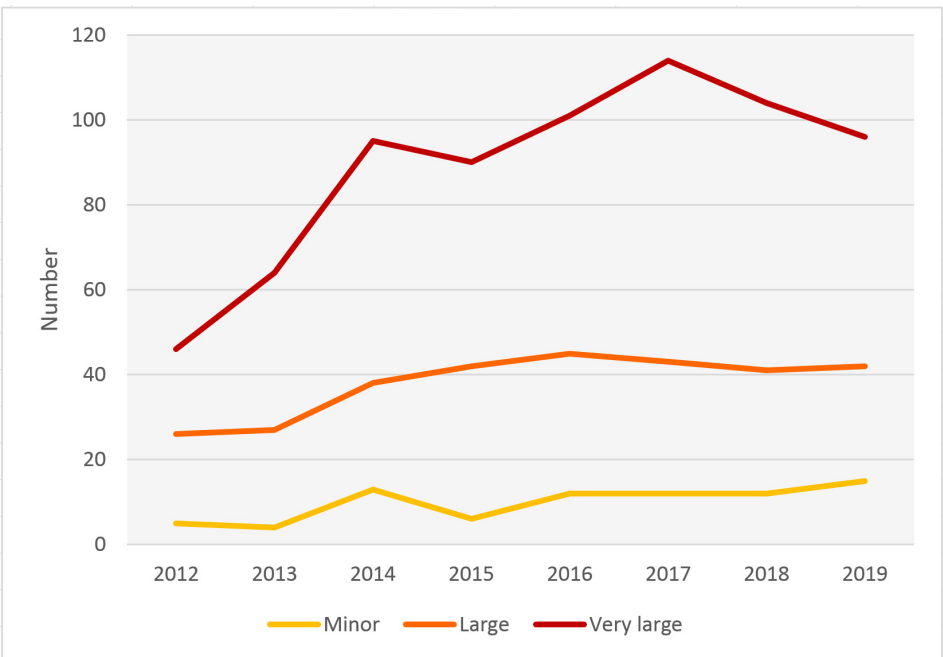


Figure 2. *Incidents reported based on their severity of impact.*
Source: *Authors using the Cybersecurity Incident Report and Analysis System – Visual Analysis Tool (ENISA, n.d.).*



Here are other relevant insights to extract from these reports, over the 7 years they have been running.

- Incidents due to extreme weather are trending upwards: heavy storms, major floods or wildfires caused by extreme drought are being spotted more often.
- Natural phenomena (in particular, wildfires) also cause the highest number of user-hours lost per incident, on average, amounting to 56 800 user-hours in 2017.
- Most incidents have an impact on mobile telephony and mobile internet. In 2017, 51 % of all reported incidents were in mobile telephony.
- Incidents in mobile telephony and mobile internet affect, on average, the most users: on average, around 500 000 users per reported incident, or around 8 % of the national user base.
- Human errors affect, on average, a high number of user connections. In 2017, human error was the category of root cause affecting the most users per incident (around 1.2 million user connections on average).
- Regarding network assets, mobile phone base stations (9 %) and controllers and mobile switches (8 %) were the network components most affected by incidents.

3.2 Societal impact and isolation when communication systems are not available

Multiple services depend on communication systems and if they fail, then it creates anxiety in society. People become ready to pay more to back up the service.

Assessing the socioeconomic impacts of outages, and in particular of the effects of major disruptions, is key to correctly assess the risk and vulnerability of a geographical region and population. Target D of the Sendai Framework for Disaster Risk Reduction addresses damages and destruction of critical infrastructures and the services disrutptions, including Information and Communication Technology (ICT) systems (UNISDR, 2017).

The direct impact of a disruption of service is usually assessed in economic terms, in the form of the value of lost service, which is one of the most commonly accepted measurements. However, social effects are not easily incorporated into impact measurements. Collaboration between economists, engineers and social scientists helps in quantifying these effects. When communication systems fail, we will naturally find a way to retrieve information. We will talk to neighbours, physically moving to seek out knowledge of the situation. We will look for alternative methods of communication. In the Storm Desmond example described below, some people sought other communication systems to get information. In this case, the individual involved had technical knowledge. Many others will not, which may result in a feeling of isolation.

Regarding the measurement of other social effects beyond the direct economic impacts of an outage, many

different approaches are used. Most studies have been on power outages, but the methods could be easily extended to analyse the effects of telecommunication system disruptions. Four of them are listed below, the first three methods being the most commonly used (Walker et al., 2014; Linares and Rey, 2013; Centolella, 2013; Grünewald and Torriti, 2012). (Rain Project, Milenko Halat)

- Customer surveys. Customers are asked their willingness to pay (WTP) to avoid outages or their willingness to accept compensation for having a higher number of interruptions. This direct method is also called the stated preference approach.

- Case studies. Past events are analysed; thus, estimations of costs are more detailed and based on actual outages. However, only limited and specific information is available (the incidents occurred in particular circumstances).

- Production function approach. The goal is to get the total value of service loss by computing the ratio of an economic measure, such as gross domestic product, and a measure of electricity consumption, e.g. kWh. Then, it is usually given in terms of EUR/kWh. Finally, cost of lost leisure time can be also included. It can be monetised by using Becker's model (Becker, 1965) as de Nooij and colleagues propose (Nooij et al., 2007).

- Market behaviour. This approach is based on the expenditures on backup devices/facilities, and the price of interruptible contracts. These expenses can reflect what is the WTP of the customers (it is a form of revealed preference). However, in regions with high reliability there are no market signals (the user trusts the service); and some community service providers (e.g. hospitals) must be equipped with backup systems by law

4 Cases: scenarios where communication networks have failed – examples of impact

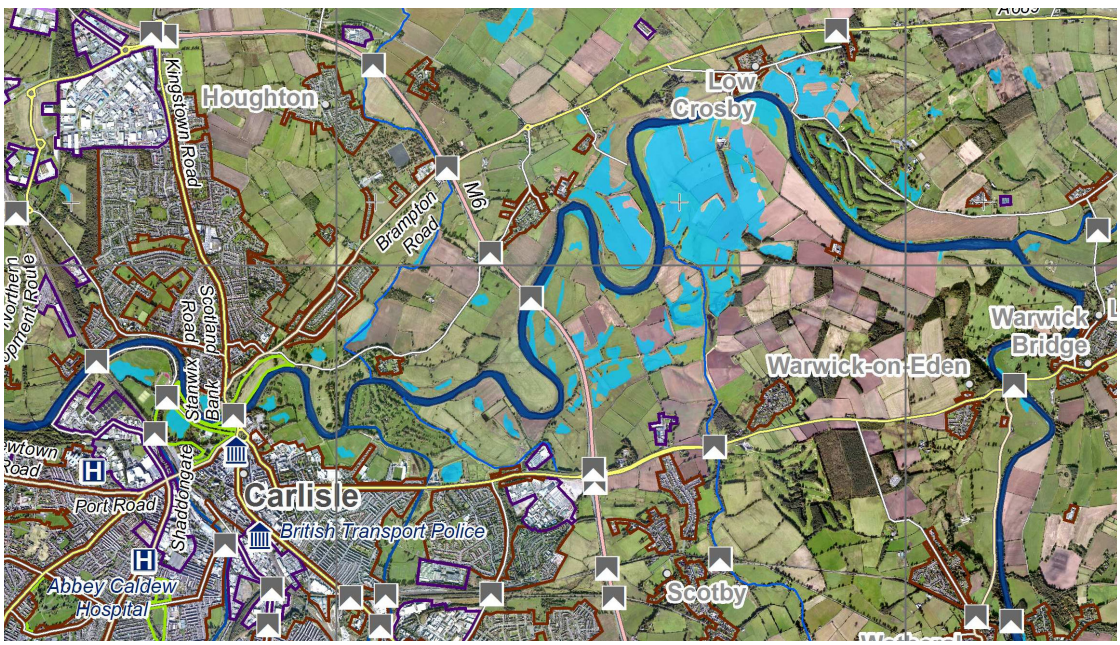
Systems need to be prepared for post-disaster situations in case there is a power failure, to avoid interruption of communication systems and protect the communication infrastructure.

4.1 Storm Desmond: communication services lost as result of power outage due to flooding

Storm Desmond was an extratropical cyclone that caused significant damage in North West England in December 2015. One month's rain fell over 24 hours. The counties of Cumbria and Lancashire were hit especially hard, with severe flooding causing significant damage to critical infrastructure and three fatalities. More than 60 000 properties in northern England were without power and more than 1 000 people were evacuated because of the floods (Davies and Glanfield, 2015).

Flood defences at Carlisle and Kendal's main electricity substations protected power supplies but the flooding of smaller sub-stations and properties resulted in a substantial number of properties losing power. At the peak of flooding, it was estimated that more than 17 00 costumers lost electricity, the majority of these in Carlisle district (Cumbria County Council, 2015) (Figure 4). It is known that telecommunication systems were impacted although the number and location of costumers is unknown as well as the duration of the disruption (Cumbria County Council, 2015; Environment Agency, 2018).

Figure 4. *Situation of Carlisle city and its surroundings on the 7th December 2015*
Source*: extracted from Copernicus, 2015. © European Union, 2015.*



The description below is of the direct experience of one of the authors, who suffered the power outage. Although it remains a partial narrative, it serves to illustrate the impact of the event.

The loss of power occurred around 22.00–23.00 on a Saturday evening. When residents woke up on Sunday morning, power had not been restored. For a local resident in the outskirts of Lancaster city centre, who had previously only experienced short power outages of 1–2 hours in recent years, this already longer outage was worrying. It was difficult to find out the status of power loss. With no electricity, there was no television reception, no ADSL (asymmetric digital subscriber line) internet access and no mobile network coverage. Although mobile phones retained battery power, there was no mobile signal. Landline telephones and local radio both remained usable. However, use and reception required knowledge and equipment that the general public would typically not have to hand. Initial attempts to connect by landline telephone were not successful owing to the use of digital enhanced cordless telecommunications (DECT) cordless phones. The base unit of a DECT system requires power, so it was inaccessible. On searching through old stores, the author found an old PSTN wired telephone. This unit was operational, as the PSTN telephone line had retained power and connectivity. A call was made to family living in a different region of the United Kingdom confirming, from internet news, that the power outage was due to flooding of the substation. However, details were limited.

As the author of this section has technical knowledge, author knew it was known that the BBC local radio service was responsible for notifying the public in cases of emergency. In this case BBC Radio Lancashire was the relevant outlet. The majority of radio receivers in the home relied on mains power and were therefore unusable. A battery-powered receiver was found. The radio was usable; however, a scan on the frequency modulation (FM) band did not find BBC Radio Lancashire. A commercial local station was found. On listening for more than an hour, no news was received but only a cycle of automated music with no presentation intervention. The author scanned again and found a weak signal for BBC Radio Cumbria. Regular announcements were made every 15 minutes regarding closed roads, where to find aid and a lot of useful supporting information. However, this information was useful in Cumbria and not entirely relevant to the locality of Lancaster, where information regarding the power outage was sought. The safety of refrigerated and frozen food became a concern after more than 12 hours of power outage.

Listening for 1–2 more hours, the author heard an announcement that power to the local FM transmitter for Lancaster had also been lost, so listeners in Lancashire should tune to the medium wave (MW) band. The specific tuning frequency was announced but unintelligible owing to the reception quality. The landline was used again to make a call to remote family to request a web search for BBC Radio Lancashire's MW tuning frequency. Details were obtained, the radio tuned and local information received on a regular basis. It became apparent that risk to the author's property was thankfully minimal, yet the power outage would persist for many days.

