Safety Science 110 (2018) 131–140

Contents lists available at ScienceDirect

Safety Science

journal homepage: www.elsevier.com/locate/safety

Increasing resilience to cascading events: The M.OR.D.OR. scenario

G. Pescaroli[a,*], R.T. Wicks[a], G. Giacomello[b], D.E. Alexander[a]

[a] Institute for Risk and Disaster Reduction, University College London, London, UK
[b] Department of Political and Social Studies, University of Bologna, Bologna, Italy

ARTICLE INFO

Keywords:
Cascading disasters
Cascading events
Critical infrastructure
Extreme space weather
Cybersecurity
Risk
Resilience

ABSTRACT

The growing complexity of global interconnected risk suggests that a shift has occurred in the way emergency planners need to improve preparedness and response to cascading events. With reference to the literature from the physical, social and political sciences, this paper analyses extreme space weather events and cyberattacks. The goal of this work is to produce a replicable scenario-building process, based on cross-disciplinary understanding of vulnerability, that could be complementary to probabilistic hazard assessment. Our hypothesis is that the technological and human component of critical infrastructure could be the primary vector for the escalation of secondary emergencies. While not themselves having direct implications in terms of loss of life, elements that are common to different risks could provide particular challenges for disaster management. Our findings identify some vulnerable nodes, such as Global Navigation Satellite System technology and remote-control systems, that could act as paths for the escalations of events. We suggest that these paths may be common to various known and unknown threats. We propose two scenarios of Massive, OveRwhelming Disruption of OpeRations (M.OR.D.OR.) that could be used for testing emergency preparedness strategies, and increasing the response to highly complex, unknown events. The conclusions highlight the open challenges of seeking to increase societal resilience. The limitations of this work are described, as are the possible challenges for future research.

1. Introduction

The vulnerability of society to cascading events is a major topic of discussion in the scientific community. It is now clear that highly interconnected and interdependent systems resulting from the technological thrust of globalization are becoming more unstable and harder to predict (Helbing, 2013). Research funders are allocating a growing amount of money to the development of strategies that improve disaster risk reduction. Hence the European Commission has supported such efforts with grants allocations in the Seventh Framework Programme and Horizon 2020 programmes. Some early research outputs suggested the need to go beyond the "toppling dominoes" metaphor, which is associated with an initial event that sets off a chain of eventualities (Khan and Abbasi, 2000, Reniers, 2009). Understanding cascading events could have larger implications for modern society because the traditional classification of natural, human-made, and hybrid disasters, reported by authors such as Shaluf (2007), seems to be an insufficient tool in the face of the high complexity of the present-day world. According to Pescaroli and Alexander (2015), cascading disasters can be distinguished by non-sequential escalations of secondary emergencies, in which primary events are less problematic than the chain of effects triggered by their impact. One of the many consequences of this non-sequential process is the disruption of critical infrastructure (CI), which can be understood as those assets or systems that are vital to the maintenance of social functions via their technological, functional, organizational, and social attributes (Alexander, 2013b). The process could be associated with failures in preparedness and response, and with passages from one state of operations to another in CI. "Normal" routines can deal with small disturbances, but they cannot cope when extraordinary measures are needed. Consequently, CI can enter into a "crisis" state, in which control is lost and emergency procedures are activated that require time and effort to bring the infrastructure back to its normal state (Nieuwenhuijs et al., 2008). In this process, the evolution of global technological systems may be one of the risk drivers. Helbing (2013) suggested that current risk analysis strategies seem to be inefficient on their own, partly because of problems in dealing with coincidences and partly because the processes that integrate event and problem trees are considered in a too-unidirectional way. The existing frameworks need to be improved by adapting preparedness strategies and deriving better tools for situational awareness in the field. Some new analyses of natural hazards and human vulnerabilities have been proposed in the literature, but the findings have rarely been used to promote complementary approaches to scenario building.

The climate change debate has raised awareness of compound

* Corresponding author.
E-mail address: gianluca.pescaroli@gmail.com (G. Pescaroli).

https://doi.org/10.1016/j.ssci.2017.12.012
Received 7 October 2016; Received in revised form 19 November 2017; Accepted 12 December 2017
Available online 05 January 2018
0925-7535/

events, which are to be understood as the simultaneous or successive combination of multiple physical processes (Field et al., 2012). This is the case, for example, when floods happen during a cold snap, or an earthquake triggers an avalanche. Analytical processes based on single variables may be unable to capture the risk represented by climate extremes, which depend on multiple drivers and multiple impacts on the human environment, and which require interdisciplinary collaborations in order to be understood (Leonard et al., 2014). Moreover, the literature on interconnected hazards places emphasis on interactions among physical dynamics, such as the causal mechanisms that develop when earthquakes generate tsunamis (Gill and Malamud, 2014). New multiple-hazard models deal with how to describe interactions, how to assess networks, and how to include events such as technological disasters (Gill and Malamud, 2016). In this context, a branch of the literature has been devoted to analysing the role and vulnerabilities of chemical facilities, which can become sources of escalation if they release their hazardous materials (Salzano et al., 2009, Krausmann et al., 2011, Antonioni et al., 2015, Argenti et al., 2016, van Staalduinen et al., 2017). Finally, the technological component of society is vulnerable to natural and human-made threats, whose effects are distinguished by high levels of uncertainty in prediction and limited examples of large-scale precursors upon which to draw (OECD, 2011). Because of the disruption of CI and essential services, events that are completely different in their nature, such as space weather and cyberattacks, may be able to trigger similar effects (Giannopoulos et al., 2012, UK Cabinet, 2015).

However, even when risk registers and national strategies make the appropriate considerations, the tendency is to separate the categories of risk, and to focus on the triggers that are perceived to be most likely to happen and considering static consequences rather than the possibility of scaling up secondary events into major disasters. Evidence shows that assessment processes are mostly based on probabilistic approaches (Giannopoulos et al., 2012), which may be the result of having only limited time series or may simply be ineffective in the case of complex events. This is in line with the approach proposed by Linkov et al. (2014), which highlighted the need for tools that are complementary to probabilistic risk assessment. These authors argued that quantitative risk analysis may be useful for 'foreseeable and calculable stress situations', while the evolving complexity of networks requires a better integration of resilience management.

It has been suggested that cascades may be associated with "black swans" or unknown, high-impact, low-probability events (Taleb, 2007), although this hypothesis has been treated with some scepticism. For example, Sornette (2009), who argued that extremes may appear more often than is generally expected. The power-law paradigm that is the basis of probabilistic risk assessment strategies may miss a population of events, defined as "dragon kings", which are characterized by amplifying mechanisms that are variable but may be analysed. Since its conception, this notion has been tested with evidence from complexity science in order to define its practical implications for risk assessment. Although capacity to predict trigger events remains limited, it has been demonstrated that cascade effects are most likely to develop in the weakest part of the system, where rigidities have accumulated.

According to Pescaroli and Alexander (2016), cascading disasters are distinguished by vulnerability paths, which result from the accumulation of unsolved weaknesses in society rather than from unexpected, unpredictable primary events. Thus, new preparedness and mitigation strategies should include the nodes that, are responsible for escalations, such as highly interconnected parts of CI, instead of concentrating merely on primary hazards such as floods. Our paper aims to develop this approach further, to provide a complementary view of existing risk assessment strategies and to suggest ways of increasing resilience to cascading events. Our hypothesis is that the technological component of critical infrastructure tends to accumulate rigidities that may be common to both natural and human-made risks. We focus on two triggers that are distinguished by high levels of uncertainty and low predictability.

Instead of using high-frequency threats, such as floods, that are well-known direct sources of loss of life and are considered routine by the emergency services, we focus on risks that can cause only indirect loss of life, such as extreme space weather and cybersecurity. We ascertain whether, despite the different nature of the triggers, there could be joint vulnerability paths that generate similar cascading escalations in the state of individual or compound risk drivers. We suggest that both extreme space weather events and well-targeted cyberattacks induce societies in highly-developed countries to be vulnerable to scenarios of Massive, Overwhelming, Disruption of Operations (acronym M.OR.D.OR.). Our goal is to point out which actions are needed in order to increase the flexibility management of response and resilience for these stressors and others that cannot be predicted with clarity.

