Nat Hazards
DOI 10.1007/s11069-016-2186-3

ORIGINAL PAPER

Critical infrastructure, panarchies and the vulnerability paths of cascading disasters

Gianluca Pescaroli[1] · **David Alexander**[1]

Received: 30 September 2015 / Accepted: 23 January 2016

Abstract Cascading effects and cascading disasters are emerging fields of scientific research. The widespread diffusion of functional networks increases the complexity of interdependent systems and their vulnerability to large-scale disruptions. Although in recent years studies of interconnections and chain effects have improved significantly, cascading phenomena are often associated with the "toppling domino metaphor", or with high-impact, low-probability events. This paper aimed to support a paradigm shift in the state of the art by proposing a new theoretical approach to cascading events in terms of their root causes and lack of predictability. By means of interdisciplinary theory building, we demonstrate how cascades reflect the ways in which panarchies collapse. We suggest that the vulnerability of critical infrastructure may orientate the progress of events in relation to society's feedback loops, rather than merely being an effect of natural triggers. Our conclusions point to a paradigm shift in the preparedness phase that could include escalation points and social nodes, but that also reveals a brand new field of research for disaster scholars.

Keywords Cascading disasters · Cascading events · Critical infrastructure · Panarchy · Interdependency · Vulnerability

1 Introduction

Over the last two decades, the disruption of critical infrastructure (CI) has determined a progressive change in attitudes to preparedness and emergency management. Until the early 2000s, the security of assets such as power plants, water supplies and communications was taken for granted, and the systems were optimised for efficiency and low-cost

✉ Gianluca Pescaroli
gianluca.pescaroli.14@ucl.ac.uk

[1] Institute for Risk and Disaster Reduction, University College London, London, UK

Published online: 12 February 2016

operation, rather than to be resilient (Lewis 2006). Episodes such as the 11 September 2001 terrorist attacks, the 2004 Indian Ocean tsunami, the 2005 London bombings and Hurricane Katrina in 2005 encouraged the implementation of security strategies to protect critical infrastructure (NATO 2007). However, a new kind of threat emerged that required other steps. Events such as the eruption of Eyjafjallajökull volcano (2010), the Tōhoku earthquake and tsunami (2011), and Hurricane Sandy in 2013 persuaded the world community to consider "cascading" disasters and their effects upon a globally networked society. According to Pescaroli and Alexander (2015), this kind of phenomenon is distinguished by its high level of complexity and the presence of nonlinear paths that lead towards secondary events (Fig. 1).

In many cases, the overall impact of a crisis is caused by failure or disruption of critical infrastructure, as happened in the Fukushima nuclear accident, the paralysis of European aviation associated with Eyjafjallajökull, and the energy distribution crisis triggered by Superstorm Sandy. In each case, interconnected and interdependent pathways were generated along which crises propagated and, in doing so, cascades of effects were created (Helbing 2013). Clearly, the scales are different for each of these examples, and so is their global reach. Superstorm Sandy had a massive effect, but a regional one; Eyjafjallajökull affected Europe, an entire continent, with outlying effects in the form of passengers stranded outside Europe; and the earthquake, tsunami and Fukushima nuclear release led to consequences that were spread over all the countries and continents with which Japanese industry interacts. At the largest scale so far, floods in Thailand in 2010 led to a worldwide shortage of computer components (Chongvilaivan 2012).

In particular, critical infrastructures can be seen as central elements in a widespread network of risk, because, for the most part, they have physical attributes as well as functional and organisational ones (Alexander 2013b). They can be associated with widespread breakdowns, which may cause great harm and may become full-blown transboundary catastrophes (Boin and Mc Connell 2007; Ansell et al. 2010). In other words, it is evident that modern technology is being integrated into complex socio-technological networks that increase the impact of local events upon broader crises

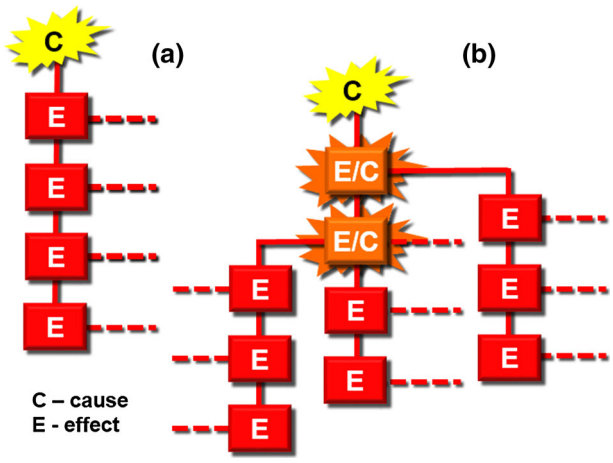

Fig. 1 Visual representation of cascading disasters (Pescaroli and Alexander 2015): **a** linear path of events in disasters and **b** nonlinear path of cascading, including amplification and subsidiary events

(Egan 2007). In strategic sectors such as energy, telecommunication and transportation, a development in one part of an infrastructure network can rapidly create much broader effects by cascading throughout the network and possibly spilling over into other networks (Amin 2002: 67). In the present day, there is a broadening societal consensus on the need to maintain critical infrastructure (Comes and Van de Walle 2014). Governments have begun to understand that relations among elements of infrastructure are key challenges (Van Eeten et al. 2011), and this is reflected in the mobilisation, in the European Commission's (EC's) Seventh Framework (FP7) and Horizon 2020 programmes, of funds for research on this issue. However, only a few authors have provided a comprehensive overview of the critical infrastructure landscape and its associated risk patterns in terms of cascading disaster (McGee et al. 2014).

In the context of this research, cascades can be defined as sequences of events governed by cause–effect relationships. As coincidence plays a significant, although rather unpredictable, role in crises (Stallings 2006), the first task in evaluating a cascading disaster is to ascertain the degree of causality between the elements of the sequence. Disasters are rare because it is unusual that the independent accumulation of vulnerabilities at different scales suddenly connects. However, when this occurs, the presence of a line of causality between diverse incidents and their impacts denotes a cascade. Such is the complexity and level of independence in modern life that cascading disasters become ever more likely.

Many studies of cascading crises and disasters refer to the "toppling domino metaphor", which is visualized in Fig. 1, path (a). The usual interpretation of this is that an initial event sets of a chain of eventualities that, at some point, includes the "top event", or most disastrous consequence (Khan and Abbasi 2000; Kadri et al. 2014). The principal assumption in this model is that there is a chain of weakness in which a linear sequence of events proceeds with unidirectional causality, and all eventualities or incidents are effects and the triggering event is the primary cause. Most critical infrastructure is too complex for this model to function adequately. In the rest of this paper, we will endeavour to explain why that is so and show how the "toppling domino" metaphor is inadequate for complex, intersecting systems in which there are high degrees of mutual interdependency.