Initially, generators were deployed and prioritised to the local hospitals. Reports were heard that mobile coverage was restored in the locality of the hospital. Over the next 24–48 hours generators were set up and for 4–5 days they supplied the majority of the 55 000 properties until the substation could be repaired.

This case study suggests that, during disaster, effective and immediate communication is essential. It can be achieved through regular training of local stakeholders on communication systems.

4.2 Manchester Arena bombing – communication services lost as a result of poor processes and configuration

At just after 22.30 on Monday 22 May 2017, a suicide bomber detonated an improvised device in the foyer of Manchester Arena. Around 14 000 people, mainly teenagers and their families, had travelled from across the United Kingdom to attend a concert by Ariana Grande, which was just coming to an end. The foyer was busy with exited concertgoers, waiting family members and merchandise sellers.

The bomb killed 22 people including many children. Over 100 were physically injured and many more suffered psychological and emotional trauma. Paramedics treated many walking wounded in the city centre. Hospitals in Greater Manchester treated people with serious injuries, transported by the ambulance service, while others made their way to hospitals across the wider region. Kerslake (2018) cites a failure of Vodafone to set up a national mutual aid telephony system. This system provides a telephone contact service for relatives to call. This failure caused significant stress and upset to the families involved that night, who were seeking to find out more about the situation of their loved ones. Some resorted to a frantic search around the hospitals of Greater Manchester in their search for information. This is an example of a typical human-made communication failure based upon commercial decisions. There was no technical fault, yet citizens' stress was exacerbated and could

have been avoided. Figure 4 shows the blast area, between the main arena and neighbouring Victoria Station. It blew people off their feet and caused widespread panic. Witnesses described hearing an explosion and seeing a flash of fire.

5 Proposed solutions

The following solutions are proposed in order to build resilience, on both a societal and a technological level.

Empower local groups/communities to respond independently

We must prepare the public for disaster in case of lost digital communication connectivity, both to obtain information regarding the situation, so that they can help themselves, and to be able to still communicate by means that have fewer capabilities but are more reliable.

Local resilience forums should work to educate the public to know how to communicate in times of crisis or communication failure. This work must take clear note of the digital divide, to offer modes of alternative communication that individuals will be able to easily use and access.

Operational mobility for responders – Europe-wide communication capabilities for public protection and disaster response

Public safety operations will be enhanced by the availability of pan-European mobile broadband. 'Operational mobility' means that a public safety responder will be able to carry out their operations wherever they physically are, and with anyone in their communication group wherever they are. All communications should not be restricted by geopolitical boundaries. BroadWay (2019) is carrying out pre-commercial procurement of technical solutions to enable operational mobility.

Explore/innovate communication technologies that can function independently from the physical infrastructure

We must not lose sight of existing, highly resilient, low-bandwidth communication techniques. Long-range services, such as low frequency, high frequency and very high frequency, can also be used to provide voice and low-speed data services, where more capable broadband is not possible. FM, amplitude modulation and short wave services have been relied upon since the early 1900s. A high number of amateur radio enthusiasts around the world continually develop new ideas to communicate over long distances. This skill set is valuable and its practitioners should be encouraged to take part in situations where response and additional communication methods are needed in times of disaster.

Capacity building to 'build back better': speedy restoration of the communication system

Reliance only on fixed infrastructure for mobile phones leaves us vulnerable. Preparation should seek to rapidly replace service in circumstances where service is lost to equipment failure or damage. Tactical networks should be prepared to enable fast replacement of mobile coverage. Airborne coverage may be provided by aircraft, balloons, satellites, etc. Cells on wheels can be deployed to provide additional or replacement coverage.

Legislation

Policy and legislation should make operators of communication infrastructures responsible for maintaining a high level of resilience, taking into account all possible options to keep people connected. especially in compromised technical situations, and especially when social situations require additional support when disaster hits. Citizens should remain connected. This is becoming a societal expectation.

Mobile communication services for public safety responders should have the highest priority over and above all non-safety-critical communications. Service availability of mobile communication for responders should be the same everywhere, at all times and whatever the conditions when a responder needs to operate.
Legislation about public alerts should require guarantees of service to reach the public with information regarding developing situations where public safety is at increased risk.

Building a resilient communication capability

Legislation should aim to guarantee availability of communication services. The need to power new communication systems reliably is crucial, especially in terms of crisis, but awareness of the need is diminishing. When power fails, communication networks fail in a cascade. Communication failure leads to limited response by emergency services, restricted communication to and from the public, potential for lack of coordination, and the possibility of lost lives and/or public disorder. Current mobile communication connectivity is not resilient and cannot be relied upon, yet the public and business increasingly depend upon it.

For example, the highly trusted wired ISDN/PSTN communication infrastructure (landlines) will be turned off by 2025 . Security systems for both building security and fire protection have relied on this highly reliable wired service for more than 30 years. ISDN and PSTN lines carry voice, data and, crucially, their own autonomous source of power, independent from the power grid. Replacing ISDN with optical fibre or wireless communication removes the possibility of delivering dedicated power over a long range. Power will have to be delivered locally, creating a significant reliance on power supply for communication equipment to be locally resilient.

Building a secure communication capability

New cybersecurity certification processes, as a result of the EU Cybersecurity Act, are under development at the time of writing. They will be focused on new challenges posed by the development of new communication network infrastructures such as 5G. Those certification processes should, however, retrospectively apply to all existing communication infrastructure. Communication networks of all natures should be covered. This includes national terrestrial and international satellite infrastructures, ranging from fully licensed, managed and regulated systems to unlicensed self-deployed systems and even amateur radio.

6 Conclusions and key messages

Policymakers

- Enhance and enforce reliability policy and standards. Take a cue from the power sector regulatory standards and require something similar for telecom operators. Standardise and refine reliability indicators for all large telecom networks. Ensure that telecom and mobile network operators are fully accountable when their services fail. Policy should encourage backup power sources for mobile infrastructure and rapidly deployable coverage to improve resilience in circumstances of unavoidable communication network failure. Availability of mobile communication has become a societal expectation, especially when disaster strikes.

- Pay more attention to disaster risk and extreme weather events using quantitative analysis. For example, risks related to extreme weather receive less concern than cybersecurity, but the actual statistics tell us that weather events are a greater risk. Their impacts are greater, since other infrastructures (most notably power) are often affected simultaneously. Telecom networks are complex infrastructures, so quantitative analysis of failure is important for decision-making during an event, and to understand where to invest in future preparedness.

- Monitor our growing dependency on information infrastructures and online information technology services. Outages in information infrastructure and online services (e.g. global positioning system navigation maps, messaging apps, banking apps) are not considered as critical as an outage of the underlying telecom service. Ensure that actors within local resilience forums (or any coordinated disaster risk forum) are aware of the vulnerability of mobile communication and information services and are prepared to use alternative communication networks and information services when mainstream mobile networks and services become limited or unavailable.

- The cybersecurity of communication networks must be of primary concern. Common certification processes should assure communication for crime and disaster response to high levels of assurance, shared across all EU Member States and collaborating countries.

Practitioners and scientists

- Strive to provide quantitative risk studies. Promote and require engineering-based, quantitative risk assessment methodologies, especially when making investment decisions. Purely qualitative studies based on vague risk matrices are no longer adequate.

- Team up with engineers, statisticians and data scientists. Modern techniques, such as Bayesian networks and Monte Carlo simulation, allow engineering-based models to be combined with data-based machine learning approaches to obtain better quantitative results. Extreme weather events are becoming more important. Weather is behind a relatively small number of incidents, but those have the greatest impact because of the disruptive effects on other critical infrastructures, and because of the long times to recovery. Keep an eye on climate change trends.

- All information systems should be widely usable, and acceptable to both the public and responders'. Minimisation of the effects of the digital divide should be driven by the need for improved resilience. Ethical, legal and societal issues in different contexts of use should be a key consideration. Societal Impact of new communication methods and tools should be understood, and negative impacts mitigated.

Citizens

- Citizens must have no significant burden placed on them whereby communication technology may become a risk to societal life. Responsible behaviour is essential during disaster communication. Only authoritative and confirmed information should be communicated, to stop civil unrest during emergency period. False messages and fake news should not be circulated using social media, which would put unnecessary pressure on disaster management workers.

- Become aware of your dependency on telecoms and information services. Citizens must be offered education to make them aware of the limitations of their mobile communication and internet access technologies and information services.

- Become prepared for outages. Citizens must be provided with knowledge of how to communicate or obtain information when their familiar mobile communication or other internet connectivity becomes unavailable during compromised situations. Citizens must be prepared for outages in phone lines, the internet or online services. Keeping batteries or small generators for powering radios and phones can sometimes save lives.

- Citizens must join with policymakers, practitioners and scientists to take action for better preparedness', to protect society in the face of disaster, crime and terrorism. Regular scrutiny and mechanism should be developed to identify false information, fake news, etc., in order to avoid confusion and reduce the burden during emergency periods.

Conclusions

Critical infrastructures are complex assets and systems. This subchapter has focused on some of the CI assets and systems at risk and the potential impacts should such assets and systems be disrupted for any reason.

Section 3.4.1 provided a set of examples, with guidelines for continuity management and policies formulated in order to reduce vulnerability and increase flexibility during worst-case scenarios. It emphasised integrating cascading events into emergency management and business continuity practice, increasing awareness of interconnected dynamics and reassessing the locations of critical infrastructure based on hazards and vulnerabilities, as steps towards improving the organisational resilience of emergency facilities.

Section 3.4.2 discussed networked infrastructures, the centrality of which provides some degree of resilience by design but also results in fragilities being not only intrinsic to each technological layer but manifest at the boundaries between systems. Policymakers should focus on stakeholder engagement and information sharing, including public–private partnerships with operators and citizen involvement initiatives. Practitioners are encouraged to use new technologies, such as monitoring tools or information-sharing platforms, when faced with varying technical, financial, political, reputational and legal priorities and constraints. Training and exercises or stress tests represent an opportunity to identify gaps and coordinate for better resilience. Citizens can benefit greatly from new technologies, for instance as a way to get alerts to service disruptions and also to report quickly on the failures they observe. Scientists can assist policymakers, operators and responders in better understanding failure propagation through networks, identifying mitigation actions and optimising response plans. Scientific effort should be devoted to tool interoperability, large-scale simulation, the treatment of uncertainty, reliability and dependability assessment, as well as resilience aspects.

Section 3.4.3 addressed risks to society and the environment from damage to core industrial and energy facilities due to human-made and natural hazards and how these impacts can be prevented or reduced in the future. Policymakers (including government authorities) are encouraged to develop policies in a transparent manner, based on experience and science. Risk governance insights from different sectors, especially from high-hazard activities, could be useful guidelines in this area. Practitioners should adopt good practices in risk management, including cross-fertilisation between sectors, and develop plans to facilitate recovery after infrastructure failure.

Section 3.4.4 discussed the role of the communication systems and their varying degrees of responsibility for the transfer of information of differing levels of criticality. Decision-makers are urged to enhance and enforce reliability policies and standards, using quantitative analysis to integrate disaster risk in the political decision-making process, and being aware of modern societies' reliance on information and communication technologies. Practitioners and scientists should strive to provide quantitative analyses of risk and to use multidisciplinary approaches when supporting investment and public policy decisions. The interoperability of

information technology equipment is also emphasised as a critical area for practitioners. Lastly, citizens are encouraged to prepare for disaster-generated outages of information technology and other CI.