In the following section, we develop this idea, assuming that cross-disciplinary studies are needed in order to characterise fast-evolving socio-technological systems and complex accidents (Rasmussen, 1997). We review the literature in order to develop a consistent process of scenario building, whose methodological building blocks can be found in the work of Alexander (2000, 2016). First, we define the role of CI in cascading events. Secondly, we proceed towards a vulnerability scenario and we apply the concept of vulnerability paths to extreme space weather and cyberattacks. For reasons of feasibility and clarity, we focus on the technological and organisational components of CI, while more detailed, rigorous analysis would also include the societal, economic, and institutional or "soft infrastructure" response. In conclusion, we formulate the M.OR.D.OR. scenario, discuss its practical implications and offer some open questions for future researches.

2. Critical infrastructure, networks and cascading events

The national definitions of CI and its sectors have changed in response to the complexity of the built environment and society, and changes in strategic needs (Lazari, 2014). The importance of some assets, such as aqueducts, has been known since Roman times, and has evolved in different phases of history, e.g. the protection of power plants during the Cold War (Setola et al., 2016). However, the possible impact of CI disruption is increasing considerably with the growing role of information technology, privatisation, urbanisation, and networked dependencies between services. In the late 1990s, the Clinton administration recognised this trend through Presidential Decision Directive PDD-63, which facilitates dialogue with nations such as Canada (Setola et al., 2016).

Some key events have pushed and pulled practitioners towards a new approach to CI protection, including the terrorist attacks in New York (2001), London (2005) and Madrid (2004), as well as major disasters such as the 2004 Indian Ocean Tsunami and Hurricane Katrina in 2005 (Lazari, 2014). Nowadays, it has been widely recognized that CI is a determinant of potential cross-border and cascading crises (Egan, 2007, Boin and Mc Connell, 2007, Ansell et al., 2010, Lazari, 2014, Setola et al., 2016). Loss of services and cascading failures can be unintentional and may be triggered, for example, by environmental hazards. Alternatively, it could be the fruit of intentional attacks on vulnerable interconnected networks (Wang et al., 2013). Work by Rinaldi et al. (2001) can be considered seminal in the evolution of this field. These authors suggested that forms of CI may interact according to their location in both geographical and cyberspace, their capabilities (e.g. pumping capacity), and their memory (e.g. degradation by use). They can be visualized in terms of the resources used (inputs) and the products created (outputs). CI evolves and reflects interaction with the whole system, in terms of its political, environmental, economic and social components (Rinaldi et al., 2001). In other words, the technological components cannot be separated from the human components that develop, manage and maintain them, as shown in Fig. 1. According to Little (2002), the functional linkages become tightly coupled in vulnerable nodes, in which different attributes are concentrated, as follows: (a) the hardware, such as transmission lines, servers and

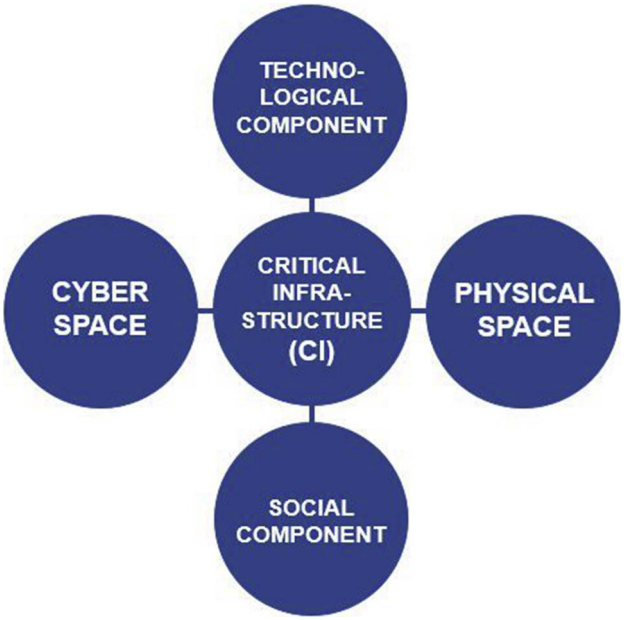

Fig. 1. Critical infrastructure as a node between cyberspace, physical space, technology and society.

satellites; (b) the software, such as information systems; and (c) the services provided, the public that uses them and the background determinants of decision making. However, sectors such as energy, telecommunication and transportation are not made up of self-standing assets. Instead, they are mainly connected to larger networks that are complex, dispersed and subject to multiple threats, such as natural hazards and terrorist outrages (Amin, 2002).

The development of CI in the built environment is associated with technological and managerial components that could generate cascading disruptions, even without a direct and evident physical connection (Hellstrom, 2007). Due to the complexity of their networks, smaller failures can recombine into cross-scale cascading events, thus increasing the impact of local disasters upon broader crises (Egan, 2007). Non-sequential effects and cascades are determined by shifting dependencies, which vary according to changes in the mode of operation that result from disruptions or failures (Nieuwenhuijs et al., 2008). This has very practical implications because infrastructure breakdowns go beyond the routine forms of contingency planning and emergency response. They require new strategies for coping with worst-case scenarios and training to facilitate cooperation across functional borders and hierarchical levels (Boin and McConnell, 2007).

A particular approach to CI disruption can escalate into secondary crisis that exceeds the original trigger and propagates emergencies in time and space, for example when localized floods damage a communications hub that serves a whole region (Pescaroli and Alexander (2015)). The non-sequential nature of this type of event can affect both the delivery of disaster relief and the coordination of emergency response. Pescaroli and Kelman (2017) compared three case studies in which international relief was deployed in highly-developed countries, and found that CI affected the supply of and demand for goods and expertise. The cascades generated by secondary emergencies were visible in the rapidity with which supply and demand were scaled up in response to the loss of services (e.g. meals ready to eat in response to lack of electricity). This also pertained to the hazardous component of CI (e.g. the supply of dosimeters in the face of nuclear meltdown). In order to understand these results, two different aspects must be considered: the direct effects of CI disruption in terms of the loss of services and function; and the indirect effects derived from the hazardous nature of the CI, such as environmental pollution or contamination (Alexander, 2013b). In the first case, the literature shows that accidents involving energy, telecommunications and Internet disruption are more diffuse than might be expected, and they can become drivers of cascades in other sectors (Luiijf et al., 2009, Van Eeten et al., 2011). Recent grants by the European Commission have supported the improvement of methodologies for assessing these aspects of cascades, in order to understand the interconnectivity and interdependencies among infrastructure types (e.g. Hassel et al., 2014).

CI disruptions also have indirect effects that may require specialised emergency efforts and are associated with vulnerable equipment in industrial and chemical facilities. On the one hand, researchers have considered the implications when natural hazards trigger technological accidents ('NaTech' events), which show how events such as floods, earthquakes and lightning can generate dispersion of toxic materials, contamination, fires and explosions (Krausmann et al., 2011). This has affected mitigation and planning strategies in different ways. For instance, in creating early warning systems, probabilistic hazard analysis has been applied with fragility curves of industrial equipment (Salzano et al., 2009). Probabilistic equipment failures and the recurrence of hazardous releases in risk-prone areas have been used to implement safety measures (Antonioni et al., 2015). On the other hand, the indirect effects of the disruption of chemical facilities can be caused by human-made threats and in particular terrorism. The possibility of attacks has been measured through functional risk assessments designed to integrate the likelihood of threats and potential losses (van Staalduinen et al., 2017), while new models have been created in order to define the performance of countermeasures and protection systems (Argenti et al., 2016).

Both direct and indirect effects of CI disruptions can spread a crisis across local, national and trans-national scales of space and jurisdiction, across short, medium and long timescales, and among the populations involved (Pescaroli and Alexander, 2016). Although CI failures can increase the pressure on the response system, the capacity to adapt to the evolution of crises may be limited by problems of coordination, competency, mobilisation and communication (Ansell et al., 2010). This is exacerbated by the fact that risk maps that include loss of CI and its impacts are generally unavailable or are not uniform because they separate natural and technological hazards or overlay them without taking heed of context (De Groeve et al., 2013). Even when innovative methodologies of CI risk assessment are considered, such as that produced by Kadri et al. (2014), attention remains focused on the sources of danger and the sequence generated after the failures, without including possible existing fragilities as variables. This is not necessarily wrong, but it could usefully be reinforced with complementary approaches. Helbing et al. (2015) suggested that the high variability of networks and the complexity of cascade effects may represent a real challenge to crisis management. These authors emphasise the need to increase the autonomy and adaptive capacity of all the components in the systems, and to influence planning and decision making with more equitable, decentralized approaches. The next section suggests how vulnerability paths and scenarios can be derived from the technological assets of CI.