The purpose of this article is to investigate how the progress of a cascading disaster can be guided by the vulnerability of critical infrastructure, rather than being merely an artefact of high-impact, low-probability and unexpected events. In other words, our goal is to contribute to a process of theory building that may help identify complex paths of disruption and the amplification of crises, not only in terms of *functional dependencies and interdependencies*, but also with respect to *root causes*—and *unpredictability*. The methodology of analysis that we propose below is adaptable to different geographical scales and global reaches and hence takes account of the variation in spatial extent of cascading disasters. In order to establish the scope of the concept and explain how it is used, we start by investigating the current state of knowledge about cascading failures of critical infrastructure. Secondly, we describe some of the interconnections and interdependencies that are likely to lead to the spread of cascades. Lastly, we explain how vulnerability can determine the path of the cascade and we develop an interdisciplinary, multi-level theory designed to characterise such phenomena. This will show how a systematic, holistic approach is needed in order to contain cascades effectively. We believe it will also help to set the agenda for future research.

2 Definition of critical facilities and infrastructure in society

There are many definitions of critical infrastructure in the scholarly literature. At the broadest level, it involves elements that are vital to the operation of society (Alexander 2013b). It consists of "complex networks, geographically dispersed, nonlinear, and interacting among themselves and with their human owners, operators, and users" (Amin 2002: 67). Besides its purely technical elements, critical infrastructure evolves as *processes* in which elements such as nature, culture, society, technology and politics interact dynamically (Graham 2010). It can be subjected to the direct and indirect effects of extreme events. The direct effects may involve damage to strategic buildings such as power plants, and the indirect effects can involve, for example, interruption of services or loss of capability. It could be argued that critical infrastructure is a "generator of vulnerabilities", whose locations and dependencies can propagate risk across geographical spaces (D'Ercole and Metzger 2009). According to Bouchon (2006), it can be analysed as a geographical system that is the product of context (e.g. legislation), planning and management (e.g. material infrastructure), ownership (the logic of development), geographical constraints (e.g. accessibility) and local background (e.g. environment and political culture).

NATO (2007) observed that in most countries definitions of critical infrastructure have evolved over the years in response to differences in national priorities. OECD (2008) offered a comparison between the definitions used by Australia, Canada, Germany, the Netherlands, the UK and the USA. Commonly, they associated the word "critical" with the "infrastructures that are essential to economic and social well-being, public safety and key governmental functions" (OECD 2008: 3). A broader meaning has been acquired by "infrastructure", which may include intangible assets such as supply chains and emergency services. In the Directive on European Critical Infrastructures (EC 2008), the European Commission defined the components of 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. (EC 2008: 3).

What emerges is something that associates physical disruption with the loss of functional assets in society. Moreover, official documentation provides an idea of "European critical infrastructure" (ECI) associated with those elements whose disruption engenders consequences in more than two member states, as a visible result of cross-sector and cross-border dependencies (EC 2008). A different approach is reported by the Parliamentary Assembly of NATO (2007). Here, the focus is on the new dimension acquired by critical infrastructure protection (CIP) after the terrorist attacks of 11 September 2001 in the USA, the attacks on public transportation in London (2005) and Madrid (2004) and the massive consequences of Hurricane Katrina (2005) in the southern USA and the Indian Ocean tsunami of 2004. In other words, together with the impact of political decisions associated, for example, with fluctuations in the energy sector, it is recognised that critical infrastructure is sensitive to particular threats, such as disasters or social disorder. This is usually taken into account in security strategies, risk assessments and risk-mitigation measures (NATO 2007; OECD 2008; EC 2008).

2.1 Differences and similarities between the notions of critical infrastructure and critical facilities

Together with the concept of "critical infrastructure", the literature often makes use of the term "critical facilities". These draw attention to the social and organisation context, rather than focussing on the technical assets alone, but the different use could be related more to institutional praxis than to anything of substance. Indeed, "critical facilities" seem to be associated with the sectors disaster risk reduction and emergency management more than with policy and security studies, for which "critical infrastructure" is the more common epithet. In particular, the Glossary of the United Nations International Strategy on Disaster Reduction (UNISDR 2009) does not include the term "critical infrastructure" but does refer to "critical facilities" as:

> The primary physical structures, technical facilities and systems which are socially, economically or operationally essential to the functioning of a society or community, both in routine circumstances and in the extreme circumstances of an emergency. (UNISDR 2009: 8–9).

Critical facilities are seen as "specific elements of the infrastructure that support essential services in a society" (UNISDR 2009: 9), such as water supply and communication systems or emergency operations centres. The US Federal Emergency Management Agency (FEMA) has adopted the same concept. It includes all public and private facilities that a community considers essential to the delivery of vital services and to its own protection (FEMA 2007: 2). In the following pages, we consider the terms "critical infrastructure" and "critical facilities" as synonyms, but we hope that further discussion of the definitional issue will take place in the scientific community.

2.2 Operational use of critical infrastructure and facilities

Both critical infrastructure and critical facilities can be classified into sectors and ranks that reflect their importance in crisis management. Clear examples are derived from the analysis of two countries, the UK and the USA. The UK Cabinet (2010, 2011) has identified nine sectors of national critical infrastructure: food, energy, water, communications, transportation, health, emergency services, government and finance. Other categories of national significance are civil nuclear facilities, hazardous localities, sites of cultural importance and companies that maintain information of strategic value to the Government (UK Cabinet 2011). Once defined, critical national infrastructure is rated on a "criticality scale" from 0 to 5, where 0 represents a low and 5 a maximum level. Criticality is measured in terms of (a) the interruption of essential services, (b) what this means in terms of the resulting economic impact and (c) the impact on daily life. Furthermore, three factors help define the severity level: (a) the degree of disruption to essential services, (b) the extent of the disruption in terms of population impacted or geographical spread and (c) the length of time that the disruption persists. A different approach is used by the US Government (White House 2013), which lists 16 categories. In order to clarify functions, roles and responsibilities across the Federal Government and enhance internal coordination, it has identified dependencies in each sector. At the regional level, the buildings that need to be reactivated or repaired after disasters are ranked from 1 to 5, where 1 represents the most critical infrastructure and 5 the least critical (see, for example, Hillsborough County 2009). It must be noted that the documents considered refer to both public and

private sites at which there is an assumption of responsibility to assure safety and security according to current legislation and standards.

Together with their key role in the highly developed countries (HDC), critical infrastructures and critical facilities are becoming assets of central importance to the international sharing of knowledge. For example, the Peruvian Instituto Nacional de Defencia Civil et al. (2011) assessed the essential resources for emergency response and recovery in the metropolis of Lima and Callao in order to plan alternative strategies to compensate for loss of service. Evidence from elsewhere in South America reported by both D'Ercole and Metzger (2009), and Metzger and D'Ercole (2011) helped show the Peruvians how human and material resources affect urban management procedures and how they maintain social functions associated with vulnerability reduction and the gradual acquisition of resilience.