Protecting CIs requires a comprehensive, collaborative, risk-based and integrated approach at the regional, national and cross-border levels. The protection of CIs necessitates a system that builds on and elaborates the requirements of the European Critical Infrastructure (ECI) Directive, currently under review by the Directorate-General for Migration and Home Affairs, while taking into consideration the challenges stemming from the inherent technical complexity of infrastructure systems, the diversity in ownership, geography, asset and system types, and national and EU regulations.

The organisation and structure chosen to protect CIs should allow all levels of government, all jurisdictions, all disciplines and all actors (public and private) to work together to reduce the risk from all hazards and threats to CI. Relevant EU legislation should be applied and incorporated into national law, using an integrated rather than piecemeal approach, reducing ambiguity and minimising added requirements of CI operators.

A comprehensive risk assessment is to be adopted, combining the national risk assessment requirements emerging from the Union of Civil Protection Mechanism (Decision No. 1313/2013/EU) of the European Parliament and of the Council of 17 December 2013, with the assessment of risk to CI's in the context of the ECI Directive of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection (Council Directive 2008/114/EC) and the designation of essential services in line with the NIS Directive of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (Council Directive 2016/1148/EU), at the heart of the process. Embracing a combined contingency and systems approach helps to identify hazards, vulnerabilities and threats, update the list of critical infrastructures and essential services, determine interdependencies and ultimately define capability targets.

All interested and affected parties should be involved in the process within specifically set up national sectoral bodies or forums. This can be best achieved through their security liaison officers as defined by the ECI Directive (Council Directive 2008/114/EC). Multi-agency coordination, both in the steady state and during crises, is best driven by the CI bodies/sectoral forums. National CI bodies and/or forums should bring together the public and private entities involved.

Information and communication technologies are leveraged to help build and sustain a common operational picture. Training and knowledge sharing play a central role in the process. Workshops and crisis response exercises are conducted on a regular basis, while the involvement of relevant EU institutions helps to ensure consistency at the EU level and augment local capabilities.

References

Introduction

Agius, J., Bonazountas, M., Karagiannis, G., Krikigianni, E., Tsiakos, C., 2017, 'Risk assessment: Supporting public policy in an uncertain world', in: Formosa, S. (ed.), *Emergent Realities for Social Wellbeing: Environmental, spatial and social pathways*, University of Malta, Msida, pp. 381–399.

Air University, 1987, *The United States Bombing Surveys (European War – Pacific War)*, Air University Press, Montgomery, Alabama.

European Commission, 2006, Commission communication – on a European Programme for Critical Infrastructure Protection (COM(2006) 786 final), https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2006:0786:FIN:EN:PDF.

Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, OJ L 345, 23.12.2008, pp. 75–82, https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:EN:PDF.

Karagiannis, G. M., Chondrogiannis, S., Krausmann, E., Turksezer, Z. I., 2017, *Power grid recovery after natural hazard impact*, Publications Office of the European Union, Luxembourg.

Lazari, A., 2014, *European Critical Infrastructure Protection*, Springer, London.

Linkov, I., Bridges, T., Creutzig, F., Decker, J., Fox-Lent, C., Kröger, W., Lambert, J. H., Levermann, A., Montreuil, B., Nathwani, J., Nyer, R., Renn, O., Scharte, B., Scheffler, A., Schreurs, M., Thiel-Clemen, T., 2014, 'Changing the resilience paradigm', *Nature Climate Change*, Vol. 4, No 6, pp. 407–409.

Pescaroli, G., and Alexander, D. E., 2015, 'A definition of cascading disasters and cascading effects: Going beyond the "toppling dominos" metaphor', *Planet@ Risk*, Vol. 3, No 1, pp. 58–67.

UNDRR Glossary 2017, 'Report of the open ended intergovernmental expert working group on indicators and terminology relating to disaster risk reduction', https://www.preventionweb.net/files/50683_oiewgreportenglish.pdf.

White House, 1998, The Clinton Administration's Policy on critical infrastructure protection: Presidential Decision Directive 63 (PDD-63), White Paper, 22 May 1998, https://fas.org/irp/offdocs/paper598.htm.

3.4.1 Emergency infrastructures and facilities

Aitsi-Selmi, A., Murray, V., Wannous, C., Dickinson, C., Johnston, D., Kawasaki, A., ... Yeung, T., 2016, 'Reflections on a science and technology agenda for 21st century disaster risk reduction', *International Journal of Disaster Risk Science*, Vol. 7, No 1, pp. 1–29.

Aldea-Borruel, X., Mian, J., Schnurr, A., 2019, *EARTH EX – London and Glasgow: Building resilience for global scale complex catastrophes*, Workshop Report, Electric Infrastructure Security Council and Resilience Shift, London, UK.

Alexander, D. E., 2007, 'Disaster management: From theory to implementation', *Journal of Seismology and Earthquake Engineering*, Vol. 9, No 1, pp. 39–49.

Alexander, D. E., 2016, *How to Write an Emergency Plan*, Dunedin Academic Press, Edinburgh and London.

Birkmann, J., Kienberger, S., Alexander, D. E. (eds.), 2014, *Assessment of Vulnerability to Natural Hazards: A European perspective*, Elsevier, San Diego, CA.

British Standards Institution (BSI), 2014, *Guidance on Organisational Resilience*, BSI Standards Limited.

Clark-Ginsberg, A., Rueda, I. A., Monken, J., Liu, J., and Chen, H., 2020, 'Maintaining critical infrastructure resilience to natural hazards during the COVID-19 pandemic: hurricane preparations by US energy companies', *Journal of Infrastructure Preservation and Resilience*, Vol. *1,* No 1, pp.1-6.

Coetzee, C., Van Niekerk, D., 2012, 'Tracking the evolution of the disaster management cycle: A general system theory approach', *Jàmbá: Journal of Disaster Risk Studies*, Vol. 4, No 1, pp. 1–9.

Crane, L. 2017, 'The Sun just belched out the strongest solar flare in 12 years', *New Scientist*, https://www.newscientist.com/article/2146617-the-sun-just-belched-out-the-strongest-solar-flare-in-12-years/.

Environment Agency, 2006, *Cumbria Floods Technical Report – Factual report on meteorology, hydrology and impacts of January 2005 flooding in Cumbria*, Environment Agency, London.

Environment Agency and Cumbria County Council, 2016, *Carlisle Flood Investigation Report – Flood event 5–6th December 2015*, Environment Agency, London.

European Commission, 2013a, Commission staff working document – Adapting infrastructure to climate change (SWD (2013) 137 final), European Commission, Brussels.

European Commission, 2013b, Commission staff working document – On a new approach on the European Programme for critical infrastructure protection – Making European critical infrastructure more secure (SWD (2013) 318 final), European Commission, Brussels.

EU, 2007, Directive 2007/60/EC of the European Parliament and of the Council of 23 October 2007 on the assessment and management of flood risks (Text with EEA relevance), OJ L 288, 6.11.2007, pp. 27–34.

EU, 2008, Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection (Text with EEA relevance), OJ L 345, 23.12.2008, pp. 75–82.

Helbing, D., 2013, 'Globally networked risks and how to respond', *Nature*, Vol. 497, No 7447, pp. 51–59.

Helsloot, I., Beerens, R., 2009, 'Citizens' response to a large electrical power outage in the Netherlands in 2007', *Journal of Contingencies and Crisis Management*, Vol. 17, No 1, pp. 64–68.

Hellström, T. 2007, 'Critical infrastructure and systemic vulnerability: Towards a planning framework', *Safety science*, Vol 45, No 3, pp. 415-430.

Field, C. B. (Eds.) 2012, Managing the risks of extreme events and disasters to advance climate change adaptation: special report of the Intergovernmental Panel on Climate Change (IPCC), Cambridge University Press, Cambridge.

International Standards Organisation (ISO), 2017, *Security and Resilience – Organisational resilience – Principles and attributes*, BSI Standards Limited, London.

International Standards Organisation (ISO), 2019, *Security and Resilience – Business continuity management systems – Requirements (ISO 22301:2019)*, BSI Standards Limited, London.

Jackson, K., 2019, 'California's blackouts: How did we get here and what can we do to keep the lights on?', *PRI Capital Ideas*, Vol. 5, No 11, 1-13.

Kates, R. W., Pijawka, D., 1977, 'From rubble to monument: The pace of reconstruction', in Haas, J. E., Kates, R. W., Bowden, M. J. (eds.), *Disaster and Reconstruction*, MIT Press, Cambridge, MA, pp. 1–23.

Klinger, C., Landeg, O., Murray, V. 2014, 'Power outages, extreme events and health: A systematic review of the literature from 2011–2012', *PLoS Currents*, Vol. 6, pp. 1–22.

Lindell, M. K., Prater, C., Perry, R. W., 2007, *Introduction to Emergency Management*, Wiley, Hoboken, NJ.

Linkov, I., Fox-Lent, C., 2016, 'A tiered approach to resilience assessment', in Florin, M.-V., Linkov, I. (eds.), *IRGC Resource Guide on Resilience Volume 1*, EPFL and International Risk Governance Council, Lausanne, pp.1-4, www.irgc.org/risk-governance/resilience/.

Linkov, I., Bridges, T., Creutzig, F., Decker, J., Fox-Lent, C., Kröger, W., Lambert, J. H., Levermann, A., Montreuil, B., Nathwani, J., Nyer, R., Renn, O., Scharte, B., Scheffler, A., Schreurs, M., Thiel-Clemen, T., 2014, 'Changing the resilience paradigm', *Nature Climate Change*, Vol. 4, No 6, pp. 407–409.

National Fire Protection Association, 2019, *NFPA 1600: Standard on continuity, emergency and crisis management*, National Fire Protection Association, Quincy, MA.

Neal, D. M., 1997, 'Reconsidering the phases of disasters', *International Journal of Mass Emergencies and Disasters*, Vol. 15, No 2, pp. 239–264.

Nones, M., Pescaroli, G., 2016, 'Implications of cascading effects for the EU Floods Directive', *International Journal of River Basin Management*, Vol. 14, No 2, pp. 195–204.

Perri, M. A., 2014, 'Alluvione e radio: Come il 118 ha reagito al blackout', *La Repubblica Parma*, 15 October, https://parma.repubblica.it/

cronaca/2014/10/15/news/alluvione_e_radio_come_il_118_ha_reagito_al_black_out-98187073/.

Pescaroli, G., Alexander, D. E., 2018, 'Understanding compound, interconnected, interacting, and cascading risks: A holistic framework', *Risk Analysis*, Vol. 38, No 11, pp. 2245–2257.

Pescaroli, G., Turner, S., Gould, T., Alexander, D. E., Wicks, R. T., 2017, *Cascading effects and escalations in wide area power failures: A summary for emergency planners*, UCL IRDR and London Resilience Special Report 2017-01, Institute for Risk and Disaster Reduction, University College London, DOI: 10.13140/RG.2.2.29607.04008.

Pescaroli, G., Wicks, R. T., Giacomello, G., Alexander, D. E., 2018, 'Increasing resilience to cascading events: The M. OR. D. OR. scenario', *Safety Science*, Vol. 110, No C, pp. 131–140.

Petermann, T., Bradke, H., Lüllmann, A., Poetzsch, M., Riehm, U., 2011, *What Happens during a Blackout*, Office of Technology Assessment at the German Bundestag, Berlin.