3. Steps toward a vulnerability scenario for cascading events

The likelihood of worst-case scenarios associated with the interaction of compound events, interconnected risk, and cascading crises may be elucidated with three examples: the eruption of Eyjafjallajökull (2010), the triple disaster in Japan (2011), and Hurricane Sandy (2012).

In the first case, Eyjafjallajökull produced an ash cloud that shut down air transportation over 70 per cent of Europe (Alexander, 2013). The European authorities were unprepared for the event, having anticipated limited primary physical impacts in Iceland but not the escalation to the economic and social domains that depend highly on international mobility. This scenario saw the coincidence between volcanic activity and a north-to-northwest air flow from Iceland to

Europe, which is rare but recurs approximately 6% of the time (Sammonds et al., 2011). The lack of preparedness was one of the escalating factors in the crisis and, despite the existence of well-known precursors throughout the world, volcanic ash clouds were not included in the risk registers of many countries, including the United Kingdom (Alexander, 2013).

In the second case, the triple disaster that struck northeast Japan in 2011 involved one of the most prepared nations in the world and offers different levels of lessons to learn. The impact of the earthquake was limited by pre-existing mitigation measures, but it triggered a tsunami that caused approximately 18,000 deaths (National Diet of Japan, 2012). The vulnerability of national CI was a determinant in the scaling up of the emergency, as millions of citizens were left without vital supplies and relief was difficult to deliver without lifelines. The electricity transmission line between the Fukushima Dai'ichi Nuclear Power Plant and the national grid was severed by a small landslide caused by the tsunami, while the emergency diesel generators were directly damaged by the tsunami. This resulted in a nuclear meltdown that the authorities have recognized as a human-made disaster (National Diet of Japan, 2012).

Our third example is that of Hurricane Sandy in 2012, which struck an area that was rich in CI. The hurricane caused a storm surge on the coast but soon electrical power outages became the driver of another crisis, which in turn lasted up to two weeks and required the White House to take extreme measures, such as the use of oil reserves. An estimated 72 fatalities were directly associated with the hurricane, while another 50 deaths were estimated to be the result of the extended power outages and ensuing cold weather (Blake et al., 2013).

These cases show forms of interaction and compound risk, which tends to be amplified consistently by the vulnerability of CI. According to Perrow (1999), multiple-system accidents are inevitable in highly complex technological systems, and they can be triggered by unexpected interacting failures. This is especially the case in cascading events, where cross-scale vulnerabilities are accumulated in CI to the extent that they reveal pre-existing paths that become visible when the breaking points in social, political and ecological systems are aligned (Pescaroli and Alexander, 2016). Despite being unpredictable, those rigidities are well rooted in society's feedback loops, which can be exacerbated by practices of mismanagement and production pressure (negative feedback), or reduced by good practices and adaptation policies (positive feedback). Scenario building could help to increase the sharing of information on CI dependencies that are mostly known only to technical personal, such as engineers and facility mangers. Scenarios can identify escalation points that in complex events may lead to increased demand for assistance and coordination (Alexander, 2016). By way of example, some governmental actors in the UK have created a methodology that involves scenario exercises and aims to increase the awareness and information sharing on CI interdependencies in generic urban environments (Hogan, 2013). Even if the uncertainty levels of a non-sequential chain of effects remain elevated and hard to predict, the process may help to explore the concurrent, compound and cascading drivers of the escalation process. In the literature, there is widespread recognition of the importance of preparedness practices and planning in increasing the flexibility of responses and adopting good practices, even when experience is lacking (e.g. Kartez and Lindell, 1987). Scenarios have been used in teaching emergency management, in running exercises and in conducting national risk assessments because they can help "anticipate the unforeseen" and reveal possible impact and limitations inherent in sudden evolution of the emergency (Alexander, 2000). The "building blocks" of this process include the definition of the nature of the crisis, which constitutes a starting framework. They will require a rapid and reasoned reaction on the part of emergency managers. Hence, it is not surprising that a great deal of methodology has been developed to study the interaction of vulnerability and hazard.

Scenarios can be derived from past events, or they can explore hypothetical future risks and test capacity to define innovative strategies and new tactical approaches (Alexander, 2002). The first elements to define are the so called "boundary conditions", which propose the hazard input (e.g. a magnitude 7 earthquake) and the inputs of vulnerability (e.g. the building stock, aggregate patterns of activities, and so on). The scenario then proceeds through a series of stages, which can be used to identify emergency needs and the possible contingency planning parameters, thus providing a series of answers to the question "what could happen if…" (Alexander, 2002). Similarly, scenarios are one major tool to define connections between and among the various components of system, in particular the amplifiers that increase the risk for other components (OECD, 2011). This process is vital for threats whose impacts are distinguished by high levels of uncertainty, e.g. the sensitivity of high-tech infrastructure to geomagnetic storms and other forms of 'space weather' (OECD, 2011). Scenarios may benefit from the assessment of common vulnerability paths shared with unknown threats. If vulnerability is regarded as latent susceptibility of a system, it can be understood via the analysis of known risks and possible causal roots that are concentrated in the linkages between components of subsystems, such as those in the built environment (Birkmann et al., 2014). For instance, assessment of the vulnerability of CI can be accomplished through overall analysis of vulnerability, of the kind that determines the efficiency of the overall network, and by component analysis, as in the assessment of those nodes and edges that are the most crucial to the operational capacity of the system (Wang et al., 2013).

A complementary approach is the one suggested by Linkov et al. (2014), who proposed an operational matrix for assessing the resilience of critical infrastructure, including the physical, informational, cognitive and social domains. In this case, the technological components of CI have multi-dimensional and cross-cutting aspects that cannot be separated from the political and social implications of dealing with disruption or worse. Finally, it must be noted that the resilience of CI can also be interpreted as the ability of reliability experts to elaborate contingency scenarios as situations and challenges evolve, thus breaking through the barriers of formal design (Schulman and Roe, 2007). The technological and human drivers are deeply interrelated in the way that they determine the magnitude of possible failures. Because it represents the most advanced component of CI, space-based infrastructure can be used as an example of this bonding. The 1998 failure of the Galaxy IV satellite caused 80 per cent of digital pagers in the United States to go offline. It compromised ATM transactions, credit card authorizations, and cable and broadcast transmissions (Little, 2002). The current situation is that orbital infrastructure has become essential to communication, geospatial positioning, environmental monitoring, data linkages and defence, which raises concerns about its vulnerability to threats such as cyberattacks (Livingstone and Lewis, 2016). Emergency management itself cannot be immune to the problems of cascading effects where disruption affects ground-based infrastructure, especially since the 1990s tools that make use of satellite technology have become widely adopted (Alexander, 2000).

Information and communications technology (ICT) connects all disaster response systems, including emergency services and military command–control structures along with energy supply and transportation lifelines (Hellstrom, 2007). Nowadays, failure of the Internet and communications services have the potential to 'disconnect' the population from emergency response, holding back the delivery of information and guidance during major adverse events (Sommer and Brown, 2011). Because of reciprocal feedback, such complexities may accumulate fragilities in the relationship between packet transportation networks (PTNs) and the Internet, given that the Internet needs computer networking and PTNs need energy, satellite communications and cables. At the broader level, it has been suggested that the evolving role of technology has added new layers of vulnerability to CI, creating new challenges in maintaining balanced security efforts (Lazari, 2014). The following sections address the boundary conditions for extreme space weather and cybersecurity, respectively, which are then used to develop a common perspective on the discussion.