To sum up, our review shows that the current use of terminology associates critical infrastructures and facilities with a wider range of attributes than physical buildings alone. They are seen as central nodes that endow society and the built environment with cohesiveness. They catalyse the development of functional sectors, essential services and technical assets. However, they have to be framed in terms of short- and long-term strategies that specify the range of criticality and also the responsibilities of management. The next section will describe these relationships and interdependencies in relation to cascading events.

3 Critical infrastructures, interdependencies and cascades

Nowadays, many technologies generate socio-technical networks that have distinctive spatial extents and are integrated into functions such as transportation, communication or energy supply (Bijker et al. 1987). As they grow more interdependent, they become more vulnerable to large-scale cascading disruptions across sectoral boundaries (Amin 2002). As much as the complexity of human space increases with the urbanisation process, in solving problems there is a need to find redundancy and reliable alternatives (Jha et al. 2013). Here, the built environment has to be considered as a whole, including the capacity of buildings both to withstand the impact of hazards and to influence social vulnerability (Johnson 2012). The interdependent nature of many systems significantly complicates this process and increases the potential for cascading effects and disasters to occur. For example, at a small scale, a sinkhole in a street can affect underground pipes and disrupt the distribution of a variety of utilities. If a fire is generated by the broken lines, perhaps it could not be effectively fought because of the loss of water supply in broken mains. The possible threat to proprieties and lives posed by the secondary crisis can exceed that caused by the original trigger (Little 2002).

As a second example, the public utility sector, including government services (e.g. government offices) and emergency services (e.g. hospitals), involves mutual interdependency but at the same time is interconnected with other networks so as to ensure that the social system functions (NARUC 2005). In this case, the example includes energy supply (e.g. a compressor station), electrical power (e.g. power plants), communication (e.g. switching stations), transportation (e.g. an airport), water (e.g. substations) and finance (e.g. cash dispensers). Moreover, the criticality of infrastructure results from a wide spectrum of possible relationships among inter-organisational networks, in which transfer of resources across physical spaces is related to communication of information between organisations and individuals (Pelzer and Hempel 2014). If there is insufficient capacity for

redundancy, or none at all, even isolated failures can generate cascades that involve other sectors or the whole of society. First, vulnerable equipment and materials such as storage tanks, transportation pipelines and paperwork can be related to the spreading of secondary accidents consequent upon natural hazards (Krausmann et al. 2011). Secondly, excessively prolonged service lives, ageing materials and inadequate maintenance can influence the robustness of infrastructure (Little 2002). Thirdly, societal resilience is the results of the human dimension included in critical infrastructure, such as the need for emergency managers to achieve adequate levels of preparedness and thus the need to train personnel and leaders (Boin and Mc Connell 2007).

Some forms of critical infrastructure represent potential hazards in their own right: nuclear power plants, wastewater treatment facilities and biochemical manufacturing plants are distinguished by the use of polluting material that can damage the environment and health if it is released. For example, during the 2002 floods in central Europe, inundation of the Spolana chemical plant in the Czech Republic caused a major secondary event in the form of a serious pollution hazard. This had a significant effect upon the progress of international emergency relief (Pescaroli and Alexander 2015). In contrast, the critical infrastructure related to social sectors is more easily associated with long-range and multiple-level disruptions. Luiijf et al. (2009) analysed a data set of 1749 critical infrastructure failures in 29 European nations, 95 % of which post-dated the year 2000. It emerged that cascades are fairly common and there are clear pathways of spreading. These authors found that the energy sector accounts for 60 % of all cascades, 28 % originate in the telecommunication and Internet sectors, 5 % come from the transportation sector, and 3 % are found in the water sector (Luiijf et al. 2009: 305). Triggers in the energy sector generated an average of 2.06 disruptions in other forms of critical infrastructure, and those in telecommunication caused an average of 1.86 disruptions in other sectors. In this study, each cascading effect was analysed as a disruption consequent upon the preceding event that initiated it. However, the authors were more intent on identifying and classifying cascading effects (by category, such as education, financial services and industry) rather than determining how they occurred and by what pathways. The study tended to assume linear effects, but did not analyse and verify that this was the case. Moreover, they quantified cascades (in relative percentage terms) merely on the basis of reports of their occurrence rather than on any more sophisticated enquiry. This is understandable, given the large number of events with which they were dealing.

The same observations apply to the study by Van Eeten et al. (2011), who provided similar evidence in terms of an analysis of 830 reports of incidents in the Netherlands. In this case, more than 47 % of all cascades originate within the energy sector, 44 % within telecommunications and the Internet, and 3.2 % in transportation. Energy and telecommunications trigger disruptions in other critical infrastructure sectors in line with the figures provided by Luiijf et al. (2009). However, if telecommunication services suffer from energy outages, the reverse is not necessarily true. The different behaviours of the energy sector in the Netherlands can be related to legislation and governmental actions that have created a more reliable transmission grid that exists in other countries (Van Eeten et al. 2011).

Other studies have brought together a wider spectrum of evidence about the key pathways of cascades at the global level. For example, in analysing the impact of Hurricane Sandy in 2012, Kunz et al. (2013) showed that there was a broad dependency on power and ITC systems, while in the food, beverage and tobacco sector, there was a total dependency on transportation. Sandy demonstrated that, once again, the system of critical infrastructure is heavily dependent on electrical power and, as a whole, is extremely vulnerable to natural

hazards (Comes and Van de Walle 2014). Impacts on energy supply generate consequences for telecommunications, the oil and gas industry and transportation which indirectly generate disruption and long-term cascading loops that reinforce the disruption (Comes and Van de Walle 2014). Around 50 fatalities were associated with extended power outages consequent upon Hurricane Sandy and ensuing cold weather (Blake et al. 2013).

In the case of cross-boundary crises, the role of telecommunications appears to be slightly different. For example, in December 2006 a small sea-floor earthquake in the south of Taiwan damaged submarine cables used for telephone services and Internet transmission across much of East and Southeast Asia. The consequences spread to Taiwan, Hong Kong, Japan, China, Singapore and South Korea. There were substantial economic implications, as transactions made on international financial markets were adversely affected (Smith and Petley 2009). Emerging threats include the sensitivity of hi-tech infrastructures such as satellites or power lines to natural events such as geomagnetic storms and other forms of "space weather" (OECD 2011).

Some other issues relate to transportation. In this context, both Van Eeten et al. 2011 and Luiijf et al. (2009) attributed a small but significant percentage of disruption to infrastructure as the originator of cascades. The "just-in-time" economic model that relies on the global continuity of supply can be regarded as a part of this problem. When physical damage caused by natural hazards or technical breakdown undermine long-range logistics, delays and failures may spread across interconnected supply chains and thus throughout society (OECD 2011). The 2010 eruption of Eyjafjallajökull and the consequent disruption of air transportation showed how this sector can compromise many levels of social, political and economic activities in Europe, with global consequences (Alexander 2013a). Eight and a half million people were stranded, airlines risked bankruptcy, official political campaigns were cancelled, cultural events were suspended, and major sporting events were postponed. The leading logistics couriers, such as DHL Express, were grounded and had to find alternative routes by ship or road. Supply problems led to shortages of electronic hardware and restricted the import and export of perishable goods such as fruit, vegetables, flowers and bone marrow (for transplant).