Petri, L., Ciocci, C., 2014, 'A Parma investito il poliambulatorio', *Il Giornale della Previdenza*, Vol. 8, pp. 22–23, https://www.enpam.it/news/a-parma-investito-il-poliambulatorio/.

Protezione Civile Emilia-Romagna, 2015, *Piano dei primi interventi urgenti di Protezione Civile in conseguenza delle eccezionali avversità atmosferiche che nei giorni 13 e 14 ottobre hanno colpito il territorio delle province di Parma e Piacenza*, Bologna, OCDPC 202, 14 November, http://wwwservizi.regione.emilia-romagna.it/eventicalamitosi/scheda_piano.asp?IDPiano=219.

Royal Academy of Engineering, 2016, *Living without Electricity: One city's experience of coping with loss of power*, RAE, London.

Smart, W., 2018, *Lessons learned review of the WannaCry ransomware cyber attack*, independent report for NHS, https://www.england.nhs.uk/wp-content/uploads/2018/02/lessons-learned-review-wannacry-ransomware-cyber-attack-cio-review.pdf

Sommer, P., and Brown, I. 2011, *Reducing systemic cybersecurity risk*. IFP/WKP/FGS(2011), Organisation for Economic Cooperation and Development, Paris.

Stern, E., Newlove, L., Svedin, L., 2003, *Auckland Unplugged – Experiences gained and lessons learned*, Lexington Books, Oxford.

UNISDR, 2015, *Sendai Framework for Disaster Risk Reduction*, UNISDR, Geneva, https://www.undrr.org/publication/sendai-framework-disaster-risk-reduction-2015-2030.

UNISDR, 2012, *How to Make Cities More Resilient: A handbook for local government leaders*, https://www.undrr.org/publication/how-make-cities-more-resilient-handbook-local-government-leaders.

UNISDR, 2017, *Words into Action Guidelines: National disaster risk assessment*, www.unisdr.org/we/inform/publications/52828.

UNDRR, 2019, *Words into Action Guidelines: Implementation guide for local disaster risk reduction and resilience strategies*, www.unisdr.org/we/inform/publications/57399.

Van Eeten, M., Nieuwenhuijs, A., Luiijf, E., Klaver, M., Cruz, E., 2011, 'The state and the threat of cascading failure across critical infrastructures: The implications of empirical evidence from media incident reports', *Public Administration*, Vol. 89, No 2, pp. 381–400.

World Health Organization, 2019, 'Earthquakes – Technical hazard sheet – Natural disaster profile', https://www.who.int/hac/techguidance/ems/earthquakes/en/.

World Health Organization and Public Health England, 2013, *Emergency Risk Management for Health – Overview*, Global Platform, May, http://www.who.int/.

York, C. (2020) 'Flooding, Heatwaves, Terrorism: What Would Happen If A Second Crisis Hit The UK During Coronavirus?' *Huffington Post*, 09/05/2020, https://www.huffingtonpost.co.uk/.

3.4.2 Network infrastructures

Albert, R., Jeong, H., Barabási, A.-L., 2000, 'Error and attack tolerance of complex networks', *Nature*, Vol. 406, pp. 378–382, https://doi.org/10.1038/35019019.

Alderson, D. L., Doyle J.C., 2010, 'Contrasting Views of Complexity and Their Implications for Network-Centric Infrastructures', *IEEE Transactions on Systems, Man, and Cybernetics Part A:Systems and Humans*, Vol. 40, No 4, pp. 839-852, https://doi.org/10.1109/TSMCA.2010.2048027.

Alexander, D., 2013. 'Volcanic Ash in the Atmosphere and Risks for Civil Aviation: A Study in European Crisis Management', *International Journal of Disaster Risk Science*, Vol. 4, pp. 9–19, https://doi.org/10.1007/s13753-013-0003-0.

Alexander, D., 2018, 'A Magnitude Scale for Cascading Disasters', *International Journal of Disaster Risk Reduction*, Vol. 30, Part B, pp. 180-185, https://doi.org/10.1016/j.ijdrr.2018.03.006.

Allen, M., Robert C., Cotruvo, J.A., Grigg, N., 2018, 'Drinking Water and Public Health in an Era of Aging Distribution Infrastructure', *Public Works Management & Policy*, Vol. 23, No 4, pp. 301–309, https://doi.org/10.1177/1087724X18788368.

Argyroudis, S. A., Fotopoulou S., Karafagka S., Pitilakis K., Selva, J., Salzano E., Basco, A., et al. 2019, 'A Risk-Based Multi-Level Stress Test Methodology: Application to Six Critical Non-Nuclear Infrastructures in Europe', *Natural Hazards*, Vol. 100, pp. 595–633, https://doi.org/10.1007/s11069-019-03828-5.

Bagheri, E., Ghorbani, A.A., 2008, 'The State of the Art in Critical Infrastructure Protection: A Framework for Convergence', *International Journal of Critical Infrastructures*, Vol. 4, No 3, https://doi.org/10.1504/IJCIS.2008.017438.

Bagheri, E., Ghorbani, A.A., 2010, 'UML-CI: A Reference Model for Profiling Critical Infrastructure Systems', *Information Systems Frontiers*, Vol. 12, pp. 115–139, https://doi.org/10.1007/s10796-008-9127-y.

Barabási, A.-L., 2002, Linked: The new science of networks, Perseus Books Group, New York.

Barthélemy, M., 2011, 'Spatial Networks', *Physics Reports*, Vol. 499, No 1–3, pp. 1-101 https://doi.org/10.1016/j.physrep.2010.11.002.

Beheshtian, A., Donaghy, K. P., Rouhani, O. M., Geddes, R., 2019, 'Adaptation Planning for Climate-Resilient Urban Infrastructures', *Transportation Planning and Technology*, Vol. 42, No 2, pp. 113-129, https://doi.org/10.1080/03081060.2019.1565160.

Chang, L., Dollevoet, R.P.B.J., Hanssen, R.F., 2017, 'Nationwide Railway Monitoring Using Satellite SAR Interferometry', *IEEE Journal of Selected Topics in Applied Earth Observations and Remote Sensing*, Vol. 10, No 2, pp. 596-604, https://doi.org/10.1109/JSTARS.2016.2584783.

Cimellaro, G. P., Villa, O., Bruneau, M., 2015, 'Resilience-Based Design of Natural Gas Distribution Networks', *Journal of Infrastructure Systems*, Vol. 21, No 1, https://doi.org/10.1061/(ASCE)IS.1943-555X.0000204.

Colizza, V., Barrat, A., Barthelemy, M., Vespignani, A., 2006, 'The Role of the Airline Transportation Network in the prediction and predictability of global epidemics, *PNAS*, Vol. 103, No 7, pp. 2015–2020, https://doi.org/10.1073/pnas.0510525103.

Colomina, I., Molina, P., 2014, 'Unmanned Aerial Systems for Photogrammetry and Remote Sensing: A Review', *ISPRS Journal of Photogrammetry and Remote Sensing*, Vol. 92, pp. 79-97, https://doi.org/10.1016/j.isprsjprs.2014.02.013.

Crucitti, P., Latora, V., Marchiori, M., Rapisarda, A., 2004, 'Error and Attack Tolerance of Complex Networks', In *Physica A: Statistical Mechanics and Its Applications*, Vol. 340, No 1–3, pp. 388-394, https://doi.org/10.1016/j.physa.2004.04.031.

Dai, K., Liu, G., Li, A., Ma, D., Wang, X., Zhang, B., Tang, J., Li, G., 2018, 'Monitoring Highway Stability in Permafrost Regions with X-Band Temporary Scatterers Stacking InSAR', *Sensors,* Vol. 18, No 6, pp. 1876, https://doi.org/10.3390/s18061876.

Duan, S., Lee, S., Chinthavali, S., Shankar, M., 2016, 'Reliable Communication Models in Interdependent Critical Infrastructure Networks', In *2016 Resilience Week (RWS)*, Chicago, IL, pp. 152-157, https://doi.org/10.1109/RWEEK.2016.7573324.

Duffé, P., Marec, M., Cialdini, P., 1999, *Rapport commun des missions administratives d'enquête technique française et italienne relatif à la catastrophe survenue le 24 mars 1999 dans le tunnel du Mont Blanc* (in French), 6 July.

Durante, M. G., Di Sarno, L., Zimmaro, P., Stewart, J.P., 2018, 'Damage to Roadway Infrastructure from 2016 Central Italy Earthquake Sequence', *Earthquake Spectra*, Vol. 34, No 4, pp. 1721, https://doi.org/10.1193/101317EQS205M.

ENTSO-E, 2017, *Managing Critical Grid Situations – Success & Challenges: ENTSO-E report of the January 2017 Cold Spell*, European Network of Transmission System Operators for Electricity, Brussels.

ENTSO-E, 2019a, *Statistical Factsheet 2018, Provisional values as of 5 June 2019*, European Network of Transmission System Operators for Electricity, Brussels.

ENTSO-E, 2019b, *PowerFacts Europe 2019*, European Network of Transmission System Operators for Electricity, Brussels.

ENTSO-E, 2019c, *Vision on Market Design and System Operation towards 2030*, European Network of Transmission System Operators for Electricity, Brussels.

Esposito, S., Stojadinović, B., Babič, A., Dolšek, M., Iqbal, S., Selva, J., Broccardo, M., Mignan, A., Giardini, D., 2020, 'Risk-Based Multilevel Methodology to Stress Test Critical Infrastructure Systems', *Journal of Infrastructure Systems*, Vol. 26, No 1, https://ascelibrary.org/doi/10.1061/%28ASCE%29IS.1943-555X.0000520.

EU, 2004, Directive 2004/54/EC of the European Parliament and of the Council of 29 April 2004 on minimum safety requirements for tunnels in the Trans-European Road Network, OJ L 167, 30.4.2004, p. 39–91.

EU, 2008, Directive 2008/96/EC of the European Parliament and of the Council of 19 November 2008 on road infrastructure safety management, OJ L 319, 29.11.2008, p. 59–67.

EU, 2008, Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, OJ L 345, 23.12.2008, pp. 75–82.

EU, 2017, Commission Regulation (EU) 2017/1485 of 2 August 2017 establishing a guideline on electricity transmission system operation, C/2017/5310, OJ L 220, 25.8.2017, p. 1–120.

European Commission, 2004, Communication from the Commission to the Council and the European Parliament. Critical Infrastructure Protection in the fight against terrorism, COM(2004) 702 final.

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

Eusgeld, I., Kröger, W., Sansavini, G., Schläpfer, M., Zio, E., 2009, 'The Role of Network Theory and Object-Oriented Modeling within a Framework for the Vulnerability Analysis of Critical Infrastructures', *Reliability Engineering and System Safety*, Vol. 94, No 5, pp. 954-963, https://doi.org/10.1016/j.ress.2008.10.011.

Ezell, B.C., Farr, J.V., Wiese, I., 2000, 'Infrastructure Risk Analysis Model', *Journal of Infrastructure Systems*, Vol. 6, No 3, https://doi.org/10.1061/(ASCE)1076-0342(2000)6:3(114).

FEMA, 2020, *Homeland Security Exercise and Evaluation Program*, https://www.fema.gov/emergency-managers/national-preparedness/exercises/hseep.

Florin, M.-V., Linkov, I., 2016, *IRGC resource guide on resilience*, EPFL International Risk Governance Center (IRGC), Lausanne, https://doi.org/10.5075/epfl-irgc-228206.