4. Boundary conditions: extreme space weather events

Space weather is the term used to describe changing ambient conditions in outer space that affect the Earth (Eastwood, 2008, Hapgood, 2010, Hapgood and Thomson, 2010). The Sun drives space weather, which varies with solar activity on a roughly 11-year cycle, usually tracked by counting the number of sunspots visible on the Sun. The maximum level of solar activity typically coincides with the largest number of sunspots visible on the Sun. The Sun drives extreme space weather in a number of ways, including solar fares, coronal mass ejections and geomagnetic storms:

(a) Solar flares are emissions of UV light, X-rays and particle radiation, typically over a period of minutes to hours.
(b) Coronal mass ejections (CMEs) are the explosive release of a large mass of the solar atmosphere at once. CMEs are often associated with sunspots and solar flares. Earth-directed CMEs that travel faster than 1000 km/sec take between 1 and 3 days to reach the Earth and push a shockwave in front of them that generates high-energy particle radiation.
(c) Geomagnetic storms are the response of the Earth's magnetosphere to rapid changes in pressure or magnetic field direction in the solar wind. The most extreme geomagnetic storms are caused when CMEs hit the Earth due to the very large changes in pressure and magnetic field driven by the CME. When a geomagnetic storm occurs, energy that has been stored in the Earth's magnetic field is released and causes the acceleration of ions and electrons to high-energies, which are stored in the radiation belts, and generates intense currents in the ionosphere.

Radiation from solar flares, CMEs and geomagnetic storms causes ionization and heating of the top layers of the atmosphere, disrupting radio communications and increasing the drag on low-altitude satellites, such as GNSS (Global Navigation Satellite System) and scientific mapping satellites, decreasing their lifetime in orbit. This radiation can disrupt GNSS service and satellite operations, harm astronauts, while some avionics equipment on board aircraft can suffer failures. Energetic particles in the radiation belts can as well damage satellites, disrupt the electronics on board and degrade the performance of solar panels reducing the profitability and performance of the satellites. Electrical currents generated in the ionosphere cause electrical currents on the ground via induction. These ground induced currents (GICs) travel through highly conducting material, if possible, which are typically high-voltage power lines, pipes, railways and other, metallic CI. The main risk associate with GIC is disruption of high-voltage electrical distribution networks in national power grids. The GIC enters and exits the grid via transformers and as it travels through these important CI nodes, causes the voltage cycle to drift outside the designed tolerance regime for the system. When this happens, eddy currents are generated in the transformer and half-cycle saturation can occur, heating the transformer core. This typically does not directly destroy the transformer, but can cause safety circuits to activate and disconnect the transformer from the grid. Thus, cascading blackouts can occur. There is some evidence that repeated heating via GIC that does not trip safety features reduces the operational lifetime of transformers. GIC may also cause the loss of phase-coherence across a large grid, also tripping safety features and potentially causing regional blackouts.

Extreme space weather is a newly recognized risk to human life and technology, having been added to the risk registers of the USA and UK over the last ten years (BIS, 2015, Fry, 2012). The risk is typically characterized as impacting technological CI, especially satellites, power transmission equipment and radio communications, and possibly disrupting global air transportation. Space weather affects the whole Earth and so can be considered a global phenomenon, but the most intense effects are localized to a region of a few hundred to a few thousand kilometres in size, typically in the high northern or southern latitudes. There are a number of documented historical cases of extreme space weather; all are thought to be due to very large geomagnetic storms caused by fast CMEs and very energetic flares. The first observation of such an extreme space weather event was in 1859 by Richard Carrington (Cliver and Dietrich, 2013), but subsequent events have been recorded roughly every ten years (Kilpua et al., 2015). The most recent extreme space weather events were a power blackout and damage to high-voltage transformers in Canada and the northeastern USA in 1989 and the loss of a satellite and interruption of service on many others during October and November 2003 (Kappenman, 2005). In the first case, a geomagnetic storm triggered a power outage of more than nine hours, which was exacerbated by the lack of availability of replacement parts and was contained with the voluntary reduction of power use by industrial sites, causing damages estimated at US$6 billion (OECD, 2011). Space weather has also been connected to damage to power transformers in South Africa (Gaunt, 2007), instabilities in power transmission lines over the USA (Forbes, 2012) and in Spain, and to air traffic control failures in Sweden and the USA.

The typical scale of these past events has been for power cuts to last about one day, radio communications disruption to last a few days and with satellite operations disruption every ten years (Dobbins and Schriiver, 2015). The literature provides much additional evidence of the cascading consequences of power failures and air travel disruption (Ansell et al., 2010, Alexander, 2013, Pescaroli and Alexander, 2015), but the primary impact of extreme space weather involves CI in outer space and the cybernetworks that they support. In particular, the consequences of inaccuracy or failure of GNSS have not been studied in great detail. GNSS receivers are now commonly found in all manner of devices, from mobile phones, to watches, cars, farming equipment, the avionics of aircraft and self-driving cars, aircraft autopilots and ship navigation. Some of these are thoroughly reliant on GNSS. It has been integrated into financial systems, as modern high-speed trading on the stock markets are timed by GNSS signals. A failure in GNSS, or a period of increased inaccuracy, could be caused by extreme solar flares, CMEs or geomagnetic storms (Cannon et al., 2013). The likely impact on these systems is unknown.

Each industry has a different approach to managing the risks of space weather (BIS, 2015). On the one hand, the satellite industry is the most aware of the issues because it is forced to react to these events more than are other CI providers, but the satellite industry tends not to share its knowledge or engage in dialogue with other sectors. On the other hand, the addition of extreme space weather to the National Risk Register in the UK in 2012 has meant that the National Grid and UK energy providers are improving their response plans. However, there is still much uncertainty about what could be the most cost-effective measures to promote. For example, the OECD (2011) suggested that for electricity generation companies and utilities it would not be economically sustainable to harden all transmission lines, but a possible strategy could be to focus efforts on the transformers between the generation facilities, and on the transmission grids, in order to increase the speed with which the network is restored.

To our knowledge, the risk of extreme space weather concurrent with another ongoing disaster or crisis has not been studied at all and could have important consequences. Air travel, satellite observations, GPS information and radio communications are all used to coordinate modern responses, and disruption to these services could potentially have important consequences for response to other emergencies. Although a compounding event of the intensity needed to provoke a cascading scenario must be considered infrequent, it remains in the range of plausible risk, and the ability to forecast it could be limited by the high uncertainty that is common in most long-term prediction of natural cycles. The likelihood that a space weather event will coincide with another disaster must thus be taken into account at the global level, as disasters and crises are a recurrent part of modern society and extremes are expected phenomena.

5. Boundary conditions: Cybersecurity issues

Cyberspace is more than the World Wide Web or the Internet itself. It is an “artificial dimension”, created by humans and made possible by the convergence of three “layers” (some say more): the physical layer, a logical (or syntactic) layer sitting above the first, and, sitting on top, a semantic layer (Libicki, 2009). The first, physical, layer is made of all the computers, cables, routers, and so on that support the rest. The logical layer contains the algorithms, protocols and software that, like the physical, make cyberspace function. Finally, the semantic layer displays the content, data and information that makes cyberspace meaningful for the vast majority of human users. It is fair to say that cyberspace is complex and puzzling and this is the result of the many projects that have created it, many if not most of which are independent of one another. The topology of cyberspace is also highly volatile, as ‘regions’ may appear or disappear on command or under attack from cyber- or conventional sources. Critical infrastructures are like the “nerves and blood vessels” of societies and their economies. Without them most social and economic activities would cease. They used to be mostly 'physical', but in the mid-1990s the private sector found out that it would be much more efficient to manage the infrastructures via computer networks, thus they became critical *information* infrastructures, which now extend across all three layers and are an indispensable element of cyberspace. Clearly, as large and complex systems, if they break down, they may provoke catastrophic effects (De Bruijne and Van Eeten, 2007, Hellstrom, 2007, Perrow, 1999). The list of critical information infrastructures may vary, depending on the country or institution considered, but they all tend to include banking and finance, transportation and distribution, energy, public utilities (gas, water, sewerage etc.), health, food supply, communications and key government services (Abele-Wigert and Dunn, 2006).