4 Complex adaptive systems, panarchies and cascading disasters

So far in this article, we have reviewed the different attributes of cascades in critical infrastructure. This section will propose a systems model of their role. Rinaldi et al. (2001) defined the interdependencies among critical infrastructures as *complex adaptive systems* (CAS), meaning "complex collections of interacting components in which change often occurs as a result of learning processes and where each component of an infrastructure constitutes a small part of the intricate web that forms the overall infrastructure" (Rinaldi et al. 2001: 13). According to these authors, the various components of critical infrastructure function as agents that interact according to their location in geographical space, capabilities (for example pumping capacity) and memory (the result of experiences such as degradation by overuse). Through inputs (i.e. resources to be used) and outputs (i.e. products), they communicate with the other elements of infrastructure, but they are individually capable of learning from the past and adapting to the future (e.g. enabling personnel to improve their training or adopting new technologies for monitoring).

The physical and organisational elements of infrastructure interact with the functional aspects but have to be referred to their contextual drivers, such as environment, politics and

social milieu (Rinaldi et al. 2001). Critical infrastructure has to be analysed as a series of points that accumulate different attributes and levels of complexity. The vulnerability of sub-systems is a function of the way the entire assemblage works (Bouchon 2006). This implies a need to broaden the perspective on the possible role of critical infrastructure in cascades.

According to Holling (2001), the adaptive cycles that maintain evolutionary capacity in ecology alternate periods of accumulation and transformation of resources with shorter periods in which the accumulated potential is released, perhaps by means of a crisis. "Adaptive capacity" is a measure of the vulnerability and resilience of the system to unexpected or unpredictable shocks. A nested set of adaptive cycles that evolves dynamically is described by the term "panarchy". The functioning of the adaptive cycles and the way they communicate with each other can be related to sustainability (Holling 2001). However, the metaphor does not imply fixed or regular cycles but assumes that some of the interaction occurs at multiple scales of time and physical dimensions (Walker et al. 2004). When a level of the system initiates "creative destruction", and the other levels have accumulated vulnerabilities and rigidities, the crisis spreads across the system towards a "panarchical collapse". Once thresholds are crossed, cascading effects are generated with consequent regime shifts across scales and domains (Kinzig et al. 2006). Holling (2001, p. 404) defined these circumstances symbolically as an "alignment of the stars". By this, he meant that hazard and vulnerability have to interact at different scales. In our opinion, the definition can easily be associated with the evidence for cascading disasters and their impact upon critical infrastructure. Unaligned vulnerabilities would stop the propagation of impacts: aligned vulnerabilities would facilitate it. This point will be illustrated with two examples, which are important for the concepts of both complex adaptive cycles and panarchy in relation to critical infrastructure and disasters.

Scale issues and the role of vulnerability are illustrated in Fig. 2. This takes Holling's "Möbius strip" diagram of system functions in an adaptive cycle (exploitation–conservation–reorganisation–release—Holling 2001, p. 394) and shows how it fits with diverse

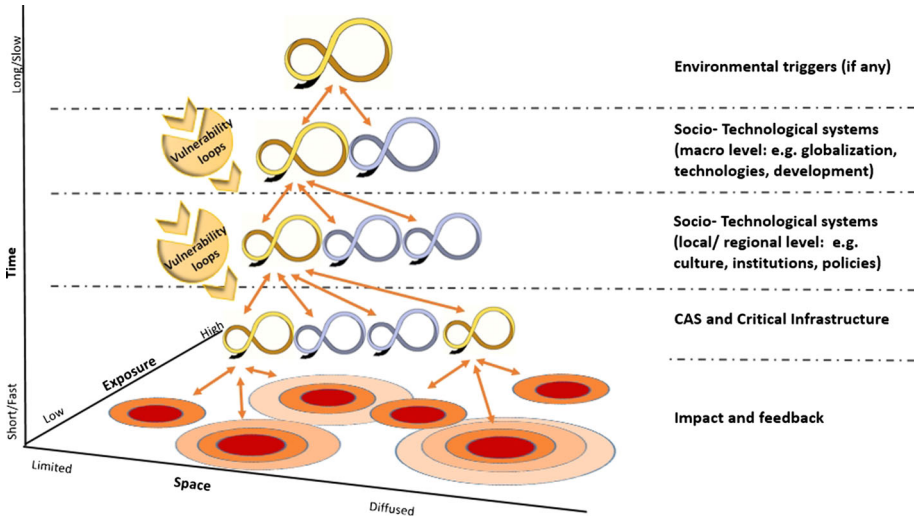

Fig. 2 Different scales, feedbacks and vulnerability paths in cascading disasters

time and space scales. These are the scales and domains that cascading effects traverse. In this diagram, the domain of critical infrastructure exists between its controlling factors, above, and its impacts, below. The arrows denote feedback in either direction.

It must be noted that our approach is not in contradiction with Perrow's theory of normal accidents (1999). Indeed, in high-risk technological systems "neither better organization nor technological innovations appear to make them less prone to system accidents" (Perrow 1999, p. 5), and "given the system characteristics, multiple and unexpected interaction of failures are inevitable" (Perrow 1999, p. 5). This is exactly what can be seen in Fig. 2 with some differences: in our perspective, cascading disasters are a consequence of vulnerabilities accumulated in different scales, which are manifested when breaking points are aligned. In other words, it is true that coincidences exist and it is impossible to monitor all the components of the system, such as a small pipe that broke in the wrong moment, but cascading events seems to be driven by a path waiting to happen and rooted in far more complex social issues.

The technical failure that started the notorious blackout of 2003 in North America was a result of the joint effect of production pressures, failure of regulatory authority, lack of risk assessment, lack of coordination among actors, and scarce consideration of precursors (Dien and Duval 2014). The accumulation of rigidities became evident when a heat wave suddenly increased the demand for energy, which required adaptation of the network to new environmental conditions which could not be achieved in time. Lack of compatibility of the timescales of impact and avoidance behaviour led to the crisis. Accumulated rigidity existed in the inability to adapt to demand caused by a change in the weather.

Similarly, in 2010, when the eruption of Eyjafjallajökull created the biggest disruption of air transportation since WWII, millions of passengers were left stranded because there was insufficient adaptive capacity in society. Commercial aviation had not been adequately coordinated or harmonised with other forms of transportation and hospitality (Parker 2014) to cope with the stranding of passengers. Concurrently, the "just-in-time" economic model that relies on the global continuity of supply relies significantly on air transportation and has airports as some of its most important nodes (Alexander 2013a). Airports and flights were then the points at which the rigidities of the transportation sector were concentrated and manifest in the form of technological and organisational fragilities.