Gai, P., Kapadia, A., 2010, 'Contagion in Financial Networks', *Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences*, Vol. 466, No 2120, https://doi.org/10.1098/rspa.2009.0410.

Galbusera, L., Giannopoulos, G., 2017, 'Exploiting Web Ontologies for Automated Critical Infrastructure Data Retrieval', In Rice, M., Shenoi, S., (Eds.), *Critical Infrastructure Protection XI*, IFIP AICT 512, pp. 119–136, https://doi.org/10.1007/978-3-319-70395-4_7.

Galbusera, L., Giannopoulos, G., 2018, 'On Input-Output Economic Models in Disaster Impact Assessment', *International Journal of Disaster Risk Reduction*, Vol. 30, Part B, pp. 186-198, https://doi.org/10.1016/j.ijdrr.2018.04.030.

Galbusera, L., Giannopoulos, G., 2019, 'Leveraging Network Theory and Stress Tests to Assess Interdependencies in Critical Infrastructures', In Gritzalis, D., Theocharidou, M., Stergiopoulos, G. (Eds,) *Critical Infrastructure Security and Resilience*, Advanced Sciences and Technologies for Security Applications, Springer, Cham, pp.135-155, https://doi.org/10.1007/978-3-030-00024-0_8.

Galbusera, L., Giannopoulos, G., Argyroudis, S., Kakderi, K., 2018, 'A Boolean Networks Approach to Modeling and Resilience Analysis of Interdependent Critical Infrastructures', *Computer-Aided Civil and Infrastructure Engineering*, Vol. 33, No 12, pp. 1041-1055, https://doi.org/10.1111/mice.12371.

Galbusera, L., Giannopoulos, G., Ward, D., 2014, *Developing stress tests to improve the resilience of critical infrastructures: A feasibility analysis*, JRC Science and Policy Report EUR 26971 EN, Publications Office of the European Union, Luxembourg.

Ghasemieh, H., Remke, A., Haverkort, B.R., 2013, 'Survivability Evaluation of Fluid Critical Infrastructures Using Hybrid Petri Nets', paper presented at 2013 IEEE 19th Pacific Rim International Symposium on Dependable Computing, Vancouver, BC, 2013, pp. 152-161, https://doi.org/10.1109/PRDC.2013.34.

Glasserman, P., Young, H.P., 2015, 'How Likely Is Contagion in Financial Networks?' *Journal of Banking and Finance*, Vol. 50, pp. 383-399, https://doi.org/10.1016/j.jbankfin.2014.02.006.

Guimerà, R., Mossa, S., Turtschi, A., Amaral, L.A.N., 2005, 'The Worldwide Air Transportation Network: Anomalous Centrality, Community Structure, and Cities' Global Roles', *PNAS*, Vol. 102, No 22, pp. 7794-7799, https://doi.org/10.1073/pnas.0407994102.

Haimes, Y.Y., Kaplan, S., Lambert, J. H., 2002, 'Risk Filtering, Ranking, and Management Framework Using Hierarchical Holographic Modeling', *Risk Analysis*, Vol. 22, No 2, pp. 383-397, https://doi.org/10.1111/0272-4332.00020.

Hallegatte, S., Rentschler, J., Rozenberg, J., 2019, 'From Micro to Macro: Local Disruptions Translate into Macroeconomic Impacts', In Hallegatte, S., Rentschler, J., Rozenberg, J. (Eds.), *Lifelines: The Resilient Infrastructure Opportunity, Sustainable Infrastructur*e, World Bank, Washington, DC, https://doi.org/10.1596/978-1-4648-1430-3_ch5.

Ham, N., Lee, S.-H., 2018, 'Empirical Study on Structural Safety Diagnosis of Large-Scale Civil Infrastructure Using Laser Scanning and BIM', *Sustainability,* Vol. 10, No 11, pp. 4024, https://doi.org/10.3390/su10114024.

Helbing, D., 2013, 'Globally Networked Risks and How to Respond', *Nature*, Vol. 497, pp. 51–59 https://doi.org/10.1038/nature12047.

Huang, Q., Monserrat, O., Crosetto, M., Crippa, B., Wang, Y., Jiang, J., Ding, Y., 2018, 'Displacement Monitoring and Health Evaluation of Two Bridges Using Sentinel-1 SAR Images', *Remote Sensing*, Vol. 10, No 11, pp. 1714 https://doi.org/10.3390/rs10111714.

ICAO, 2004, *Manual on the Regulation of International Air Transport*, doc. 9626, International Civil Aviation Organization.

ICF, 2015, *Study on the implementation and effects of Directive 2004/54/EC on minimum safety requirements for road tunnels in the transEuropean road network,* Final Report, ICF Consulting Services in association with TRT Trasporti e Territorio, 17 June, https://ec.europa.eu/transport/sites/transport/files/tunnel_final_report.pdf.

ISO, 2018, ISO 31000: 2018 Risk Management — Guidelines.

Johansen, C., Tien, I., 2018, 'Probabilistic Multi-Scale Modeling of Interdependencies between Critical Infrastructure Systems for Resilience', *Sustainable and Resilient Infrastructure*, Vol.3, No 1, https://doi.org/10.1080/23789689.2017.1345253.

Khademi, N., Balaei, B., Shahri, M., Mirzaei, M., Sarrafi, B., Zahabiun, M., Mohaymany, A.S., 2015, 'Transportation Network Vulnerability Analysis for the Case of a Catastrophic Earthquake', *International Journal of Disaster Risk Reduction*, Vol.12, pp. 234-254, https://doi.org/10.1016/j.ijdrr.2015.01.009.

Koks, E. E., Rozenberg, J., Zorn, C. , Tariverdi, M., Vousdoukas, M., Fraser, S.A., Hall, J.W., Hallegatte, S., 2019, 'A Global Multi-Hazard Risk Analysis of Road and Railway Infrastructure Assets', *Nature Communications*, Vol. 10, Article no 2677, https://doi.org/10.1038/s41467-019-10442-3.

Krausmann, E., Mushtaq, F., 2010, 'Learning Lessons from Tunnel Accidents - Recommendations in Support of the Implementation of Article 15 on Reporting of the EU Directive 2004/54/EC', *Safety Science*, Vol. 48, No 2, pp. 230-237, https://doi.org/10.1016/j.ssci.2009.09.002.

Kröger, W., 2008, 'Critical Infrastructures at Risk: A Need for a New Conceptual Approach and Extended Analytical Tools', *Reliability Engineering and System Safety*, Vol. 93, No 12, pp. 1781-1787, https://doi.org/10.1016/j.ress.2008.03.005.

Kröger, W., 2017, 'Securing the Operation of Socially Critical Systems from an Engineering Perspective: New Challenges, Enhanced Tools and Novel Concepts', *European Journal for Security Research*, Vol. 2, pp. 39–55, https://doi.org/10.1007/s41125-017-0013-9.

Kröger, W., Zio, E., 2011. *Vulnerable Systems*, Springer, London, https://doi.org/10.1007/978-0-85729-655-9.

Kundur, P., Taylor, C.W., 2007, *Blackout Experiences and Lessons, Best Practices for System Dynamic Performance, and the Role of New Technologies*, IEEE Task Force Report, IEEE Power & Energy Society.

Lee, G.C., Mohan, S.B., Huang, C., Fard, B.N., 2013, *A Study of US Bridge Failures (1980–2012)*, MCEER Technical Report.

Lewis, A.M., Ward, D., Cyra, L., Kourti, N., 2013, 'European Reference Network for Critical Infrastructure Protection', *International Journal of Critical Infrastructure Protection*, Vol. 6, No 1, pp. 51-60, https://doi.org/10.1016/j.ijcip.2013.02.004.

Lin, J., Tai, K., Tiong, R.L.K., Sim, M.S., 2016, 'A General Framework for Critical Infrastructure Interdependencies Modeling Using Economic Input-Output Model and Network Analysis', In Cardin M.A., Fong S., Krob D., Lui P., Tan Y. (Eds.) *Complex Systems Design & Management Asia. Advances in Intelligent Systems and Computing*, vol 426. Springer, Cham, pp.59-74, https://doi.org/10.1007/978-3-319-29643-2_5.

Luzi, G., M. Crosetto, and M. Cuevas-González. 2014, 'A Radar-Based Monitoring of the Collserola Tower (Barcelona)', *Mechanical Systems and Signal Processing*, Vol. 49, No 1–2, pp. 234-248, https://doi.org/10.1016/j.ymssp.2014.04.019.

Masys, A. J. 2014. *Networks and Network Analysis for Defence and Security*, Springer International Publishing, Switzerland.

Milillo, P., Perissin, D., Salzer, J.T., Lundgren, P., Lacava, G., Milillo, G., Serio, C., 2016, 'Monitoring Dam Structural Health from Space: Insights from Novel InSAR Techniques and Multi-Parametric Modeling Applied to the Pertusillo Dam Basilicata, Italy', *International Journal of Applied Earth Observation and Geoinformation*, Vol. 52, pp. 221-229, https://doi.org/10.1016/j.jag.2016.06.013.

Monserrat, O., Crosetto, M., Luzi, G., 2014, 'A Review of Ground-Based SAR Interferometry for Deformation Measurement', *ISPRS Journal of Photogrammetry and Remote Sensing*, Vol. 93, pp. 40-48, https://doi.org/10.1016/j.isprsjprs.2014.04.001.

Monstadt, J., Schmidt, M., 2019, 'Urban Resilience in the Making? The Governance of Critical Infrastructures in German Cities', *Urban Studies*, Vol. 56, No 11, pp. 2353-2371, https://doi.org/10.1177/0042098018808483.

Newman, D.E., Nkei, B., Carreras, B.A., Dobson, I., Lynch, V.E., Gradney, P., 'Risk Assessment in Complex Interacting Infrastructure Systems', In Proceedings of the 38th Annual Hawaii International Conference on System Sciences, Big Island, HI, USA, 2005, pp. 63c-63c, https://doi.org/10.1109/HICSS.2005.524.

Ntzeremes, P., Kirytopoulos, K. 2019, 'Evaluating the Role of Risk Assessment for Road Tunnel Fire Safety: A Comparative Review within the EU', *Journal of Traffic and Transportation Engineering (English Edition)*, Vol. 6, No 3, pp. 282-296, https://doi.org/10.1016/j.jtte.2018.10.008.

O'Rourke, T., 2007, 'Critical Infrastructure, Interdependencies, and Resilience', *The Bridge*, Vol. 37, No 1, National Academy of Engineering.

OECD, 2018, *Climate-Resilient Infrastructure*, OECD Environment Policy Papers, no. 14, OECD Publishing, Paris, https://doi.org/10.1787/4fdf9eaf-en.

OECD, 2019. *Good Governance for Critical Infrastructure Resilience*, OECD Reviews of Risk Management Policies, OECD Publishing, Paris, https://doi.org/10.1787/02f0e5a0-en.

Ouyang, M., 2014, 'Review on Modeling and Simulation of Interdependent Critical Infrastructure Systems', *Reliability Engineering and System Safety*, Vol. 121, pp. 43-60 https://doi.org/10.1016/j.ress.2013.06.040.

Oxley, D., 2017, *Estimating the impact of recent terrorist attacks in Western Europe*, International Air Transport Association.

Pant, R., Thacker, S., Hall, J.W., Alderson, D., Barr, S., 2018, 'Critical Infrastructure Impact Assessment Due to Flood Exposure', *Journal of Flood Risk Management*, Vol. 11, No 1, pp. 22-33 https://doi.org/10.1111/jfr3.12288.