In cybersecurity, the literature is ample and tends to focus on lack of preparedness in advanced societies (e.g. Clarke and Knake, 2011, Schwartau, 1994). It also focusses on other issues (Giacomello, 2013), such as the motives for launching cyberattacks (Rid, 2013, Arquilla and Ronfeldt, 1993), and, last but not least, the impact of cyberattacks on vital public functions (Hellstrom, 2007). It is also recognised that only state-actors with their superior resources can engage in strategic cyberattacks, as only they have the capacity to seriously hamper their enemy's activities (Kaplan, 2016, Rid, 2013). In the case of an attack by a technically proficient state, there is not much the target can do, as attacks in Estonia (2007), Georgia (2008), Iran (2009) and Ukraine (2015) showed, but this is also rare, and it is outside the scope of the present paper. However, cyberterrorists could sabotage infrastructure as a ‘force multiplier’, which can boost the effects of, say, a conventional attack, such as blocking emergency services in order to elevate the number of victims of a car bomb (Matusitz and Minei, 2009). A cyber-'force multiplier' for terrorists offers opportunities for mitigation, although these have not been exploited significantly (Giacomello, 2004; Jarvis et al., 2014). At the risk of simplification, cyberwarrior states may have the resources and capacity to destroy the interconnected CI system of a target country, regardless of how they exploit cascading effects. Non-state actors with more limited resources, mostly terrorists but perhaps also anarchist “hacktivists”, may be drawn into causing a specific infrastructure to ‘crash’, which in turn may disrupt other CI, thus capitalising for their political goals on cascading effects as force multipliers. Given this distinction, it is not surprising that one of the earliest efforts in the United States to assess the vulnerability of CI, the Presidential Commission on Critical Infrastructure Protection, came to the conclusion that, because of growing complexity and interdependence, even “minor and routine disturbance can *cascade* into a regional outage” (Marsh, 1997 - emphasis added).

For non-state actors, the most disruptive course of action seems to be a focus on electricity, information and communications technologies (ICT) and possibly also on emergency services. As was quickly recognized for the first of these, “prolonged disruption in the flow of energy would seriously affect every infrastructure” (Marsh, 1997: 12). Chai et al. (2008: 269) demonstrated the primacy of electricity and ICT as “the most important critical infrastructures, in terms of their contribution to infrastructure interdependency, thus vulnerability.” The geographical scale and duration of interruptions of those CI would depend on a number of factors, but mostly on access to skills, finance and intelligence by the attackers. The more of this, the greater the damage. Portable EMP (electro-magnetic pulse) tools would probably be included. Nevertheless, the greatest assistance to attackers would come from the fragmented organizational structure of CI, which is not only divided between public and private sectors, but the latter is, in turn, made of different stakeholders who not always cooperate and sometimes, despite good intentions, may even compete with one another (Kaplan, 2016, De Bruijne and Van Eeten, 2007). In particular, the organization of cybersecurity in space lacks global coherence, and is distinguished by problems of communication regarding access to high-level classified information (Livingstone and Lewis, 2016).

Again, the GNSS is a key example of a CI asset in space that, if compromised, would disrupt services over large geographical areas. As the Global Positioning System (GPS) became the United States’ sole GNSS, it was thus almost inevitable that the exclusive reliance on it, combined with other complex interdependencies, would raise the potential for single point failure and cascading effects (Marsh, 1997: A19). As noted above, it is difficult to estimate the possible extent of an induced disruption, as many intervening variables may affect the outcome.

Nevertheless, we will consider energy grid disruptions in the United States over the last 15 years as examples of wide-spread disruptions. The data are openly available from various sources and give interesting insights.[1] Over that period, 20 per cent of disrupting events were attributed to physical and cybervandalism, which is the second most common cause of damage after severe weather. While it would clearly be wrong to associate this figure with one for cyberattacks, we should consider that it is only relatively more difficult to accomplish damage via cyberspace than it is by vandalism, but the former is far less risky for the perpetrators than the latter. These conditions make it necessary to include cyberattacks in the M.OR.D.OR. scenario.

6. Discussion: The M.OR.D.OR. Scenario

Although common vulnerability may exist in CI, extreme space weather events and cybersecurity have rarely been used together to build scenarios. In general, such events and factors can trigger similar cascading effects as those associated with CI disruption. They represent an indirect threat to life more than a direct one (OECD, 2011, UK Cabinet, 2015). Buckerfield de la Roche (2013) reported an attempt to create a dialogue on the common issues of outer space and cyberspace in two conferences held in 2012, which brought together specialists from 15 countries. As the vulnerability of space-based assets is increasing rapidly, better collaboration, cooperation and information sharing are required. New forms of governance are needed in order to cover the expansion of infrastructure, but there is some concrete risk that both outer space and cyberspace could be perceived as militarized, and that this could hamper if not reduce information sharing. Similarly, cyber-technology has an emerging value, is constantly updated and has multiple uses and purposes, which increases the risk that it will be treated inadequately in legislation (Livingston and Lewis, 2016). Despite early attempt to link extreme space weather and cybersecurity in policies on European CI, they remain largely without a perspective of common integration (Lazari, 2014).

Here, we argue that there is a link between cyber- and space weather risk by adopting the approach of vulnerability paths suggested

[1] See Jordan Wirfs-Brock, “Data: Explore 15 Years Of Power Outages”, Inside Energy, August 18, 2014 available from < http://insideenergy.org/2014/08/18/data-explore-15-years-of-power-outages/ > .

by Pescaroli and Alexander (2016). The technological nodes of CI accumulate fragilities in political, behavioural and managerial components that have common triggers that could escalate in cascading disasters. This should not be considered only in term of CI interconnectivity and interdependencies, but should also be dealt with in the practice of emergency management and planning.

The literature reported in previous sections suggested that common vulnerability paths exist in emerging technologies such as GPS and satellite infrastructure. In line with the model adopted by Hellström (2007), these are more likely to be vulnerable because they accumulate root causes and dynamic pressures that contribute to the creation and amplification of unsafe conditions in the intersection of information systems, human drivers and the physical components of CI. On the one hand, nothing excludes the very same components being vulnerable, simply because there is a lack of information sharing, to other known or unknown risks. On the other hand, the differences between the full breakdown of the system and the need to contain the scaling up could be inherent in the flexibility and adaptation capacity of the responders and of society. In other words, the problems related to the human component of CI, meaning political and managerial decision making, are likely to be affected in the same way if a high level of uncertainty and lack of information are not compensated for by training and preparedness strategies (Kartez and Lindell, 1987, Little, 2002, Boin and Mc Connell, 2007, Schulman and Roe, 2007, Ansell et al., 2010, Alexander, 2000, 2002, 2016).

In terms of scenario building, the vulnerability paths of both extreme space weather and cybersecurity define a type of scenario that we call Massive, Overwhelming, Disruption of Operations (acronym M.OR.D.OR.), as shown in Fig. 2. Here, the crisis could result from highly complex cascades that are triggered by threats, which are not fully appreciated by emergency managers and which escalate as they incorporate the technological components of CI (Amin, 2002, Little, 2002, Hellstrom, 2007, Boin and McConnell, 2007, Egan, 2007, Helbing, 2013, Alexander, 2016). In other words, both extreme space weather and cybersecurity could highlight vulnerable nodes in physical and cyber-dimensions that could be rooted in negative social feedback, such as production pressure on large-scale networks. The lack of (knowledge about) precursors could limit the capacity to react of the same decision makers, who may find themselves in a condition of high uncertainty. However, adopting the perspective of Sornette (2009), the worst case could be worse than what is expected. It could be possible that cascades driven by the technological components of CI could recombine with compounding dynamics such as those described by Leonard et al. (2014). A scenario in which an initial event of random intensity, such as a local or regional flood, happens to coincide with a technological based escalation remains possible. It has been suggested that shocks originating in the cyber-domain could be triggered by attacks on CI that happen during another crisis, and which could limit the capacity of technicians to activate protection measures (Sommer and Brown, 2011). The notion that cascading disasters could be the result of an accumulation of rigidities and cycles in different systems reinforces the need to integrate resilience management with risk assessment (Helbing, 2013, 2015, Linkov et al., 2014, Pescaroli and Alexander, 2016).

We present two example scenarios of the type of scenarios that fit in the definition of MO.R.D.OR.:

(a) In the first scenario, extreme space weather events or cyberattacks happen on their own and spread towards a technological network in physical space, as reported in official risk registers such as that of the UK Cabinet Office (2015). The existence of common vulnerability paths could be used to test the flexibility and adaptability of response to the highly uncertain escalation of secondary emergencies determined by CI disruptions, when the identification of the trigger could itself be a source of doubt that could shut down ordinary procedures (Pescaroli and Alexander, 2016). The development of a scenario for emergency management would focus on how to maintain the continuity of services, for example, in the case of the breakdown of vulnerable nodes, as in GPS failures, with a need to determine which actions should have priority in order to minimize the disruption of the social fabric. There are key issues regarding the role of shared knowledge about which sectors to concentrate on in recovery as a matter of priority. There also needs to be common legislation and policies that attribute roles and responsibilities, even when the scenarios carry a high level of uncertainty. This may be particularly relevant in the case of events that do not represent a direct physical threat to life, but which may result in indirect losses due to the escalating disruption of services.
(b) M.OR.D.OR. could potentially be considered a knock-down event in which emergency management is required to act against a

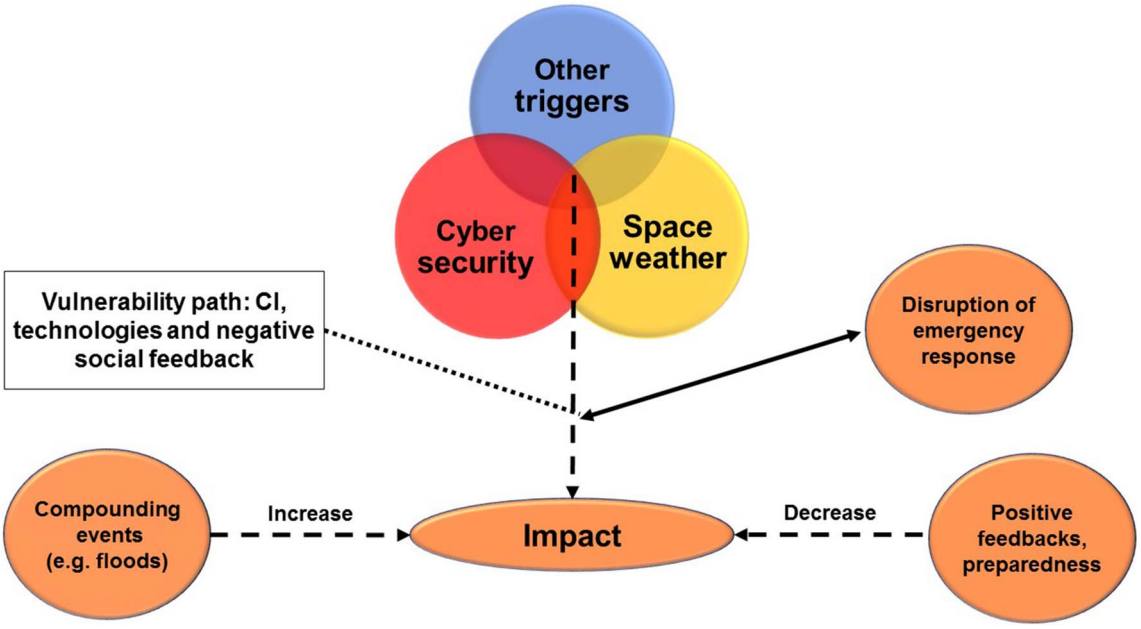

Fig. 2. Massive OveRwhelming disruption of OpeRations scenario.

well-known threat to life and also scale up processes in the cyber-dimension. In the case of extreme space weather, this stems from the coincidence of natural cycles of the sun, and earth dynamics, such as those described by Field et al. (2012). Alternatively, as noted by Sommer and Brown (2011), cybersecurity may result from well-targeted, human-made decisions. These may exploit rigidities, mismanagement or conflicting policies in the social domain. In both cases, scenarios focus on the conflicting needs of fast response to an initial, well-known emergency and the partial or total loss of the technological component of emergency response. We need to address the priority actions required to contain further scaling up, mainly by adapting tools and procedures to maintain basic operational capacity during a possible high-impact technological loss.

Clearly, both scenarios imply high uncertainty in the extension of service disruption through short, medium and long spatial and temporal scales. The testing of the scenarios should consider different levels of impact (local, regional, national and transnational). It should also be differentiated by the level of criticality of the disruption of CI with particular respect to interconnected and interdependent services. Better system design and management can have a strong influence upon the process (Helbing et al., 2015). The development of guidelines and training that could be used in adverse circumstances could also be of help. After the impact of the triggers, the worst escalation drivers could be related to the human dimension of mismanagement or to lack of training, which has been reported in the work by Rasmussen (1997), in research about high-reliability CI (Schulman and Roe, 2007), and in the frameworks for cascading disasters and interconnected risks. Similarly, as reported in Section 3, the potential impact on CI of external events could be reduced by improving the awareness of decision makers about the possible protection systems that are available and about the criteria for designing CI in a safer way.

In conclusion, it must be noted that M.OR.D.OR. is far from being an exercise in ‘crying wolf’. The very same conditions that occurred during the 2003 blackouts in Europe and northeast America might seem improbable if we merely change their trigger in the description of the scenario (Schulman and Roe, 2007). This episode highlighted the vulnerability of shipping to electronic interference through GNSS. It disrupted operations in several ports, and required personnel to go “back to basics” and do everything on paper (Saul, 2017). Something similar also happened in South Korea in 2016, when signals were jammed and hundreds of fishing vessels had to return to their ports (Saul, 2017). Moreover, in September 2017, the strongest solar flare in 12 years degraded radio and GPS communications on one side of the planet (Crane, 2017) while Hurricane Irma was challenging emergency services across the Atlantic coasts in the wake of Hurricane Harvey. (While there is at the time of writing no evidence that this complicated the deployment of relief, the hemisphere affected was the very same one.) M.OR.D.OR. might be a remote possibility, but history is full of low-probability, high-impact events that have happened in real life. In order to produce some clear answers about the possible levels of flexibility and adaptation in the response capacity, this scenario, we argue, should be developed and applied in real exercises with emergency managers and CI providers. We also argue that the opportunity costs of doing so, rather than spending the money on something else, have never been higher. The long-lasting problem of lack of information sharing and conflicting definitions of competencies could be revealed as something that is essential to address now (Boin and McConnell, 2007, Ansell et al., 2010).

7. Conclusions

This paper has suggested that the technological component of CI accumulates vulnerabilities which could be coincident between natural and human-made risks, and that this could be a source of escalation in cascading disasters. We analysed possible triggers, such as extreme space weather events and cybersecurity, and demonstrated that there are common vulnerability paths that can compromise or challenge emergency management and planning. This could be common to other triggers that are unknown, or at least highly uncertain, and that require increased flexibility in preparedness and response by means of improved training and scenario building. We have argued that the consideration of two different scenarios of Massive, Overwhelming, Disruption of Operations (acronym M.OR.D.OR.) could be used to improve organizational resilience. First, the trigger events could be regarded as happening on their own, as in, for example, solar flares or well-targeted cyberattacks. In this case, the focus should be on testing the capacity to respond to secondary emergencies which are caused by the failure of CI. Secondly, more attention should be given to compounding events that are normally considered unlikely to happen. This perspective could associate well known physical threats (e.g. floods) to other events that are less foreseeable or that maintain higher levels of uncertainty, involving, for example, cyberspace and communications and causing operational failure of GNSS. Scenario building can help to maintain operational capacity and reassess the priorities for response. It can increase the capacity of the response system to adapt and be resilient. In both the cases, as we have explained, the scenario escalates at different scales and to different levels of disruption, which could require priorities, resources and information sharing to be reassessed in order to maintain emergency capacity during crisis.

This work does not pretend to be exhaustive but aims to provide a preliminary application of a vulnerability scenario based on theoretical research on complex systems, such as that carried out by Sornette (2009), Helbing (2013), Linkov et al. (2014) and Pescaroli and Alexander (2016). Rather than a final product, it is an attempt to apply a new cross-disciplinary approach to the strategies designed to organise and prepare for cascading events. We recognise the existence of many limitations and hope that they will be investigated in the future. For feasibility reasons, we have focused on the technological component of CI. Although we have considered the social impacts and drivers of MO.R.DO.R., future research should develop the common paths associated with softer infrastructures that are part of the social fabric.

We currently lack a single answer to a very simple question: how likely is M.OR.D.OR. to happen? Where triggers such as high-impact extreme space weather events could happen at the same time as other natural hazards, cascading events must be expected to be infrequent, but this does not mean that such eventualities are impossible or are a case of 'crying wolf'. The problem may lie in how probability and risk are translated into preparedness strategies and policy making, which suggests that further studies are needed in order to find optimal training strategies for maximizing the complementarities of the different methodologies. Even if some of the literature suggests that current risk models could be insufficient to define probabilities in highly complex systems, a more refined answer could be given with the application of new dimensions, such as big data and neural networks. Moreover, because they are different in their root causes but similar in their possible escalation points, there are still unanswered questions about the differences between natural and human-made triggers and their dynamics.

It is perfectly possible that the evolution of cyberwarfare could lead the sort of situation envisaged by the M.OR.D.OR. scenario. There needs to be a common technique for defining escalation points and thresholds, one that is complementary to the scenario building process. Strategies for multidisciplinary resilience assessment of complex systems are promising here (Linkov et al., 2014). We need to determine the possible level of disruption that could be managed, in relation to both the capacity of local components and the overall level of interconnection among networks such as those that transmit electricity. In conclusion, for feasibility reasons, this paper does not include any analysis of the evolution of incidents, although this could be a useful tool for improving the understanding of such processes. Future research should better address how to reduce the vulnerabilities that are common to different threats. It should also model the evolution of the system and help maximize preparedness efforts before a triggering event. Ideally,

this could be used by industry and policy makers to develop more resilient components of CI, by recasting the most interconnected and fragile nodes in a more decentralized and sustainable way.

Acknowledgements

The work of Gianluca Pescaroli and David Alexander has been carried out under the aegis of the EC FP7 FORTRESS project, 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. Cross-disciplinary collaboration between the authors was supported by the UCL Knowledge Exchange Award and the UCL Institute for Risk and Disaster Reduction. A final acknowledgement is made to Matthew Dodd (UCL) for proposing some outstanding questions that were the primary inspiration for this paper, and to UCL Earth and Planetary Sciences Departments for helping us make an answer to these questions. We gratefully acknowledge the help of the guest editors of the special issue of the journal, and the feedback of Luca Galbusera (EU JRC).

Appendix A. Supplementary material

Supplementary data associated with this article can be found, in the online version, at http://dx.doi.org/10.1016/j.ssci.2017.12.012.

References

Abele-Wigert, I., Dunn, M. (Eds), 2006. International CIIP Handbook 2006 Vol. I: An Inventory of 20 National and 6 International Critical Information Infrastructure Protection Policies. Swiss Federal Institute of Technology, Zürich.
Arquilla, J., Ronfeldt, D., 1993. Cyberwar is coming!. Comparat. Strat. 12 (2), 141–165.
Alexander, D.E., 2000. Scenario methodology for teaching principles of emergency management. Disaster Prevention Mange.: Int. J. 9 (2), 89–97.
Alexander, D.E., 2002. Principles of Emergency Planning and Management. Oxford University Press, Oxford.
Alexander, D.E., 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, D.E., 2013b. Critical infrastructure. In: Penuel, K.B., Statler, M., Hagen, R. (Eds.), Encyclopaedia of Crisis Management. Sage, Thousand Oaks, California, pp. 208–211.
Alexander, D.E., 2016. How to Write an Emergency Plan. Dunedin Academic Press, Edinburgh.
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. Contingencies Crisis Manage. 18 (4), 195–207.
Argenti, F., Landucci, G., Reniers, G., 2016. Probabilistic vulnerability assessment of chemical clusters subjected to external Acts of Interference. Chem. Eng. Trans. 48, 691–696.
Antonioni, G., Landucci, G., Necci, A., Gheorghiu, D., Cozzani, V., 2015. Quantitative assessment of risk due to NaTech scenarios caused by floods. Reliab. Eng. Syst. Saf. 142, 334–345.
Birkmann, J., Kienberger, S., Alexander, D.E., 2014. Assessment of Vulnerability to Natural Hazards- An European Perspective. Elsevier, San Diego, CA.
Blake, E.S., Kimberlain, T.B., Berg, R.J., Cangialosi, J.P., Beven, J.L., 2013. Tropical cyclone report Hurricane Sandy (AL182012), 11–29 October 2012. National Hurricane Centre, Miami, Florida.
Boin, A., Mc Connell, A., 2007. Preparing for critical infrastructure breakdowns: the limits of crisis management and the need for resilience. J. Contingencies Crisis Manage. 15 (1), 50–59.
Buckerfield de la Roche, A., 2013. The merger of two global commons: the need for new governance. Space Policy 29 (2), 159–163.
Cannon, P., Angling, M., Barclay, L., Curry, C., Dyer, C., Edwards, R., Greene, G., Hapgood, M., Horne, R.B., Jackson, D., Mitchell, C.N., Owen, J., Richards, A., Rodgers, C., Ryden, K., Saunders, S., Sweeting, M., Tanner, R., Thomson, A., Underwood, C., 2013. Extreme space Weather: Impacts on Engineered Systems and Infrastructure. Royal Academy of Engineering, London.
Cliver, E.W., Dietrich, W.F., 2013. The 1859 space weather event revisited: limits of extreme activity. J. Space Weather Space Clim. A31, 2–15.
Chai, C.L., Liu, X., Zhang, W.J., Deters, R., Liu, D., Dyachuk, D., Tu, Y.L., Baber, Z., 2008. Social network analysis of the vulnerabilities of interdependent critical infrastructures. Int. J. Crit. Infrastruct. 4 (3), 256–273.
Clarke, R.A., Knake, R.K., 2011. Cyber War. HarperCollins, New York.
Crane, L., 2017. The Sun just belched out the strongest solar flare in 12 years. New Scientist, 06/09/2017, www.newscientist.com (accessed 08.09.17).
De Groeve, T., Annunziato, A., Vernaccini, L., Salamon, P., Thielen, J., San Miguel, J., Camia, A., Vogt, J., Krausmann, E., Wood, M., Guagnini, E., Giannopoulos, G., Pursiainen, C., Gattinesi, P., 2013. Overview of Disaster Risks that the EU Faces. European Commission, JRC Scientific and Policy Reports, Ispra.
De Bruijne, M., van Eeten, M., 2007. Systems that should have failed: Critical infrastructure protection in an institutionally fragmented environment. J. Contingencies Crisis Manage. 15 (1), 18–29.
Department for Business, Innovation and Skills, 2015. Space weather preparedness strategy. Version 2.1. Ref: BIS/15/457, www.gov.uk (accessed 04.10.16).
Dobbins, R.W., Schriiver, K., 2015. Electrical Claims and Space Weather Measuring the Visible Effects of an Invisible Force. Zurich Insurance Group Ltd., Zurich.
Eastwood, J.P., 2008. The science of space weather. Phil. Trans. R. Soc. 366, 4489–4500.
Egan, M.J., 2007. Anticipating future vulnerability: defining characteristics of increasingly critical infrastructure –like systems. J. Contingencies Crisis Manage. 15 (1), 1–17.
Field, C.B., Barros, V., Stocker, T.F., Dahe, Q., 2012. Managing the Risks of Extreme Events and Disasters to Advance Climate Change Adaptation: Special Report of the Intergovernmental Panel on Climate Change. Cambridge University Press, Cambridge.
Forbes, K.F., Cyr, O.C.St., 2012. Did geomagnetic activity challenge electric power reliability during solar cycle 23? Evidence from the PJM regional transmission organization in North America. Space Weather 10 (5), 1–14.
Fry, E.K., 2012. The risks and impacts of space weather: Policy recommendations and initiatives. Space Policy 28, 180–184.
Gaunt, C.T., Coetzee, G., 2007. Transformer failures in regions incorrectly considered to have low GIC-risk. IEEE Powertech Conference, 978-1-4244-2190-9, pp. 807–812.
Giacomello, G., 2004. Bangs for the buck: a cost-benefit analysis of cyberterrorism. Stud. Conflict Terrorism 27 (5), 387–408.
Giacomello, G. (Ed.), 2013. Security in Cyberspace: Targeting Nations, Infrastructures, Individuals. Bloomsbury Books, New York.
Giannopoulos, G., Filippini, R., Schimmer, M., 2012. Risk assessment methodologies for critical infrastructure protection. Part I: A state of the art. European Commission Joint Research Centre, Ispra.
Gill, J.C., Malamud, B.D., 2014. Reviewing and visualizing the interactions of natural hazards. Rev. Geophys. 52 (4), 1–43.
Gill, J.C., Malamud, B.D., 2016. Hazard Interactions and Interaction Networks (Cascades) within multi-hazard methodologies. Earth Syst. Dyn. 7, 659–679.
Hapgood, M., 2010. Towards a scientific understanding and the risk from extreme space weather. Adv. Space Res. 47 (12), 2059–2072.
Hapgood, M., Thomson, A., 2010. Space weather: it's impact on Earth and implications for business. Lloyds 360 Risk Insight, www.lloyds.com (accessed 16.06.17).
Hassel, H., Johansson, J., Cedergren, A., Svegrup, L., Arvidsson, B., 2014. Method to study cascading effects. CascEff project, D2.1, www.casceff.eu (accessed 16.06.17).
Helbing, D., 2013. Globally networked risks and how to respond. Nature 497, 51–59.
Helbing, D., Brockmann, D., Chadefaux, T., Donnay, K., Blanke, U., Woolley-Meza, O., Moussaid, M., Johansson, A., Krause, J., Schutte, S., Perc, M., 2015. Saving human lives: What complexity science and information systems can contribute. J. Stat. Phys. 158 (3), 735–781.
Hellström, T., 2007. Critical infrastructure and systemic vulnerability: towards a planning framework. Saf. Sci. 45 (3), 415–430.
Hogan, M., 2013. Anytown: Final Report [Internet]. London Resilience, London, www.londonprepared.gov.uk (accessed 16.06.17).
Jarvis, L., Macdonald, S., Nouri, L., 2014. The cyberterrorism threat: Findings from a survey of researchers. Stud. Conflict Terrorism 37 (1), 68–90.
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.
Kaplan, F., 2016. Dark Territory: The Secret History of Cyber War. Simon & Schuster, New York.
Kartez, J.D., Lindell, M.K., 1987. Planning for uncertainty: the case of local disaster planning. J. Am. Plann. Assoc. 53 (4), 487–498.
Kappenman, J.G., 2005. An overview of the impulsive geomagnetic field disturbances and power grid impacts associated with the violent Sun-Earth connection events of 29–31 October 2003 and a comparative evaluation with other contemporary storms. Space Weather, 3 (S08C01), pp. 1–21.
Khan, F.I., Abbasi, S.A., 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.
Kilpua, E.K.J., Olspert, N., Grigorievskiy, A., Käpylä, M.J., Tanskanen, E.I., Miyahara, H., Kataoka, R., Pelt, J., Liu, Y.D., 2015. Statistical study of strong and extreme geomagnetic disturbances and solar cycle characteristics. Astrophys. J. 806 (2), 1–7.
Krausmann, E., Renni, E.M., Campedel, M., Cozzani, V., 2011. 'Industrial accidents triggered by earthquakes, floods and lightning: lessons learned from a database analysis'. Nat. Hazards 59, 285–300.
Leonard, M., Westra, S., Phatak, A., Lambert, M., Van den Hurk, B., McInnes, K., Risbey, J., Schuster, S., Jakob, D., Stafford-Smith, M.A., 2014. A compound event framework for understanding extreme impacts. WIREs Clim. Change 5, pp. 113–128.
Lazari, A., 2014. European Critical Infrastructure Protection. Springer, London.
Libicki, M.C., 2009. Cyberdeterrence and Cyberwar. RAND Corporation, Santa Monica, CA.
Livingstone, D., Lewis, P., 2016. Space: The Final Frontier for Cybersecurity? The Royal Institute of International Affairs, Chatham House, London.
Linkov, I., Bridges, T., Creutzig, F., Decker, J., Fox-lent, C., et al., 2014. Changing the resilience paradigm. Nat. Clim. Change 4, 407–409.
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.
Little, R.G., 2002. Controlling cascading failure: understanding the vulnerabilities of

interconnected infrastructures. J. Urban Technol. 9 (1), 109–123.
Marsh, R.T., 1997. Critical foundations: Protecting America's infrastructures. President's Commission on Critical Infrastructure Protection (PCCIP). October, Washington DC, www.fas.org (accessed 04.10.16).
Matusitz, J., Minei, E., 2009. Cyberterrorism: Its effects on health-related infrastructures. J. Digital Forensic Pract. 2 (4), 161–171.
National Diet of Japan, 2012. The Official Report of the Fukushima Nuclear Accident Independent Investigation Commission, Executive Summary. The National Diet of Japan, Tokio.
Nieuwenhuijs, A., Luiijf, E., Klaver, M., 2008. Modeling dependencies in critical infrastructures. In: Goetz, E., Shenoi, S. (Eds.), Critical Infrastructure Protection, IFIP Series, vol. 253, pp 205–214.
OECD, 2011. OECD Reviews of Risk Management Policies, Future Global Shocks, Improving Risk Governance. Organization for Economic Co-operation and Development, Paris.
Perrow, C., 1999. Normal accidents. Living with high risk technologies. Princeton Paperbacks, Chichester.
Pescaroli, G., Alexander, D.E., 2015. A definition of cascading disasters and cascading effects: Going beyond the “toppling dominos” metaphor. Planet@Risk, Global Forum Davos, 3(1), pp. 58–67.
Pescaroli, G., Alexander, D.E., 2016. Critical infrastructure, panarchies and the vulnerability paths of cascading disasters. Nat. Hazards 82 (1), 175–192.
Pescaroli, G., Kelman, I., 2017. How critical infrastructure orients international relief in cascading disasters. J. Contingency Crisis Manage. 25 (2), 56–67.
Reniers, G., 2009. Man-made domino effect disasters in the chemical industry: the need for integrating safety and security in chemical clusters. Disaster Adv. 2 (2), 3–5.
Rasmussen, J., 1997. Risk management in a dynamic society: a modelling problem. Safety Sci. 27 (2/3), 183–213.
Rid, T., 2013. Cyber War Will not Take Place. Oxford University Press, Oxford.
Rinaldi, S.M., Peerenboom, J.P., Kell, T.K., 2001. Identifying, understanding, and analysing critical infrastructure interdependency. IEEE Control Syst. Mag. 21 (6), 11–25.
Sammonds, P., McGuire, B., Edwards, S., 2011. Volcanic Hazard from Iceland. Institute for Risk and Disaster Reduction. University College London, London. Available from: < www.ucl.ac.uk/rdr/documents > .
Salzano, E., Garcia Agreda, A., Di Carluccio, A., Fabbrocino, G., 2009. Risk assessment and early warning systems for industrial facilities in seismic zones. Reliab. Eng. Syst. Saf. 94, 1577–1584.
Schulman, P.R., Roe, E., 2007. Designing infrastructures: dilemmas of design and the reliability of critical infrastructures. J. Contingencies Crisis Manage. 15 (1), 42–49.
Setola, R., Rosato, V., Kyriakides, E., Rome, E., 2016. Managing the Complexity of Critical Infrastructures. Studies in Systems, Decision and Control book series, 90, SpringerLink.
Sornette, D., 2009. Dragon-kings, black swans and the prediction of crises. Int. J. Terraspace Sci. Eng. 2 (1), 1–18.
Schwartau, W., 1994. Information Warfare: Chaos on the Electronic Superhighway. Thunders Mountain Press, New York.
Van Eeten, M., Nieuwenhuijs, A., Luiijf, E., Klaver, K., Cruz, E., 2011. The state and the threat of cascading failure across critical infrastructures: the implication of empirical evidence from media incident reports. Public Admin. 89 (2), 381–400.
Van Staalduinen, M.A., Khan, F., Gadag, V., Reniers, G., 2017. Functional quantitative security risk analysis (QSRA) to assist in protecting critical process infrastructure. Reliab. Eng. Syst. Saf. 157, 23–34.
UK Cabinet Office, 2015. National Risk Register of Civil Emergencies. UK Cabinet Office, Whitehall, London.
Sommer, P., Brown, I., 2011. Reducing systemic cybersecurity risk. IFP/WKP/FGS(2011) 3, Organisation for Economic Cooperation and Development, Paris.
Taleb, N., 2007. The Black Swan: The Impact of the Highly Improbable. Random House, London.
Shaluf, I.M., 2007. An overview on the technological disasters. Disaster Prevention Manage. 16 (3), 380–390.
Saul, J., 2017. Global shipping feels fallout from Maersk cyber-attack. Reuters, 29/6/2017, www.reuters.com (accessed 30.06.17).
Wang, S., Hong, L., Ouyang, M., Zhang, J., Chen, X., 2013. Vulnerability analysis of interdependent infrastructure systems under edge attack strategies. Safety Sci. 51 (1), 328–337.