Individual critical infrastructures (such as electricity generation and distribution or food supply) are complex adaptive systems with different parameters and different speeds of recovery following disruption. The density of the networks varies, and so do the rates of response to perturbations of the system. However, there are obvious interdependencies between the systems, such as the need for electricity supply in order to refrigerate food. There is a need to understand the cycles of functioning of each CI system and the vital points of contact with, and dependency upon, other systems. Failure at the points of mutual dependency will propagate a lag in the recovery process, and that is in addition to lags propagated by movement down a single system, for example, from the national to the local level. A considerable challenge is inherent in this concept: to understand how complex systems adapt to the forces that drive them, and simultaneously to understand how they adapt to each other through complex interdependencies.

We argue that cascading disasters have similar dynamics to the spread of crisis in panarchies: an environmental hazard or other threat can be a trigger of dynamic processes that weaken the system. Society and its components (e.g. policies, organisations and economics) occupy the intermediate levels between localised infrastructure and international interdependencies. Nodes in critical infrastructure amplify the structural weaknesses by transmitting them across scales. Cascades may result from a lack of sustainability in the

system, for example where they are associated with long-range supply processes, management cultures or to consumer behaviour. On the one hand, this is in line with the idea that cascading ecological crises, such as those related to climate change, are nonlinear consequences of complex causal chains in which environmental dynamics react to human stressors (Galaz et al. 2011). On the other hand, cascading effects accompany a transition from a stable to an unstable state of the system and are amplified by latent vulnerabilities, such as the increasing interdependency of functional sectors in modern global society (Helbing 2013).

The power outage of 2003 in Italy furnishes an example of scale effects in critical infrastructure cascades. On the night of 28 September 2003, electricity was being imported into Italy from Switzerland via three routes. A short circuit occurred when one transmission line overheated and touched the branch of a tree. Transmission automatically switched to the other two lines and then shut itself down to prevent them from overheating too. A series of blackouts propagated from the Swiss–Italian border progressively as far as Sicily and Geneva, affecting 56 million people. Trains were marooned in tunnels, and people were trapped in elevators. Civil aviation was briefly shut down. In this example, a very localised fault rapidly spread to the level of international system-wide effects. Transportation, health systems, the Internet and building maintenance were affected, and lack of refrigeration put foodstuffs at risk. However, as the blackout occurred in the night on a Sunday morning, many effects were localised and hence on the scale of the original fault. Nevertheless, loss of electrical power to the Internet propagated failure at power stations through inability to transmit control data (Bacher and Näf 2003). The extraordinary extent of the power failure was the result of cascades in independent networks being transmitted to each other through the nodes of contact (Buldyrev et al. 2010).

In order to understand the evolution of the system, three contributing factors must be considered determinant: interactions within in the system, context such as institutional conditions, and a triggering event, which may show that random factors can determine the temporal evolution of the system (Helbing 2013: 54). To sum up, we argue that the interdependencies among critical infrastructure in the form of complex adaptive systems (Rinaldi et al. 2001) can be seen as the nodes that concentrate micro- and macro-dynamics that join together panarchies, globally networked risks and cross-scale interactions. Cascades are more the product of an "alignment of stars", as Holling would have it, than to unexpected, low-probability, high-impact events. Although it can be argued the existence of "normal accidents" (Perrow 1999), we think cascading could be significantly more dependent by contextual dynamics that relate the single components to cross-scale interactions. When a triggering event happens, they progress by unsolved vulnerabilities that are concentrated in critical infrastructure. They recombine and generate a nonlinear progression of events that amplify the overall impact of disasters. However, they are usually deeply rooted in pre-existing factors, as analysed in the next section.

5 Vulnerability path

The previous sections of this paper defined critical infrastructure and explained its possible role in the spread of cascading disasters. This section will concentrate on understanding vulnerability as a sort of directional path. In one of the most widely used books on disaster reduction, Wisner et al. (2003) suggested that different levels of vulnerability have to be considered if one is to identify the root causes of disaster, and they are determined by

social systems and power relations, not natural forces (Wisner et al. 2003: 7). They can be generated by processes that operate at different spatial and temporal scales, including national and international ones. According to these authors, vulnerability is a phenomenon that has multiple layers and different ways in which it progresses. It can be seen as the result of interactions among root causes, some of which are inherent in cultures and some in economic models, dynamic pressures (e.g. dependencies on critical systems) and unsafe conditions (e.g. precarious margins of production).

The thematic spheres of economy, social activity and environment must be considered as a whole by including organisational and institutional aspects as well as environmental and social ones (Birkmann 2007). However, it should be noted that vulnerability reduction strategies and mitigation options are conditioned by political choices and cultural constraints. Moreover, pervasive weaknesses in organisational structures directly influence levels of vulnerability and a system's capacity to react to a crisis, from the chain of command and control that organises preparedness and relief, to the state of critical infrastructure that can profoundly affect both the delivery of aid and welfare and the spread of secondary disasters. In other words, adopting the wrong measures or making unwise political and economic decisions can be seen to be an overall cause of disaster (Green 2005).

Political decision making is usually embedded in local or national culture, and those two factors can mutually influence each other. Cruz (2012) reported that, even where implementation is the preserve of experts, the adoption of building codes and standards is more likely to succeed if there is effective social demand for safety or there are the resources to apply the measures properly. In particular, in critical infrastructure, vulnerability reduction strategies may enter into conflict with a series of pre-existing routines and priorities that orient the decision-making process of citizens, organisations and politicians (Boin and Mc Connell 2007). It is essential to use a vulnerability assessment process to understand the pattern and path of such factors during periods of quiescence, and above all shortly before an extreme event (Johnston et al. 2006). This must involve the joint efforts of technical specialists, managers and public authorities in order to understand how critical infrastructure is vulnerable and how it loss will affect society. Hence, appropriate channels need to be utilised to educate the population, train personnel, involve the community and define the responsibilities of stakeholders. The key areas are public education, land-use control, government policy on critical and public facilities, land and property acquisition, building codes, safety standards and research (Johnston et al. 2006: 63). Because incompetence and corruption generate common failings that involve the social context, the effectiveness of government may be a crucial issue (Smith and Petley 2009).

Hellström (2007) adapted the model by Wisner et al. (2003) and defined critical infrastructure as a set of technological systems that fulfil social functions according to four principles: functional interlocking, dependencies and interdependencies among systems); temporal embeddedness (the depth of the changes required by innovation in the technological systems); critical socio-technical tipping-points (strategic connections, thresholds and interactions between society and technology); and dynamic and reversible effects (how root causes and unsafe conditions become dynamic pressures). This approach extended the "pressure-and-release" model of Wisner et al. (2003) to new forms of technological progress. It seems to confirm the association of Holling's "alignment of stars" (2001) in terms of cascading disasters (Pescaroli and Alexander 2015). Hazard impacts tend to be dependent on pre-existing vulnerability factors, and the aggregation of vulnerabilities and pressures at some point of the system are the trigger of crisis or disaster (Hellström 2007: 427). Alexander (2000) showed how feedback processes in political, technological social

and cultural contexts can favour unprotected development and inhibit mitigation (Fig. 3). When the mitigating factors provided by knowledge and good governance are overwhelmed by negative factors such as negligence and increases in vulnerability, losses are hard to avoid.