Pant, R., Thacker, S., Hall, J.W., Barr, S., Alderson, D., Kelly, S., 2016, 'Analysing the Risks of Failure of Interdependent Infrastructure Networks', In Hall, J.W., Tran, M., Hicjord, A.J., Nicholls, R.J. (Eds.) *The Future of National Infrastructure: A System-of-Systems Approach*, Cambridge University Press, pp. 241-267, https://doi.org/10.1017/CBO9781107588745.013.

Panzieri, S., Setola, R., Ulivi, G., 2005, 'An Approach to Model Complex Interdependent Infrastructures', *IFAC Proceedings Volumes*, Vol. 38, No 1, pp. 404-409, https://doi.org/10.3182/20050703-6-cz-1902.00068.

Peduto, D., Nicodemo, G., Maccabiani, J., Ferlisi, S., 2017, 'Multi-Scale Analysis of Settlement-Induced Building Damage Using Damage Surveys and DInSAR Data: A Case Study in The Netherlands', *Engineering Geology*, Vol. 218, pp. 117-133, https://doi.org/10.1016/j.enggeo.2016.12.018.

Pereyra, J., He, X., Mostafavi, A., 2016, 'Multi-Agent Framework for the Complex Adaptive Modeling of Interdependent Critical Infrastructure Systems', In *Proceedings of the 2016 Construction Research Congress*, San Juan, Puerto Rico, https://doi.org/10.1061/9780784479827.156.

Pieraccini, M., 2013, 'Monitoring of Civil Infrastructures by Interferometric Radar: A Review', *The Scientific World Journal*, Vol. 2013, article no 786961, https://doi.org/10.1155/2013/786961.

Pinnaka, S., Yarlagadda, R., Cetinkaya, E.K., 2015, 'Modelling Robustness of Critical Infrastructure Networks', presented at *2015 11th International Conference on the Design of Reliable Communication Networks, DRCN 2015*, Kansas City, MO, pp. 95-98, https://doi.org/10.1109/DRCN.2015.7148995.

Poljanšek, K., Casajus Valles, A., Marin Ferrer, M. (Eds.), 2019, *Recommendations for National Risk Assessment for Disaster Risk Management in EU*, EUR 29557 EN, Publications Office of the European Union, Luxembourg.

Rehak, D., Senovsky, P., Hromada, M., Lovecek, T., Novotny, P., 2018, 'Cascading Impact Assessment in a Critical Infrastructure System', *International Journal of Critical Infrastructure Protection*., Vol. 22, pp. 125-138, https://doi.org/10.1016/j.ijcip.2018.06.004.

Rinaldi, S.M., Peerenboom, J.P., Kelly, T.K., 2001, 'Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies', *IEEE Control Systems Magazine*, Vol. 21, no 6, pp. 11-25, https://doi.org/10.1109/37.969131.

Rodrigue, J.P., Comtois, C., Slack, B., 2016, *The Geography of Transport Systems*, Routledge, London, https://doi.org/10.4324/9781315618159.

Rozenberg, J., Alegre, X.E., Avner, P., Fox, C., Hallegatte, S., Koks, E., Rentschler, J., Tariverdi, M., 2019. *From A Rocky Road to Smooth Sailing*, Sector note for LIFELINES: The Resilient Infrastructure Opportunity, World Bank, Washington, DC, https://doi.org/10.1596/31913.

Satumtira, G., Dueñas-Osorio, L., 2010, 'Synthesis of Modeling and Simulation Methods on Critical Infrastructure Interdependencies Research', In Gopalakrishnan K., Peeta S. (Eds.) *Sustainable and Resilient Critical Infrastructure Systems*, Springer, Berlin, Heidelberg, pp. 1- 51, https://doi.org/10.1007/978-3-642-11405-2_1.

Schaberreiter, T., Bouvry, P., Röning, J., Khadraoui, D., 2013, 'A Bayesian Network Based Critical Infrastructure Risk Model', In Schütze O., Coello Coello, C.A., Tantar, A.A., Tantar, E., Bouvry, P., Del Moral, P., Legrand, P. (Eds.) *EVOLVE - A Bridge between Probability, Set Oriented Numerics, and Evolutionary Computation II*, Advances in Intelligent Systems and Computing, Vol. 175. Springer, Berlin, Heidelberg, pp. 207 – 218, https://doi.org/10.1007/978-3-642-31519-0.

Schrefler, L., Dinu, A., 2018, Road *infrastructure and tunnel safety, Briefing, Implementation Appraisal*, European Parliamentary Research Service, https://www.europarl.europa.eu/RegData/etudes/BRIE/2018/611028/EPRS_BRI(2018)611028_EN.pdf.

SESAR, 2019, *SESAR solutions catalogue 2019*, Third Edition, SESAR Joint Undertaking, Publications Office of the European Union, Luxembourg.

Solari, L., Barra, A., Herrera, G., Bianchini, S., Monserrat, O., Béjar-Pizarro, M., Crosetto, M., Sarro, R., Moretti, S., 2018, 'Fast Detection of Ground Motions on Vulnerable Elements Using Sentinel-1 InSAR Data', *Geomatics, Natural Hazards and Risk*, Vol. 9, No 1, pp.152-174, https://doi.org/10.1080/19475705.2017.1413013.

Sterbenz, J.P.G., Çetinkaya, E.K., Hameed, M.A, Jabbar, A., Qian, S., Rohrer, J. P., 2013, 'Evaluation of Network Resilience, Survivability, and Disruption Tolerance: Analysis, Topology Generation, Simulation, and Experimentation: Invited Paper', *Telecommunication Systems*, Vol. 52, pp. 705–736, https://doi.org/10.1007/s11235-011-9573-6.

Sullivan, A., 2019, 'German air traffic software glitch one of several problems afflicting sector', *Deutsche Welle*, 25 March, https://www.dw.com/en/german-air-traffic-software-glitch-one-of-several-problems-afflicting-sector/a-48053507.

Teza, G., Galgaro, A., Moro, F., 2009, 'Contactless Recognition of Concrete Surface Damage from Laser Scanning and Curvature Computation', *NDT and E International*, Vol. 42, No 4, pp. 240-249, https://doi.org/10.1016/j.ndteint.2008.10.009.

Thacker, S., Barr, S., Pant, R., Hall, J.W., Alderson, D., 2017, 'Geographic Hotspots of Critical National Infrastructure', *Risk Analysis*, Vol. 37, No 1, pp. 2490-2505, https://doi.org/10.1111/risa.12840.

Theocharidou, M., Galbusera, L., Giannopoulos, G., 2018, 'Resilience of Critical Infrastructure Systems: Policy, Research Projects and Tools', In Trump, B. D., Florin, M.-V., Linkov, I. (Eds.). *IRGC resource guide on resilience (vol. 2): Domains of resilience for complex interconnected systems*, EPFL International Risk Governance Center, Lausanne, CH.

Trump, B. D., Florin, M.-V., Linkov, I., *IRGC resource guide on resilience (vol. 2): Domains of resilience for complex interconnected systems*, EPFL International Risk Governance Center, Lausanne, CH, https://doi.org/10.5075/epfl-irgc-257279.

UCTE, 2004, *Final Report of the Investigation Committee on the28 September 2003 Blackout in Italy,* UCTE Report, Union for the co-ordination of transmission of electricity, Brussels.

UCTE, 2007, *Final Report System Disturbance on 4 November 2006,* UCTE Report, Union for the co-ordination of transmission of electricity, Brussels.

UNDRR, 2015, Sendai framework for action on disaster risk reduction 2015–2030, United Nations Office for Disaster Risk Reduction, https://www.unisdr.org/we/coordinate/sendai-framework.

Vespignani, A., 2009, 'Predicting the Behavior of Techno-Social Systems', *Science*, Vol. 325, No 5939, pp. 425-428, https://doi.org/10.1126/science.1171990.

Zhang, B., Ding, X. Werner, C., Tan, K., Zhang, B., Jiang, M., Zhao, J., Xu, Y., 2018, 'Dynamic Displacement Monitoring of Long-Span Bridges with a Microwave Radar Interferometer', *ISPRS Journal of Photogrammetry and Remote Sensing*, Vol. 138, pp. 252-264, https://doi.org/10.1016/j.isprsjprs.2018.02.020.

Zio, E.. 2016, 'Challenges in the Vulnerability and Risk Analysis of Critical Infrastructures', *Reliability Engineering and System Safety*, Vol. 152, pp. 137-150 https://doi.org/10.1016/j.ress.2016.02.009.

3.4.3 Core industrial and energy facilities

Airmic, 2011, *Roads to Ruin: A study of major risk events: their origins, impact and implications*, Airmic, UK, https://www.airmic.com/technical/library/roads-ruin-analysis.

Avižienis, A., Laprie, J.-C., Randell, B., 2000, 'Fundamental concepts of dependability', Computing Science, Technical report series, No CS-TR-739, University of Newcastle upon Tyne.

Bloomfeld, R., Chozos, N., Nobles, P., 2009, *Infrastructure Interdependency Analysis: Requirements, capabilities and strategy*, Adelard LLP, London.

Boin, A., McConnell, A., 2007, 'Preparing for critical infrastructure breakdowns: The limits of crisis management and the need for resilience', *Journal of Contingencies and Crisis Management*, Vol. 15, No 1, pp. 50–59.

BSEE, 2011, *Report regarding the causes of the 20 April 2010 Macondo well blowout*, Bureau of Safety and Environmental Enforcement, 14 September, https://www.bsee.gov/sites/bsee.gov/files/reports/safety/dwhfinal.pdf.

BP, 2015, *Gulf of Mexico Environmental Recovery and Restoration: Five year report*, March 2015, https://www.aph.gov.au/DocumentStore.ashx?id=33f4ea2f-fdd7-4246-ad51-485a814fa8f9&subId=412091.

CCPS, 2000, *Guidelines for chemical process quantitative risk analysis*, 2nd ed., Center for Chemical Process Safety, American Institute of Chemical Engineers, New York.

Chakraborty, A., Ibrahim, A., Cruz, A. M., 2018, 'A study of accident investigation methodologies applied to the Natech events during the 2011 Great East Japan earthquake', *Journal of Loss Prevention in the Process Industries*, Vol. 51, pp. 208–222.

Cox, T., 1998, 'Risk integration and decision-making', in: Kirchsteiger, C., Christou, M. D., Papadakis, G. A. (eds.), *Risk assessment and management in the context of the Seveso II Directive*, Industrial Safety Series, Vol. 6, Elsevier, Amsterdam, pp. 277-312.

Cozzani, V., Salzano, E., 2017, 'Quantitative methods for Natech risk assessment', in: Krausmann, E., Cruz, A. M., Salzano, E. (eds.), *Natech Risk Assessment and Management – Reducing the risk of natural-hazard impact on hazardous installations*, Elsevier, Amsterdam, pp. 143-156.

Cozzani, V., Krausmann, E., Reniers, G., 2013, 'Other causes of escalation', in: Reniers, G., Cozzani, V. (eds.), *Domino Effects in the Process Industries – Modeling, prevention and managing*, pp. 154-174, Elsevier, Waltham.

Cruz, A. M., Krausmann, E., 2008, 'Damage to offshore oil and gas facilities following Hurricanes Katrina and Rita: An overview', *Journal of Loss Prevention in the Process Industries*, Vol. 21, No 6, pp. 620-626.

Cruz, A. M., Okada, N., 2008, 'Methodology for preliminary assessment of Natech risk', *Natural Hazards*, Vol. 46, No 2, pp. 199–220.

Cyprus, Ministry of Defence, 2013, 'Ο Υπουργός Άμυνας προήδρευσε Υπουργικής Επιτροπής για το Βασικό Εθνικό Σχέδιο "Ζήνων"', http://www.mod.gov.cy/mod/mod.nsf/All/2F672ABF214D259EC2257D9E002A91C8?OpenDocument.

Cyprus, Ministry of the Interior, 2016, 'Γνωστοποίηση Δύναμης Πολιτικής Άμυνας προς το Κοινό για την Εκπόνηση και Αναθεώρηση των Εξωτερικών Σχεδίων Επείγουσας Ανάγκης', http://www.moi.gov.cy/moi/CD/cd.nsf/All/5E42176FB5C653DCC22580370041FA58?OpenDocument.

De Almeida, A., Cavalcante, C., Alencar, M. H., Ferreira, R. J., de Almeida-filho, A., Garcez, T. V., 2015, *Multicriteria and multiobjective models for risk, reliability and maintenance decision analysis*, 1st ed., Springer, New York.

DNV GL, 2015, *Summary of Macondo Inquiries*, 30 April, http://app.e.dnvgl.com/e/er?s=861531437&lid=498.

Electricity Authority of Cyprus, 2018, *Εγχειρίδιο Πολιτικής Πρόληψης Ατυχημάτων Μεγάλης Κλίμακας*, https://www.eac.com.cy/EL/EAC/

Operations/Documents/%CE%95%CE%A0%CE%A0%CE%91%CE%9C%CE%9A_SEVESO-III_signed.pdf.

eNATECH, 2018, 'Natech information', https://enatech.jrc.ec.europa.eu/Natech/6.

EU, 1997, Council Directive 96/82/EC of 9 December 1996 on the control of major-accident hazards involving dangerous substances, OJ L 10, 14.1.1997, p. 13-33.

EU, 2008, Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, OJ L 345, 23.12.2008, p. 75–82.

EU, 2012, Directive of the European Parliament and of the Council of 4 July 2012 on the control of major-accident hazards involving dangerous substances, amending and subsequently repealing Council Directive 96/82/EC, OJ L 197, 24.7.2012, p. 38–71.

EU, 2013, Directive 2013/30/EU of the European Parliament and of the Council of 12 June 2013 on safety of offshore oil and gas operations and amending Directive 2004/35/EC, OJ L 178, 28.6.2013, p. 66–106.

EU, 2017, Regulation (EU) 2017/1938 of the European Parliament and of the Council of 25 October 2017 concerning measures to safeguard the security of gas supply and repealing Regulation (EU) No 994/2010, OJ L 280, 28.10.2017, p. 1–56.

European Commission, 2011, Commission staff working paper – Impact assessment accompanying the document Proposal for the Regulation of the European Parliament and of the Council on safety of offshore oil and gas prospection, exploration and production activities, SEC(2011), 1293 final.

Evripidou, S., 2011, '"Criminal errors" in navy base blast', *Cyprus Mail*, 12 July, https://cordelia.typepad.com/anastasia/2011/07/criminal-errors-in-cyprus-navy-base-blast.html.

Florin, N., Ristea, M., Cotorcea, A., Atodiresei, D., 2016, 'Human reliability using the fault tree analysis: A case study of a military accident investigation', in *Proc.: 21st International Conference - The Knowledge-Based Organization*, Sibiu, Romania, 11-13 June 2015, pp. 215–219, De Gruyter Open.

Gautam, K. P., van der Hoek, E. E., 2003, 'Literature study on environmental impact of floods', Delft Cluster-publication DC1-233-13, Delft, The Netherlands, https://repository.tudelft.nl/islandora/object/uuid:4080519e-a46d-4e96-8524-62ee8fd93712/datastream/OBJ.

Gill, J., 2016, 'Disaster prosecution is, well, a disaster', *New Orleans Advocate*, 12 March, https://www.nola.com/opinions/james_gill/article_0e57b06a-9de1-5e96-b780-dd6af02c1028.html.

Gill, D. A., Ritchie, L. A., 2018, 'Contributions of technological and Natech disaster research to the social science disaster paradigm', in: Rodríguez, H., Donner, W., Trainor, J.E. (eds.), *Handbook of Disaster Research*, 2nd Ed., pp. 39-60, Springer, Cham.

Girgin, S., Necci, A., Krausmann, E., 2017, 'Natech hazard and risk assessment', in: *Words into Action Guidelines: National disaster risk assessment – governance system, methodologies, and use of results*, United Nations Office for Disaster Risk Reduction (UNISDR), Geneva.

Girgin, S., Necci, A., Krausmann, E., 2019, 'Dealing with cascading multi-hazard risks in National Risk Assessment: The case of Natech accidents', *International Journal of Disaster Risk Reduction*, Vol. 35, 101072.

Graham, B., Kreilly, W. K., Beinecke, F., Boesch, D. F., Garcia, T. D., Murray, C. A., Ulmer, F., 2011, *Deep Water – The Gulf oil disaster and the future of offshore drilling: report to the President*, National Commission on the BP Deepwater Horizon Oil Spill and Offshore Drilling.

Gyenes, Z., Heraty Wood, M., 2018, 'Lessons learnt from major accidents relating to emergency response', in: *Towards an all-hazards approach to emergency preparedness and response: Lessons learnt from non-nuclear events*, Nuclear Energy Agency, Organisation for Economic Co-operation and Development, Paris, pp. 25-44.

Hajipapas, A., Hope, K., 2011, 'Protests follow Cyprus navy fire deaths', *Financial Times*, 12 July, https://www.ft.com/content/02df9b86-aca9-11e0-a2f3-00144feabdc0.

Heraty Wood, M., Fabbri, L., 2019, 'Challenges and opportunities for assessing global progress in reducing chemical accident risks', *Progress in Disaster Science*, Vol. 4, 100044.

Hudec, P., Lucš, O., 2004, 'Flood at SPOLANA a.s. in August 2002', *Loss Prevention Bulletin*, Vol. 180, pp. 36–39.

IRGC, 2020, 'What is risk governance?', International Risk Governance Council, https://irgc.org/risk-governance/what-is-risk-governance/.

Kamil, M. Z., Taleb-Berrouane, M., Khan, F., Ahmed, S., 2019, 'Dynamic domino effect risk assessment using petri-nets', *Process Safety and Environmental Protection*, Vol. 124, pp. 308–316.

Khakzad, N., 2015, 'Application of dynamic Bayesian network to risk analysis of domino effects in chemical infrastructures', *Reliability Engineering & System Safety*, Vol. 138, pp. 263–272.

Krausmann, E., 2017, 'Natech risk and its assessment', in: Krausmann, E., Cruz, A. M., Salzano, E. (eds.), *Natech Risk Assessment and Management – Reducing the risk of natural-hazard impact on hazardous installations*, Elsevier, Amsterdam, pp. 105-118.

Krausmann, E., Cruz, A. M., Salzano, E., 2017a, *Natech Risk Assessment and Management – Reducing the risk of natural-hazard impact on hazardous installations*, Elsevier, Amsterdam.

Krausmann, E., Köppke, K.-E., Fendler, R., Cruz, A. M., Girgin, S., 2017b, 'Qualitative and semi-quantitative methods for Natech risk assessment', in: Krausmann, E., Cruz, A. M., Salzano, E. (eds.), *Natech Risk Assessment and Management – Reducing the risk of natural-hazard impact on hazardous installations*, Elsevier, Amsterdam, pp. 119-142.

Krausmann, E., Girgin, S., Necci, A., (2019), 'Natural hazard impacts on industry and critical infrastructure: Natech risk drivers and risk management performance indicators', *International Journal of Disaster Risk Reduction*, Vol. 40, 101163.

Küfeoğlu, S., 2015, 'Economic impacts of electric power outages and evaluation of customer interruption costs', doctoral dissertation, Aalto University, Finland.

Laprie, J.-C., 2008, 'From dependability to resilience', http://2008.dsn.org/fastabs/dsn08fastabs_laprie.pdf.

Lohr, S., 2011, 'Stress test for the global supply chain', *New York Times*, 19 March, http://archive.nytimes.com/www.nytimes.com/2011/03/20/business/20supply.html.

Luijf, E., Klaver, M., 2009, 'Insufficient situational awareness about critical infrastructures by emergency management', in: Proc. Symp. C3I for Crisis, Emergency and Consequence Management, Bucharest, Romania, 11–12 May, Paper MP-IST-086-10, pp. 10-1–10-10.

MIIB, 2008, *The Buncefield Incident 11 December 2005 – The final report of the Major Incident Investigation Board*, Vol. 1,

ftp://transp.cheng.auth.gr/Risk%20Analysis%20Reports/2005%20Buncefield%20report.pdf

Moore, L., Murray, S., Vaughan, J., 2013, 'Agreement reached on EU offshore oil & gas safety legislation', *Lexology*, 6 March, https://www.lexology.com/library/detail.aspx?g=72177ddd-3252-4c89-a032-41cc6e10be1c.

NASEM, 2018, *Designing Safety Regulations for High-Hazard Industries*, National Academies of Sciences, Engineering, and Medicine, Washington, DC, The National Academies Press, USA.

Nafday, A. M., 2009, 'Strategies for managing the consequences of black swans', *Leadership and Management in Engineering*, Vol. 9, No 4, pp. 191–197.

NEA, 2018, *Towards an all-hazards approach to emergency preparedness and response: Lessons learnt from non-nuclear events*, Nuclear Energy Agency, Organisation for Economic Co-operation and Development, Paris.

Necci, A., Cozzani, V., Spadoni, G., Khan, F., 2015, 'Assessment of domino effect: State of the art and research needs', *Reliability Engineering & System Safety*, Vol. 143, pp. 3–18.

NOAA, 2010, 'BP oil spill: NOAA modifies commercial and recreational fishing closure in the oil-affected portions of the Gulf of Mexico', Southeast Fishery Bulletin, FB10-055, National Marine Fisheries Service, 21 June.

OECD, 2003, 'OECD guiding principles for chemical accident prevention, preparedness and response', 2nd ed., *Series on Chemical Accidents*, No 10, Organisation for Economic Co-operation and Development, Paris.

OECD, 2012, *Global Modelling of Natural Hazard Risks: Enhancing existing capabilities to address new challenges*, OECD Global Science Forum, Organisation for Economic Co-operation and Development, n.p.

OECD, 2014, *Regulatory Enforcement and Inspections*, OECD Best Practice Principles for Regulatory Policy, Organisation for Economic Co-operation and Development, Paris.

OECD, 2015, 'Addendum Number 2 to the OECD Guiding principles for chemical accident prevention, preparedness and response (2nd ed.) to address natural hazards triggering technological accidents (Natechs)', *Series on Chemical Accidents*, No 27, Organisation for Economic Co-operation and Development, Paris.

Oltermann, P., 2017, 'Italy declares state of emergency after deadly gas explosion in Austria', *The Guardian*, 12 December, https://www.theguardian.com/world/2017/dec/12/italy-declares-state-emergency-gas-explosion-austria.

Pallardy, R., 2018, 'Deepwater Horizon oil spill', *Encyclopædia Britannica*, available at https://www.britannica.com/event/Deepwater-Horizon-oil-spill.

Pan, E., 2005, 'Katrina and oil prices', Council on Foreign Relations, 7 September, https://www.cfr.org/interview/katrina-and-oil-prices.