This dynamic seems to be recurrent. For example, negligence was a significant factor that determined the Fukushima meltdown (Synolakis and Kânoðlu 2015), but it was also a factor in the secondary disasters caused by the 2002 floods in the Czech Republic (Pescaroli and Alexander 2015). The absence of international coordination during the disruption of European civil aviation resulting from the 2010 volcanic eruption in Iceland did not happen by chance (Alexander 2013a; Parker 2014), but was the output of clear political choices that failed to take account of a concrete and plausible risk. In fact, it can be argued that human failures or structural vulnerabilities are visible in most disasters in which cascading effects are present, and they are often associated with low levels of institutional accountability. The evidence to support this approach can provide by the most famous among the cascading events, the meltdown of the Fukushima Daïchi Nuclear Power Plant, which followed the Tōhoku earthquake and tsunami of March 2011. In the official documentation of the National Diet of Japan Fukushima (2012), it was stated that: "The TEPCO Fukushima Nuclear Power Plant accident was the result of collusion between the government, the regulators and TEPCO, and the lack of governance by said parties… Therefore, we conclude that the accident was clearly 'manmade'" (National Diet of Japan Fukushima 2012: 16). Root causes were associated with the organisational and regulatory system, but also with the failure to take a series of preventative measures such as the adaptation of flood barriers to new risk scenarios. The Commission revealed that, even if they were aware of the risk, the protagonists failed to develop the basic safety requirements, to implement structural reinforcements or adopt adequate protection measures.

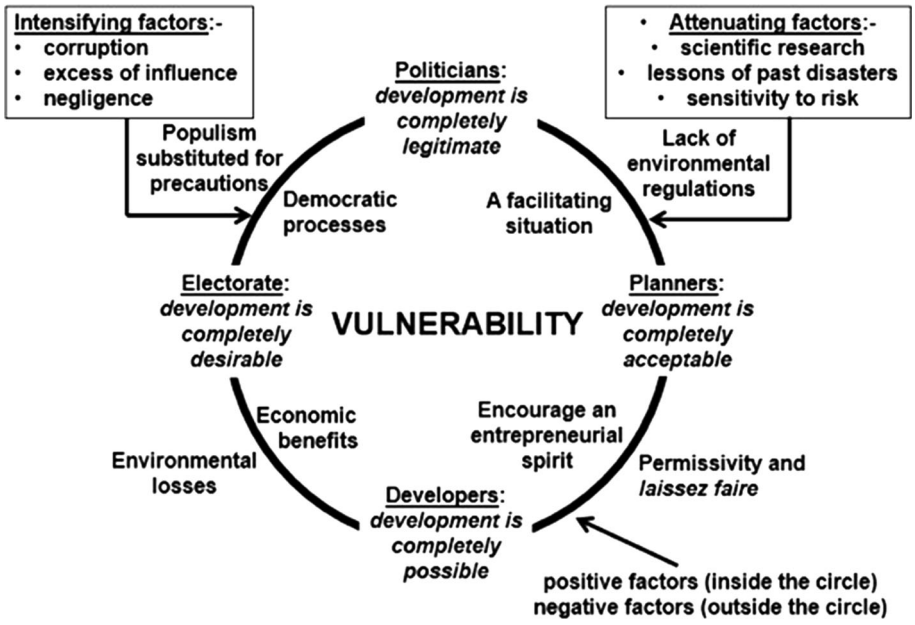

Fig. 3 Vicious circle of increases in vulnerability: a positive feedback situation (*source*: Alexander 2000)

However, the Fukushima case suggests that there should be a focus that is broad enough to include another critical element: the society in charge of the nuclear power plant (TEPCO) and the governmental bodies in charge of monitoring safety levels "postponed putting safety measures in place, or made decisions based on their organisation's self-interest, and not in the interest of public safety" (National Diet of Japan Fukushima 2012: 16). The resilience of infrastructure can be compromised by preferring a logic of maximum profit or assiduously following the "predatory models of neoliberal financial capital" (Graham 2010: 14).

A recurrent problem is that interdependent networks have been "consistently pushed to the edge of their design envelopes, under pressure to maximise, if not optimise, their performance" (Schulman et al. 2004). For example, Dien and Duval (2014) showed that, in both the blackout in North America in 2003 and the near miss at the Davis Besse nuclear power station in 2002, the pressure on productivity caused performance to be put before safety. This occurred in correspondence with different levels of organisational and management failures: a weakness of the regulatory authorities, lack of risk assessment and training, limitations on feedback from the operating environment, and poor coordination among operators. In other words, the vulnerability of critical infrastructure cannot be related only to the built environment but must also be connected to the different levels of responsibility and human interaction: pre- and post-emergency management, urban and infrastructural planning, and political and social visions (Graham 2010).

6 Conclusion

In line with Holling (2001), we have endeavoured to show how cascading disaster can be seen as an "alignment of stars" in socio-ecological systems. The diffusion of consequences appears to be determined by vulnerabilities that are latent in global society (Helbing 2013), which may be manifest in complex and secondary events (Pescaroli and Alexander 2015). Despite the common conception that cascading disasters are unexpected low-probability, high-impact events, in our opinion they are well rooted in society's feedback loops (Alexander 2000). Elements such as corruption, negligence, maximisation of profit and the structural weaknesses of the global socio-economic system should be seen as causes to be studied and addressed. In practical terms, the role of critical infrastructure in cascading disasters suggests that it is necessary to create a new culture of preparedness at the international level, for many of the scenarios involve international transboundary crises.

We argue that, although because of their high complexity and cross-scale dynamics cascading disasters cannot be prevented, latent vulnerability can be understood and addressed before the trigger events occur. We need to broaden the consensus on the development of new tools and strategies. The literature shows that neither vulnerability assessment (Little 2002) nor contingency planning (Boin and Mc Connell 2007) are sufficient on their own. It can be true that sometimes "the problem is just something that never occurred to the designer" (Perrow 1999), but how to tackle the "alignment of stars" that generate the cascade? We suggest shift attention from *risk scenarios based on hazard* to *vulnerability scenarios* based on potential escalation points. That is to say, we cannot know which events can happen at the macroscopic level, but we can identify the sensitive nodes that are capable of generating secondary events at the smallest scale. This point presents significant methodological challenges, but the final output could be used to highlight the weakest nodes that are most significant when cascades are generated. It could help create

common rankings of critical infrastructure based on interdependencies and hazard potentials and thus help to improve existing rankings (UK Cabinet 2011). For example, if authorities, organisations and managers are able to improve the way they exchange information on critical infrastructure, this will improve their ability to recognise and deal with the triggers of the kinds of crisis that have widespread effects among the many users of the infrastructure in question. Moreover, instead of generating reasonable worst-case scenarios based on the initial triggers, we could shift the emphasis to reasonable worst-case *amplification* scenarios.

If a systems perspective such as that offered by Holling (2001) is adopted, cascading disasters can be seen as a manifestation of a lack of sustainability in adaptive and evolutionary processes. The sensitivity of global supply in the energy and transportation sectors to localised disruption underlines this point, but further discussion and research are needed in order to clarify and test the concept. Our theoretical approach has many limitations, including the difficulty of establishing cause and effect in complex situations, the challenge of modelling the complexity of interactions among parallel systems of critical infrastructure, and the difficulty of translating effects from one scale to another. However, as these are mostly limitations based on the need to fill in details, we argue that they do not invalidate our findings. Although lack of training and management technique are key drivers of vulnerability, we must also consider the need for a wider integration of social behaviour and community-based perspectives. Further research is needed in order to ascertain whether cascading ecological crisis models are fully applicable to situations in which the hazards revolve around malfunctioning (Galaz et al. 2011). Early warning, the behaviour of operators, communication failures and bureaucratic conflicts are some of the areas in which further research could help us to understand how cascading disasters propagate in critical infrastructure, and how their progress can be arrested.

Acknowledgments This work has been carried out under the aegis of the EC FP7 FORTRESS project. FORTRESS, funded by the European Commission within FP7 Area 10.4.1, Preparedness, Prevention, Mitigation and Planning, TOPIC SEC-2013.4.1-2 SEC-2013.2.1-2, Grant 607579. We wish to thank our partners for much useful dialogue, in particular Yves Dien, Carole Duval (Electicitè De France, EDF), Leon Hempel and Rober Pelzer (Technische Universität Berlin, TUB), who supported our work with key insights from their experience. A special acknowledgement is made to our colleagues Ilan Kelman, Robert Wicks (IRDR) and Charles Parker (CNDS) for their precious feedbacks on the theoretical framework.

References

Alexander DE (2000) Confronting catastrophe. Oxford University Press, New York

Alexander DE (2013a) Volcanic ash in the atmosphere and risks for civil aviation: a study in European crisis management. Int J Disaster Risk Sci 4(1):9–19

Alexander DE (2013b) Critical infrastructure. In: Penuel KB, Statler M, Hagen R (eds) Encyclopedia of crisis management. Sage, Thousand Oaks, pp 208–211

Amin M (2002) Toward secure and resilient interdependent infrastructures. J Infrastruct Syst 8(3):67–75

Ansell C, Boin A, Keller A (2010) Managing transboundary crises: identifying the building blocks of an effective response system. J Conting Crisis Manag 18(4):195–207

Bacher R, Näf U (2003) Report on the blackout in Italy on 28 September 2003. Swiss Federal Office of Energy, Berne, 25 pp

Bijker W, Huges TP, Pinch T (1987) The social construction of technological systems: new directions in the history of sociology of technology. MIT Press, Cambridge
Birkmann J (2007) Risk vulnerability indicators at different scales: applicability, usefulness and policy implications. Environ Hazards 7(1):20–31
Blake ES, Kimberlain TB, Berg RJ, Cangialosi JP, Beven JL (2013) Tropical cyclone report hurricane sandy (AL182012), 11–29 October 2012. National Hurricane Centre, Miami, Florida. http://www.nhc.noaa.gov. Accessed 3 Sep 2015
Boin A, Mc Connell A (2007) Preparing for critical infrastructure breakdowns: the limits of crisis management and the need for resilience. J Conting Crisis Manag 15(1):50–59
Bouchon S (2006) The vulnerability of interdependent critical infrastructures systems: epistemological and conceptual state of the art. European Commission, Brussels. Institute for the Protection and Security of the Citizen, EC Joint Research Centre, Ispra. Bookshop.europa.eu. Accessed 26 Sep 2015
Buldyrev SV, Parshani R, Paul G, Stanley HE, Havlin S (2010) Catastrophic cascade of failures in interdependent networks. Nature 464:1025–1028
Chongvilaivan A (2012) Thailand's 2011 flooding: its impact on direct exports and global supply chains. ARTNeT Working Paper Series 113, Asia-Pacific Research and Training Network on Trade, Bangkok, 33 pp
Comes T, Van de Walle B (2014) Measuring disaster resilience: the impact of Hurricane Sandy on critical infrastructure systems. In: Proceedings of the eleventh international ISCRAM conference, University Park, Pennsylvania, USA, May 2014, pp 195–204. http://iscram2014.ist.psu.edu. Accessed 11 July 2015
Cruz AM (2012) Protection of infrastructures. In: Wisner B, Gaillard JC, Kelman I (eds) Handbook of hazards and disaster risk reduction. Routledge, Oxford, pp 676–686
D'Ercole R, Metzger P (2009) Territorial vulnerability: a new approach of risks in urban areas. Cybergeo: European Journal of Geography. Dossiers, Vulnérabilités urbaines au sud, 447. http://cybergeo.revues.org. Accessed 11 July 2015
Dien Y, Duval C (2014) Near misses and influence effects: indirect factors of cascading in critical infrastructures. In: Pescaroli G, Alexander D, Sammonds P (eds) Pathogenic vulnerabilities and resilient factors in systems and populations experiencing a cascading disaster—deliverable 2.1. FORTRESS Project, 57–69. http://fortress-project.eu
Egan MJ (2007) Anticipating future vulnerability: defining characteristics of increasingly critical infrastructure—like systems. J Conting Crisis Manag 15(1):1–17
European Commission (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. http://europa.eu. Accessed 31 July 2015
FEMA (2007) Design guide for improving critical facility safety from flooding and high winds. US Federal Emergency Management Agency, Washington, DC
Galaz V, Moberg F, Olsson EK, Paglia E, Parker C (2011) Institutional and political leadership dimensions of cascading ecological crisis. Public Adm 89(2):361–380
Graham S (2010) Disrupted cities. Routledge, New York
Green P (2005) Corruption, construction and catastrophe. Br J Criminol 45:528–546
Helbing D (2013) Globally networked risks and how to respond. Nature 497:51–59
Hellström T (2007) Critical infrastructure and systemic vulnerability: towards a planning framework. Saf Sci 45:415–430
Hillsborough County (2009) Hillsborough county local mitigation strategy. Appendix K-1 Critical Facilities, Hillsborough County, Florida. http://www.hillsboroughcounty.org. Accessed 11 July 2015
Holling CS (2001) Understanding the complexity of economic, ecological, and social systems. Ecosystems 4(5):390–405
Instituto Nacional de Defencia Civil, Programa de les Naciones Unides Para el Des Arollo, Cooperazione Internazional – Coopi, Institute de Reserche pour le Developpment (2011) Estudio Sirad – Sistema de Informacion Geografico y analisis de recursos esenciales para la respuesta y recuperacion temprana ante la ocurrencia de un sismo y/o tsunami en el area metropolitana de Lima y Callao. Instituto Nacional de Defencia Civil, Lima
Jha AK, Miner TW, Stanton-Geddes Z (2013) Building urban resilience principles. International Bank for Reconstruction and Development, World Bank, Washington DC. http://elibrary.worldbank.org. Accessed 11 July 2015
Johnson C (2012) Urban and regional planning and disasters. In: Wisner B, Gaillard JC, Kelman I (eds) The Routledge handbook of hazards and disaster risk reduction. Routledge, Oxon, pp 641–675
Johnston D, Becker J, Cusins J (2006) Lifelines and urban resilience. In: Paton D, Auld T (eds) Disaster resilience an integrated approach. Thomas Publisher LTD, Springfield, pp 3–18

Kadri F, Birregah B, Châtelet E (2014) The impact of natural disasters on critical infrastructures: a domino effect-based study. J Homel Secur Emerg Manage 11(2):217–242
Khan FI, Abbasi SA (2000) Studies on the probabilities and likely impacts of chains of accident (domino effect) in a fertilizer industry. Process Saf Prog 19(1):40–56
Kinzig AP, Ryan P, Etienne M, Llison H, Elmqvist T, Walker BH (2006) Resilience and regime shifts: assessing cascading effects. Ecol Soc 11(1):20
Krausmann E, Renni EM, Campedel M, Cozzani V (2011) Industrial accidents triggered by earthquakes, floods and lightning: lessons learned from a database analysis. Nat Hazards 59:285–300
Kunz MB, Mühr T, Kunz-Plapp JE, Daniell JE et al (2013) Investigation of Superstorm Sandy 2012 in a multi-disciplinary approach. Nat Hazards Earth Syst Sci 13:2579–2598
Lewis TG (2006) Critical infrastructure protection in homeland security. Wiley, Hoboken
Little RG (2002) Controlling cascading failure: understanding the vulnerabilities of interconnected infrastructures. J Urban Technol 9(1):109–123
Luiijf E, Nieuwenhuijs A, Klaver M, Van Eeten M, Cruz E (2009) Empirical findings on critical infrastructure dependencies in Europe. In: Setola R, Geretshuber S (eds) CRITIS 2008, LNCS 5508, pp 302–310
McGee S, Frittman J, Ahn S, Murray S (2014) Risk relationships and cascading effects in critical infrastructures: implications for the Hyogo framework. United Nations Office for Disaster Risk Reduction, Global Assessment Report on Disaster Risk Reduction. http://www.preventionweb.net. Accessed 27 Sep 2015
Metzger P, D'Ercole R (2011) Les risques en milieu urbain: éléments de reflexion. EchoGéo 18:2–13
NARUC (2005) Technical assistance brief on critical infrastructure protection-utility and network interdependencies: what state regulators need to know. National Association of Regulatory Utility Commissioners, Washington, DC. www.naruc.org. Accessed 27 Sep 2015
National Diet of Japan (2012) The official report of the Fukushima nuclear accident independent investigation commission, executive summary. The National Diet of Japan, Tokio. www.reliefweb.int. Accessed 10 Feb 2016
NATO (2007) 162 CDS 07 E REV 1—the protection of critical infrastructures. Parliamentary Assembly of the North Atlantic Treaty Organisation, Brussels. http://www.nato-pa.int. Accessed 09 March 2015
OECD (2008) Protection of "critical infrastructure" and the role of investment policies relating to national security. Organization for Economic Co-operation and Development, Paris, 2008. http://www.oecd.org. Accessed 15 July 2015
OECD (2011) OECD reviews of risk management policies, future global shocks, improving risk governance. Organization for Economic Co-operation and Development Paris. http://www.oecd.org. Accessed 11 July 2015
Parker C (2014) Complex negative events and the diffusion of crisis: lessons from the 2010 and 2011 Icelandic volcanic ash cloud. Swed Soc Anthropol Geogr 97(1):97–108
Pelzer R, Hempel L (2014) Resilience within a social perspective. In: Pescaroli G, Alexander D, Sammonds P (eds) Pathogenic vulnerabilities and resilient factors in systems and populations experiencing a cascading disaster—deliverable 2.1. FORTRESS Project, 39-43. http://fortress-project.eu. Accessed 27 Sep 2015
Perrow C (1999) Normal accidents: living with high risk technology. Princeton University Press, Princeton, New Jersey
Pescaroli G, Alexander DE (2015) A definition of cascading disasters and cascading effects: going beyond the "toppling dominos" metaphor. Planet@Risk Glob Forum Davos 3(1):58–67
Rinaldi SM, Peerenboom JP, Kell TK (2001) Identifying, understanding, and analysing critical infrastructure interdependency. IEEE Control Syst Mag 21(6):11–25
Schulman P, Roe E, van Eeten M, De Bruijne M (2004) High reliability and the management of critical infrastructures. J Conting Crisis Manag 12(1):14–28
Smith K, Petley D (2009) Environmental hazards. Assessing risk and reducing disaster, 5th edn. Routledge, New York
Stallings RA (2006) Causality and "natural" disasters. Contemp Sociol 35(3):223–227
Synolakis C, Kânoðlu U (2015) The Fukushima accident was preventable. Philos Trans R Soc A 373:1–23
UK Cabinet Office (2010) Strategic framework and policy statement on improving the resilience of critical infrastructure to disruption from natural hazards. Cabinet Office, Whitehall, London. https://www.gov.uk. Accessed 14 July 2015
UK Cabinet Office (2011) Keeping the country running: natural hazards and infrastructure. Cabinet Office, Whitehall, London. https://www.gov.uk. Accessed 11 July 2015
UNISDR (2009) UNISDR terminology on disaster risk reduction. United Nations International Strategy for Disaster Reduction, Geneva, Switzerland. http://www.unisdr.org. Accessed 11 July 2015

Van Eeten M, Nieuwenhuijs A, Luiijf E, Klaver K, Cruz E (2011) The state and the threat of cascading failure across critical infrastructures: the implications of empirical evidence from media incident reports. Public Adm 89(2):381–400

Walker B, Holling C, Carpenter S, Kinzig A (2004) Resilience, adaptability and transformability in social–ecological systems. Ecol Soc 9(2):5

White House (2013) Presidential policy directive. Critical infrastructure security and resilience. Directive/PPD-21. White House, Washington DC. http://www.whitehouse.gov. Accessed 11 July 2015

Wisner B, Blaikie P, Cannon T, Davis I (2003) At risk-natural hazards, people's vulnerability and disasters. Routledge, New York