Petit, F., Verner, D., Brannegan, D., Buehring, W., Dickinson, D., Guziel, K., Haffenden, R., Philips, J., Peerenboom, J., 2015, *Analysis of Critical Infrastructure Dependencies and Interdependencies*, Risk and Infrastructure Science Centre, Argonne National Laboratory, Argonne, IL.

Polyviou, P., 2011, *Πόρισμα μονομελούς ερευνητικής επιτροπής για τη διεξαγωγή έρευνας σχετικά με την έκρηξη που επισυνέβη την 11η Ιουλίου 2011 στη Ναυτική Βάση 'Ευάγγελος Φλωράκης' στο Μαρί*, https://web.archive.org/web/20111005090635/http:/media.cna.org.cy/pdf/PORISMA.pdf.

Reliefweb, 2002, 'Czech chemical firm criticised after flood-related spill', 21 August, https://reliefweb.int/report/czech-republic/czech-chemical-firm-criticised-after-flood-related-spill.

Reniers, G., Cozzani, V. (eds.), 2013, *Domino Effects in the Process Industries – Modeling, prevention and managing*, Elsevier, Waltham.

Rinaldi, S., Peerenboom, J., Kelly, T., 2001, 'Identifying, understanding, and analyzing critical infrastructure interdependencies', *IEEE Control Systems Magazine*, Vol. 21, No 6, pp. 11–25.

Sengupta, A., Bandyopadhyay, D., van Westen, C. J., van der Veen, A., 2016, 'An evaluation of risk assessment framework for industrial accidents in India', *Journal of Loss Prevention in the Process Industries*, Vol. 41, pp. 295–302.

Snow, N., 2010, 'Deepwater drilling moratorium may temporarily cost 8,000–12,000 jobs, Senate panel told', *Oil and Gas Journal*, Vol. 108, No 36, pp. 17–18, http://www-az-ori.pennwell.com/content/ogj/en/articles/print/volume-108/issue-36/general-interest/deepwater-drilling-moratorium-may-temporarily-cost.html.

Suarez-Paba, M. C., Tzioutzios, D., Cruz, A. M., Krausmann, E., 2020, 'Toward Natech resilient societies', in: Yokomatsu, M., Scawthorn, C., Hochrainer-Stigler, S. (eds.), *Disaster Risk Reduction and Resilience*, Springer, Singapore, pp. 45-64.

Tharp, P., 2010, 'Stormy weather: BP's stock hits new low', *New York Post*, 26 June, https://nypost.com/2010/06/26/stormy-weather-bps-stock-hits-new-low/.

Tomic, B., Kulig, M., Strupczewski, A., Vigne, S., Hilden, W., 2008, 'Cross-cutting comparison of regulation and operation of industries requiring specific safety rules: Workshop summary', EUR 23203 EN, European Commission, Luxemburg.

Uijt de Haag, P. A. M., Ale, B. J. M., 1999, *Guidelines for Quantitative Risk Assessment (Purple Book)*, CPR 18E, Committee for the Prevention of Disasters, The Hague.

UNECE, 1998, Convention on access to information, public participation in decision-making and access to justice in environmental matters, https://www.unece.org/fileadmin/DAM/env/pp/documents/cep43e.pdf.

UNECE, 2015, Convention on the transboundary effects of industrial accidents, https://www.unece.org/fileadmin/DAM/env/documents/2017/TEIA/Publication/ENG_ECE_CP_TEIA_33_final_Convention_publication_March_2017.pdf.

Vaughan, A., 2018, 'BP's Deepwater Horizon bill tops $65bn', *The Guardian*, 16 January, https://www.theguardian.com/business/2018/jan/16/bps-deepwater-horizon-bill-tops-65bn.

Weber, H. R., 2010, 'Time to scrap BP brand? Gas station owners divided', *Associated Press*, 30 July, http://www.nbcnews.com/id/38493212/ns/business-us_business/.

3.4.4 Communication systems

Accenture and Ponemon Institute, 2017, The cost of cybercrime study. Insights on the security investments that make a difference, https://www.accenture.com/t20170926T072837Z_w_/us-en/_acnmedia/PDF-61/Accenture-2017-CostCyberCrimeStudy.pdf.

Accenture and Ponemon Institute, 2019, The cost of cybercrime, Ninth annual cost of cybercrime study, https://www.accenture.com/_

acnmedia/pdf-96/accenture-2019-cost-of-cybercrime-study-final.pdf.

BBC, 2017, 'Manchester attack: What we know so far', https://www.bbc.com/news/uk-england-manchester-40008389.

Becker, G. S., 1965, 'A theory of the allocation of time', *The Economic Journal*, Vol. 75, No 299, pp. 493–517.

Blackman, C., Forge, S., 2019, 5G Deployment: State of Play in Europe, USA and Asia, Study for the Committee on Industry, Research and Energy, Policy Department for Economic, Scientific and Quality of Life Policies, European Parliament, Luxembourg, https://www.europarl.europa.eu/RegData/etudes/IDAN/2019/631060/IPOL_IDA(2019)631060_EN.pdf

BroadWay, 2019, 'Project BroadWay: Pre-commercial procurement of a pan-European broadband mobile system for PPDR', www.broadway-info.eu.

Centolella, P., McGranahan, M., 2013, 'Understanding the value of uninterrupted service', *Proceedings of the CIGRE 2013 Grid of the Future Symposium,* Boston, Massachusetts, October 21.

Chaffey, D., 2018, 'Global social media research summary 2018', Smart Insights, https://www.smartinsights.com/social-media-marketing/social-media-strategy/new-global-social-media-research/.

Commission of the European Communities, 2006, Communication from the Commission on a European Programme for Critical Infrastructure Protection, COM(2006) 786 final, https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2006:0786:FIN:EN:PDF.

Copernicus, 2015, Carlisle - UNITED KINGDOM, Flood - Situation as of 07/12/2015, Delineation Map, https://emergency.copernicus.eu/mapping/ems-product-component/EMSR147_01CARLISLE_DELINEATION_OVERVIEW/1

Cumbria County Council, 2015, *Flooding in Cumbria – December 2015: Impact Assessment,* https://cumbria.gov.uk/elibrary/Content/Internet/536/671/4674/17217/17225/43312152830.PDF

De Nooij, M., Koopmans, C., Bijvoet, C., 2007, 'The value of supply security: The costs of power interruptions: Economic input for damage reduction and investment in networks', *Energy Economics*, Vol. 29, No 2, pp. 277–295.

Davies, K. L., Glanfield, E., 2015, 'The devastation from above: Aerial photographs show widespread flooding across Cumbria caused by Storm Desmond as residents tell of despair after £48 million flood defences fail to do their job', *Daily Mail*, 6 December, https://www.dailymail.co.uk/news/article-3348001/Storm-Desmond-wreaks-flood-havoc-Cumbria-Scotland-1-000-homeless-60-000-properties-without-power-50-severe-flood-warnings-force.html.

ENISA, 2014, *Technical Guideline on Incident Reporting, Technical guidance on the incident reporting in Article 13a*, ENISA, Greece, https://resilience.enisa.europa.eu/article-13/guideline-for-incident-reporting/Article_13a_ENISA_Technical_Guideline_On_Incident_Reporting_v2_1.pdf.

ENISA, 2018, 'ENISA Annual Privacy Forum 2018: shaping technology around data protection and privacy requirements', https://www.enisa.europa.eu/news/enisa-news/enisa-annual-privacy-forum-2018-shaping-technology-around-data-protection-and-privacy-requirements.

ENISA, n.d., Cybersecurity Incident Report and Analysis System – Visual Analysis Tool, https://www.enisa.europa.eu/topics/incident-reporting/cybersecurity-incident-report-and-analysis-system-visual-analysis/visual-tool

Environment Agency, 2018, *Estimating the economic costs of the 2015 to 2016 winter floods*, Environment Agency, Bristol, United Kingdom, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/672087/Estimating_the_economic_costs_of_the_winter_floods_2015_to_2016.pdf

Europatr, 2019, 'Telecom rules', https://ec.europa.eu/digital-single-market/en/news/qa-commission-launches-360deg-review-telecoms-rules-and-seeks-views-about-future-needs-internet

EU, 2008, Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, OJ L 345, 23.12.2008, p. 75–82.

EU, 2009, Directive 2009/140/EC of the European Parliament and of the Council of 25 November 2009 amending Directives 2002/21/EC on a common regulatory framework for electronic communications networks and services, 2002/19/EC on access to, and interconnection of, electronic communications networks and associated facilities, and 2002/20/EC on the authorisation of electronic communications networks and services (Text with EEA relevance), OJ L 337, 18.12.2009, p.37.

EU, 2019, Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (Text with EEA relevance), OJ L 151, 7.6.2019, p. 15–69.

Europol, 2018, *Internet Organised Crime Threat Assessment 2018*, Europol, https://www.europol.europa.eu/internet-organised-crime-threat-assessment-2018.

Grünewald and Torriti, 2012, 'Demand response: A different form of distributed storage?', in: *2012 International Conference on Smart Grid Technology, Economics and Policies (SG-TEP)*, IEEE, pp. 1–5.

GSMA, 2019, *The Mobile Economy Global*, GSMA, https://www.gsma.com/mobileeconomy/wp-content/uploads/2018/02/The-Mobile-Economy-Global-2018.pdf.

Halat, M., Clotet, X., Gaitan, V., Zafeiropoulos, I.., 2015, Social impact of failures in E & TC infrastructures, RAIN Project, Deliverable 4.3, http://rain-project.eu/wp-content/uploads/2015/12/D4-3-Social-Impact-of-ETC-infrastructures.pdf

Kerslake, L., Deeming, H., Goodwin, A., Lund, K., Wahlström, M., 2018, *The Kerslake Report: An independent review into the preparedness for, and emergency response to, the Manchester Arena attack on 22nd May 2017*, https://www.jesip.org.uk/uploads/media/Documents%20Products/Kerslake_Report_Manchester_Are.pdf

Linares, P., Rey, L., 2013, 'The costs of electricity interruptions in Spain: Are we sending the right signals?', *Energy Policy*, Vol. 61, pp. 751–760.

Mehrabian, A., 1971, *Silent Messages*, 1st ed., Wadsworth, Belmont, CA.

NCSC, 2019, 'NCSC advice following WhatsApp vulnerability', https://www.ncsc.gov.uk/guidance/whatsapp-vulnerability.

Tweed, K., 2013, 'Why cellular towers in developing nations are making the move to solar power', Scientific American, https://www.scientificamerican.com/article/cellular-towers-moving-to-solar-power/.

UNISDR, 2017, *Technical Guidance for Monitoring and Reporting on Progress in Achieving the Global Targets of the Sendai Framework for Disaster Risk Reduction*, https://www.unisdr.org/files/54970_techguidancefdigitalhr.pdf

Walker, A., Cox, E., Loughhead, J., Roberts, J., 2014, *Counting the Cost: The economic and social costs of electricity shortfalls in the UK*, Royal Academy of Engineering, London.

Conclusions

EU, 2008, Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, OJ L 345, 23.12.2008, pp. 75–82, https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:EN:PDF

EU, 2013, Decision No 1313/2013/EU of the European Parliament and of the Council of 17 December 2013 on a Union Civil Protection Mechanism (Text with EEA relevance), OJL 347, 20.12.2013, pp. 924–947, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32013D1313&from=EN.

EU, 2016, Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, OJ L 194, 19.7.2016, pp. 1–30, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN.