Organisation for Economic Co-operation and Development

GOV/PGC/HLRF/RD(2017)4

For Official Use **English - Or. English**

1 December 2017

PUBLIC GOVERNANCE DIRECTORATE
PUBLIC GOVERNANCE COMMITTEE

High Level Risk Forum

Critical Infrastructure Crisis Management

5-7 December 2017
OECD Conference Centre
Paris, France

This paper is presented in support of discussions in Sessions 7a and 7b, as well as Session 9. It is written by Professor Eric K. Stern, University at Albany and Swedish Defense University.

Jack Radisch; +33 1 45 24 18 03; jack.radisch@oecd.org

JT03424056

Critical Infrastructure Crisis Management

Executive Summary

1. Among the most developed countries, there is an increasing awareness of growing dependencies upon and vulnerabilities to disruptions of a number of key, interconnected infrastructure systems and their associated supply chains. Such disruptions tend to create chains of cascading consequences with profound effects on vital societal functions. While there are many potentially fruitful ways of approaching the challenge of identifying risks to such critical infrastructures and improving the resilience of critical infrastructure systems in highly developed countries, one potentially fruitful avenue is to view disruptions of critical infrastructure systems as strategic and operational **crises** involving diverse sets of actors and stakeholders including both governmental and non-governmental actors (Newlove et al, 2003; Boin and McConnell, 2007; c.f. OECD 2005).

2. Recent events—as well as many cases documented in the literature—clearly demonstrate the severe disruptions and domestic/international policy challenges associated with critical infrastructure crises. All three of the major US hurricanes of the fall 2017 season (Harvey, Irma, and Maria) involved profound and in some instances extremely prolonged disruptions of critical infrastructure systems including electrical power and fuel distribution, mobile communications and internet, food and water distribution systems, healthcare, and transportation.[1] These cases also provide vivid examples of cascading effects producing potentially devastating and even life-threatening downstream effects of critical infrastructure disruption. For example, storm-related disruption of the power grid and both primary and secondary cooling systems at the Arkema plant in Texas, created a secondary disaster when it became impossible to maintain safe temperatures for volatile chemical compounds stored at the facility, resulting in a series of uncontrolled explosions at the plant and the release of noxious and potentially toxic fumes .[2] Parallel, though perhaps more subtly deadly risks emerged in the health care system, as power and supply chain failures impacted hospital and nursing home functionality, critical care systems (e.g. dialysis for patients with kidney failure), pharmaceutical supply chains etc.

[1] See e.g. http://www.cnn.com/specials/us/hurricane-harvey http://www.cnn.com/specials/hurricane-irma ; https://www.theatlantic.com/science/archive/2017/10/what-happened-in-puerto-rico-a-timeline-of-hurricane-maria/541956/ for overviews.

[2] http://www.npr.org/sections/health-shots/2017/11/02/558313744/in-the-wake-of-chemical-fires-texans-worry-about-toxic-effects?sc=tw

3. Furthermore, the crisis approach is promising from a policy enhancement perspective for a number of reasons. Disruption of critical infrastructure systems are a common *consequence* of the occurrence of many other types of natural and "man-made" hazards and threats such as extreme terrestrial and space weather events, terrorism, major industrial or construction accidents, cyber-attacks on health care data systems[3] etc. In addition, they may arise from deliberate civil and system protection measures (e.g. protective shut downs in advance of extreme weather) and public reactions (crisis-related citizen usage surges can disrupt telecommunications systems, hoarding behaviors can disrupt supply chains, spontaneous or poorly planned evacuations can dangerously disrupt road transportation) as well as from the hazards themselves. Furthermore, major societal crises can be initially triggered due to processes and factors i*nternal to critical infrastructure systems* which cause them to fail, triggering a variety of secondary failures and disruptions of systems and societal functions linked to them. In fact, not only can disruption of critical infrastructure systems be either cause or consequence of crisis, but they can also serve as *crisis intensifiers* which can spread the crisis to additional domains, generate additional complex problem sets characterized by tensions among core societal values, proliferate uncertainty, and increase time pressures experienced by public, private, and non-profit sector decision-makers. Note that these intensifiers coincide with the components of a widely used and practically relevant definition of crisis which will be treated in more detail below.

4. Finally, explicitly considering major critical infrastructure disruptions from the perspective of crisis/crisis management enables the policymaker and analyst to draw inspiration from an extensive multi-disciplinary literature and the community of practice and expertise associated with the Strategic Crisis Management working group of the OECD High Level Risk Forum which has conducted a sustained and fruitful exploration strategic crisis management challenges and good practices in recent years (Baubion, 2013; OCED 2015 *The Changing Face of Strategic Crisis Management*). In fact, this working paper rests on two complementary pillars. The first is the results of an expert workshop held in Geneva in June 2017 as part of the Strategic Crisis Management Working Group process (see below).[4] The second pillar is the literature on strategic crisis management in general and managing critical infrastructure disruptions in particular. Some highlights of this literature will be presented below.

5. Not surprisingly in light of the above, many OECD countries—as well as regional actors like the EU-- have developed programs and practices designed to improve resilience of critical infrastructure systems.[5] In recognition of the importance of this work combined with awareness of significant room for improvement in this area, the OECD and the Swiss Federal Government arranged a workshop in Geneva June of 2017 to bring together government, private sector and academic experts in an effort to take stock of current knowledge and practices. A great variety of programmatic efforts, projects, case

[3] For an example of such an attack (on the UK National Health Service) , see https://www.theguardian.com/society/2017/may/12/hospitals-across-england-hit-by-large-scale-cyber-attack

[4] For documentation, see http://www.oecd.org/governance/6th-workshop-strategic-crisis-management.htm .

[5] Many of these efforts are summarized in the OECD *Toolkit for Risk Governance* https://www.oecd.org/governance/toolkit-on-risk-governance/home/

experiences, formats, and proposed good practices were presented. For example, participants were briefed on:

- The experience of the United States with regard to establishing partnerships for rapid restoration of critical infrastructure services and functionality.[6]
- Case studies of critical infrastructure failures and tools/technologies for improving critical infrastructure resilience and crisis management capacity including perspectives from Switzerland, the Netherlands, and the European Union (Joint Research Center).
- Governance challenges and good practices with regard to critical infrastructure crisis planning
- Partnership with critical infrastructure operators for rapid service restoration with perspectives and experiences from Sweden, Switzerland, Japan, and Korea.

6. In addition, a multi-stage interactive exercise session was held at the workshop. One part focused on identifying a set of emerging risks, hazards, and threats. That was followed by a more in-depth group-based scenario exercise focusing on transnational critical infrastructure crisis management—using an extreme space weather scenario as a point of departure.[7]

7. The rest of this report will be structured as follows. First, the notion of viewing critical infrastructure disruptions as crises will be presented and illustrated with a variety of examples. Second, five key tasks of crisis management will be explicated and discussed in terms of their application to the specific realm of critical infrastructure crises (Boin et al, 2005/2-16; c.f. Baubion, 2013). The concluding section of the paper will summarize the results from the literature and the Geneva Workshop of 2017 with regard to challenges and good practices for building resilience and *preparing* for critical infrastructure crisis management.

[6] See https://www.dhs.gov/critical-infrastructure-resources and https://www.oecd.org/governance/toolkit-on-risk-governance/goodpractices/page/uscriticalinfrastructureprotectionandresiliencetoolkit.htm

[7] Regarding the latter, see https://www.slideshare.net/OECD-GOV/prof-eric-stern-exercice-6th-oecd-workshop-on-strategic-crisis-management and the appendix to this paper.

1. Critical Infrastructure Disruption as Crisis

8. If one is to speak meaningfully about disruptions of critical infrastructure as crises, it helpful to apply an explicit crisis definition as the casual and policy usage of the term tends to vary widely across policy and academic contexts (and scholars) and can generate significant misunderstanding.

1.1. Crisis definition[8]

9. In light of the dramatic consequences of the various forms of critical infrastructure disruptions noted above, one can safely argue that-- though somewhat different in terms of the specifics of the direct and cascading effects involved-- by definition the disruption of **critical** infrastructure systems has the potential to spawn crises.[9] In fact, the adjective *critical* and noun *crisis* are related; one standard meaning of critical refers to being at or on the verge of crisis. [10]

10. From the perspective of policy decision-making a crisis may be usefully defined in terms of three subjective criteria perceived by strategic leaders (as well as by those for whom they are responsible): *threat, uncertainty*, and *urgency* (Rosenthal, 't Hart, and Charles 1989; Stern 2005; cf. Hermann 1963).[11] These criteria are not only helpful in distinguishing crises from other types of situations, but also provide a means for probing and preparing to act during them. The components of crisis will be introduced from a general perspective in the paragraphs below and then applied to the domain of critical infrastructure disruption in the following section.

11. First, crises are associated with *threats* to (and often potential opportunities to promote) the core *values* cherished by decision makers and/or their constituencies. These include among others human life, public health and welfare, democracy, civil liberties and rule of law, political autonomy, economic viability and public confidence in leaders and institutions. Leaders must also be prepared to cope with conflicts among such values (Farnham, 1997). The threat of terrorism, for example, entails potential conflicts between security considerations and civil liberties, as demonstrated by the post-9/11 debates on the Patriot Act, Guantanamo Bay, and more recently regarding electronic surveillance practices. Corresponding tensions can emerge with regard to potential public safety and health measures associated with other contingencies as well, such as quarantine restrictions in epidemics and mandatory evacuation orders in the face of hazards such as storms, wildfires, or toxic spills.

[8] The following four paragraphs have been adapted from Stern/OECD (2015:45).

[9] It is beyond the scope of this paper to take a position on exactly how to define the term critical infrastructure and determine which infrastructures should be regarded as critical. Definitions and attributions of criticality vary considerably and it has been suggested that some governments define the term so broadly that prioritization becomes problematic. See e.g. Riedman, David. "Questioning the Criticality of Critical Infrastructure: A Case Study Analysis." *Homeland Security Affairs 12, Essay 3 (May 2016).* https://www.hsaj.org/articles/10578

[10] https://www.merriam-webster.com/dictionary/critical

[11] For a critical discussion of the relative importance of these criteria, see Hermann and Dayton (2009)

12. Second, crises are associated with high degrees of *uncertainty* regarding the nature of the threat (i.e. the known and unknown unknowns), the contours of an appropriate response, or the possible ramifications of various courses of action. For example, the causes and manner of contagion of sudden acute respiratory syndrome (SARS) were not known during the initial outbreak in 2003 (Kleinman and Watson 2005). It was difficult for Chinese and Canadian authorities to deal with the public health challenges-- and the political, social, and economic consequences-- of this disease in the absence of such knowledge (Olsson and Lan eds, 2011). Some analysts distinguish between 'familiar' and 'novel' contingencies, when it comes to crises. All else being equal, the more familiar the contingency (and the more it conforms to scenarios used prior to the crisis as a basis for planning, training, and exercising), the more likely it is that crisis managers will face moderate levels of uncertainty and be working in the domain of structured problem-solving. The more unexpected and novel the event, the greater the uncertainty and the more ill-structured the domain in which crisis managers must operate. Coping with such novel contingencies and the cascading shocks associated with them makes the already difficult challenges of crisis sense- and decision-making even more demanding (c.f. Baubion, 2013).

13. Third, crises are associated with a sense of *urgency*. Events are perceived as moving quickly and there are fleeting windows of opportunity to influence their course. Effective, proactive intervention can minimize vulnerability (such as by getting citizens or mobile assets out of harm's way before a storm hits), and help to prevent or mitigate the impact of a potential threat (e.g. disrupting a terror plot or isolating carriers of a highly infectious disease). Additional time pressure stems from the relentless pace of the 24-hour news cycle. Strategic decision makers and their organizations must cultivate the capacity to diagnose situations and formulate responses under severe time pressure. Thus, crises force decision makers to make some of the most consequential decisions in public life under extremely trying circumstances.

1.2. Applying the Crisis Definition to Critical Infrastructure Disruptions

14. **Values**: The infrastructure systems we are concerned with in this paper are labelled critical for a reason. These are systems vital to sustaining life, health, welfare and functionality in highly developed societies and disruptions to them tend to have a dramatic and cascading impact on core societal values. Furthermore, policy decisions regarding managing the consequences of disruption and priorities as well as resource allocations with regard to system restoration involve (often competing) core values for societies and organizations. Political leaders and infrastructure operators face typical dilemmas with regard to protective shut down of systems. Proactively shutting down systems in the face of threat or hazard warnings can help to reduce exposure and avoid damage. For example, the U.S. civilian air transportation system was completely shut down in the wake of the 9/11 attacks. Similar preventative measures—with dramatic impacts on air-- and indirectly ground transportation-- were initially taken to reduce risk to air traffic stemming from volcanic dust during the eruption of the Icelandic volcano in 2010. However, it should be noted that such protective measures can cause severe disruption and post-decision controversy in and of themselves—especially if the potential threat triggering the measures does not materialize. Conversely, failure to take protective measures in the event of a major attack or destructive storm can expose government leaders and infrastructure operators to even more devastating liability and criticism. To take another example, for example, failure of the power grid can cause life and health-threatening consequences through impacts on food storage and preparation, hospital and

critical care functionality, traffic management, temperature (heating or cooling of indoor spaces) etc. Failure to maintain or rapidly restore service can negatively impact trust in government and in critical infrastructure operators alike (Newlove et al, 2003). To take another example, Cyber-attacks can cause severe financial and reputational damage to individuals and institutions as indicated by the cyber-attacks on the 2016 U.S. election and the Equifax data breach. Furthermore, as so called cyber-physical systems become more common and cyber-weapons more sophisticated, cyber-attacks are liable to cause material as well less tangible forms of damage and pose severe threats to human life as well as information security.[12] Finally, it should be noted that many disruptions also raise significant issues of justice, fairness, and liability with regard to the distribution of responsibility for costs or other negative consequences stemming from the direct and indirect impacts of critical infrastructure disruption.

15. **Uncertainty:** As in many other realms of crisis, uncertainties abound when it comes to critical infrastructure crises. These uncertainties typically stem from a number of sources. These include uncertainty about the impacts and trajectories of acute natural hazards or potential threats originating from human adversaries. For example, despite advances in hurricane modelling and healthy competition between European and North American modellers, it remains difficult to predict hurricane tracks with sufficient timeliness and accuracy to enable efficient evacuation—as the experience of Florida (USA) with Hurricane Irma clearly demonstrated. In that case, areas feared to be in danger were proactively evacuated, but the storm did not cooperate and some of the evacuated persons ended up leaving areas less affected by Irma and ended up in areas hit harder by the hurricane.[13] Other forms of uncertainty stem from inadequate understanding of system interdependencies and vulnerabilities. These can result in unanticipated pathways to failure and consequences of disruption. Further uncertainties stem from difficulties in predicting and coordinating responses of citizens and various non-governmental actors to warnings, safety recommendations, and protective orders. Will the issuance of an evacuation order lead to an orderly exodus from an urban area or prolonged gridlock that will cause an additional disruption of the transportation system and increase citizen exposure to a threat or hazard? For example, the Mayor Sylvester Turner of Houston chose not to emphasize proactive evacuation as a civil protection strategy for Hurricane Harvey due to concerns over these types of uncertainties.[14]

16. Similarly, other type of potential uncertainty has to do with how much cooperation and solidarity to expect from citizens, neighbours or partners (c.f. Gronvall, 2001; Boin et al, 2012)? Will a recommendation to households to make sure to have essential supplies lead to sensible preparations or exaggerated hoarding behaviours that disrupt supply chains? Will citizens respond to calls to conserve water or energy to an extent sufficient to mitigate an escalating crisis? How will neighbouring jurisdictions (municipalities, provinces or states, countries) respond to calls for assistance? Will they live up to obligations to provide mutual aid, assistance, and potentially scarce critical

[12] For an introduction to this issue, see https://www.dhs.gov/science-and-technology/csd-cpssec

[13] http://www.cbc.ca/news/world/hurricane-irma-florida-1.4282370 . For an introduction to hurricane modelling for the non specialist, see https://www.washingtonpost.com/news/capital-weather-gang/wp/2017/09/05/understanding-hurricane-forecasts-making-sense-of-spaghetti-cones-and-categories/?utm_term=.7338866469a2

[14] http://www.cnn.com/2017/08/27/us/houston-evacuation-hurricane-harvey/index.html

resources if they are facing a potential or actual threat—or intense domestic political pressure-- as well?

2. Time Pressure

17. Time pressure manifests in a number of ways with regard to critical infrastructure crisis management. First of all, there is often a "window of opportunity" for proactive protection measures such as a grid or transportation system shut down of the kind discussed above. As a threat or hazard is becoming more immanent, it may be possible to reduce exposure in various ways. For example, shutting down or reducing load on a power grid or satellite-based communications or navigation systems can reduce vulnerability to damage caused by extreme solar storms.[15] Similarly, heightening security or shutting down air or rail traffic in response in response to an acute terrorist threat (9/11, 7/7) or hazard (hurricane force winds or volcanic ash) can help to protect assets and/or users of the infrastructure systems in question. However, such opportunities tend to be time sensitive and may be fleeting. Other systems (such as some pharmaceuticals production and supply chains, nuclear power, and some chemical storage sites e.g. Arkema) may require continuous access to refrigeration, power, fuel or cooling water to maintain safe operations, creating intense time pressure to restore functionality should disruptions occur. Should deviations from normal functionality occur, there may be limited time to intervene in order to prevent accidents or other forms of cascading disruptions from occurring. Similarly, there may be limited time to attempt to influence public behaviors in ways that will protect systems or prevent disruption to critical infrastructures and supply chains (c.f. Holeguin-Veras et al, 2012). Efforts to get the public to conserve water (e.g. during the California drought) or power to protect vulnerable power transmission systems (e.g. Auckland, Outer Banks) are likely to involve considerable urgency. Finally, inquiries, criticism, and pressure from media (traditional and social), advocacy groups, opposition and competitor groups can create additional forms of time pressure and add additional time-sensitive tasks to the burdens carried by crisis managers.

18. Clearly contingencies involving critical infrastructure disruptions—whether as a triggering event or (potential) consequence of natural hazards, large scale accidents, or deliberate attacks—meet the crisis criteria proposed above. Note that these criteria can be easily turned into diagnostic questions that can help crisis managers make sense of events involving potential or actual critical infrastructure disruption (c.f Stern, 2009; OECD 2015):

- What values are at stake in this situation?
- What are the critical uncertainties and what can be done to reduce them?
- How much time is available for deliberation and decision-making?

[15] https://www.msb.se/Upload/Forebyggande/Naturolyckor_klimat/Solstormar/Space%20Weather%20and%20CI%20Summit%20FINAL.PDF

3. Crisis Management Tasks and Application to Critical Infrastructure Crisis

3.1. Core Crisis Management Tasks

19. Several decades of intensive empirical research on crisis management shows that leaders face recurring challenges when confronted with (the prospect of) community (or organizational/national/international) crises (Boin et al, 2005/2016). These are:

- sense-making,
- decision-making,
- meaning-making,
- ending and accounting,
- and learning and changing.

20. These tasks are germane to leaders and other crisis managers across sectors and are central not only to effective crisis leadership in a particular incident but also to creating better pre-conditions for future incidents and resilient adaptation to changing environmental conditions over the longer term. Hannah et al (2009 p. 902) drawing upon Leonard and Howitt (2007) suggest that different forms of leadership may be needed in different phases of a disaster or crisis. The following conceptualization identifies crisis leadership tasks likely to arise a variety of extreme events.

21. *Sensemaking* in crisis refers to the challenging task of developing an adequate interpretation of what are often complex, dynamic, and ambiguous situations (c.f. Weick; 1988; Stern 2015). This entails developing not only a picture of what is happening but also an understanding of the implications of the situation from one's own vantage point and that of other salient stakeholders. As Alberts and Hayes (2003) put it: "Sense-making is much more than sharing information and identifying patterns. It goes beyond what is happening and what may happen to what can be done about it." (p.102).

22. Making sense of critical infrastructure crises is a challenging task. As we have seen, uncertainties, ambiguities, with regard to threats, hazards, latent vulnerabilities as well as complex interdependencies within and among critical infrastructure systems make sense-making extremely difficult. Even when warnings are forthcoming—for example with regard to natural disasters such as hurricanes and flooding where monitoring and detection systems have improved significantly in recent years in many parts of the world—it is often very difficult to predict with confidence how particular critical infrastructures will be impacted or what the cascading effects of disruptions might be. This task is even more difficult with regard to novel, relatively unanticipated crises in which information and data-sharing networks and expert communities of practice may be underdeveloped and much of the sense-making work must take place on a relatively improvised basis. This was the case to a considerable extent during the Volcanic Ash Cloud crisis sparked by volcanic activity in Iceland in 2010 bringing commercial air traffic to a halt over much of Europe (Parker, 2014). for example. In such cases, difficult scientific and technical assessments with regard to "exotic" issues must be produced and communicated to governmental and other key decision-makers under crisis conditions. In many countries this still occurs largely on an ad hoc basis, though others such as the UK

have developed (or are in the process of developing) Scientific Advisory Groups for Emergencies [SAGE].[16]

23. A first step in making sense of a critical infrastructure crises is to identify key public, private, and non-profit actors and stakeholders and gather information via various forms of (social and technical) networks associated with or connecting across critical infrastructure sectors. Many highly developed countries have or are in the process of developing strategies and collaborative fora to improve critical infrastructure protection and resilience. Such efforts, hopefully undertaken well before the onset of a crisis can improve the flow of information, contribute to improved situational awareness, and facilitate "heedful inter-relating" and other forms of crisis management cooperation among diverse sets of actors involved in governing, operating, or using critical infrastructures.[17] Making sense of critical infrastructure crises is, of course, facilitated by deeper and more dynamic understanding of systems and cross system-interdependencies. As a result, efforts to improve technologies for mapping, modelling, simulation, and visualization of such systems can contribute not only to system design improvements to improve resilience and reliability but also to capacity for crisis management and rapid restoration.[18] [This issue will be discussed further in the final section of this paper.] Another promising development—to the extent that communications and mobile data networks remain available—for improving situational awareness in critical infrastructure crisis is citizen crowdsourcing. Armed with smartphones and web and geographic information system (GIS)-based platforms for aggregating, analyzing, integrating and transposing data, citizens as well as various forms of organized official or unofficial responders can act as sensors (Stern, 2017; Akghar, Staniforth, and Waddington eds. 2017).

24. *Decision-making* refers to the fact that crises tend to be experienced by leaders (and those who follow them) as a series of 'what do we do now' problems triggered by the flow of events. These decision occasions emerge simultaneously or in succession over the course of the crisis (Stern, 1999; Newlove et al, 2003; Stern et al 2014). Coping with critical infrastructure disruptions and managing the restoration process tends to require an interdependent series of crucial decisions and to be taken in a timely fashion under very difficult conditions by a variety of public, private , and non-profit sector actors and stakeholders. Note that governance arrangements may vary significantly across highly developed countries with regard to extent of public control, regulation and ownership of critical infrastructures.

25. It is important to keep in mind that decisions in critical infrastructure crises will by definition be be taken under highly stressful conditions of considerably uncertainty, time pressure, and threat to core societal and organizational values, as noted above. Furthermore, conflicts among values are to be expected, contributing further to the decisional stress load facing decision-makers (c.f Lebow and Stein, 1994).

[16] For an overview of this challenge and discussion of emerging good practices based on the results of a workshop hosted by OECD and UK Met, see https://www.wiltonpark.org.uk/wp-content/uploads/WP1564-Report.pdf

[17] See the OECD Risk Governance Tool kit for numerous examples of such efforts in the OECD countries.

[18] See the power point briefing from the European Joint Research Center (Giannoupolous) https://www.slideshare.net/OECD-GOV/dr-georgios-giannopoulos-jrc-6th-oecd-workshop-on-strategic-crisis-management

26. It may be helpful to consider typical examples of the kinds of decisions that are likely to arise in the context of a critical infrastructure crisis. Taking a threat/disruption to electric power infrastructure as an example, the following are just some of the very difficult crisis decisions that may be required (Newlove et al, 2013; Parker et al, 2009; Nye, 2010):

- Decisions to issue warnings regarding threats, hazards, and possible power grid disruptions and/or their consequences.
- Decisions to order protective shutdowns to protect system components (e.g. power generation or transmission) or prevent unsafe or unduly risky operations under conditions of acute threat or mounting natural hazard.
- Decisions to request or order mandatory power conservation to prevent further degradation of the power system.
- Decisions regarding how to allocate drastically reduced supplies of power and scarce repair capabilities and resources.
- Decisions regarding requesting, providing or accepting mutual aid (e.g. in the form of components or repair crews from other regions of the country and/or from other countries).
- Decisions regarding provision of financial resources for response and recovery, and/or accepting financial responsibility for the direct and indirect costs and consequences associated with outages and restoration.
- Decisions regarding public health and safety measures (food safety and pharmaceuticals interventions for compromised refrigeration, decisions regarding hospital continuity of service) necessitated by power outages etc.).
- Decisions regarding civil protection measures—e.g. evacuation orders or instruction to shelter-in-place, curfews-- for populations potentially endangered by consequences of power outages and supply chain disruptions and/or the hazards and threats which triggered them.
- Decisions regarding measures for restoration and recovery, some of which may conflict with normal rules, practices and procedures for building planning and permission, environmental protection, etc.

27. Thus decision-making in critical infrastructure crises, as in other types of crisis events, is extremely difficult and demanding.

28. *Meaning-making (and crisis communication)* refers to the fact that leaders—from public, private, and non-profit sectors alike—must attend not only to the operational crisis communications challenges associated with a contingency, but also to the ways in which various stakeholders and constituencies perceive and understand it. Because of the emotional charge associated with disruptive events, followers look to leaders to help them to understand the meaning of what has happened and place it a broader perspective. By their words and deeds, leaders can convey images of competence, control, stability, sincerity, decisiveness, and vision—or their polar opposites.

29. Critical infrastructure crises can pose unique challenges with regard to crisis communication in general and meaning-making in particular. First of all information and communications technology-- and critical infrastructures which support them-- may be directly affected by the impact of accidents, natural hazards or attacks associated with the crisis. Extreme earth (windstorms, floods) and space weather (e.g. solar storms) events as well as physical and cyber-attacks can disrupt the capacity to communicate via both wired and wireless communications networks for shorter or longer periods. In addition, many types of events (again including both deliberate attacks, major accidents, and natural

hazard based events) may be associated with increased citizen and responder communications traffic to the extent that vulnerable communications networks may fail or have severe degradations with regard to access, reliability, or quality of communications. As a result, crisis managers may have difficulty in sending and receiving messages and sharing data when ability to do so matters most.

30. For example, during prolonged summertime power outage in Auckland, New Zealand in 1998 , the normal press briefing facilities (among other key functions and coordination centers for city government) were unusable due to high temperatures and lack of functioning elevators. As a result, Mayor Les Mills ended up conducting much of his business and media interviews from his car and mobile phone from various locations around the city, which complicated the coordination of operations and messaging. The power company, Mercury Energy, responsible for the outage was kind enough to offer the Mayor the use of their press briefing facilities which had functioning power and communications. Unfortunately for the Mayor, this also entailed giving his briefings from a podium boldly displaying the logo of what was at the time a very unpopular critical infrastructure operator. This served to symbolically associate the Mayor with the power company at a time when a degree of critical distance would have served him better politically. It should be noted that he lost the next election, in part due to what some regarded as a subpar performance in critical infrastructure crisis management (Newlove et al, 2003).

31. Hurricane Maria in Puerto Rico in the fall of 2017 is another excellent example. Vulnerable communications and electrical power networks, already battered by Hurricane Irma, were devastated by Hurricane Maria. As a result, much of the response and early recovery effort took place under particularly challenging conditions and large portions of the stricken island remained without power and electricity as not only days but weeks passed. Use of modular cellular technologies (so called cells on wheels, or COWS) were helpful in restoring communications in certain urban or or other particularly sensitive areas, but were insufficient to restore communications capacity for the bulk of the island.[19] Degraded communications capacity can limit the ability of communities to self-organize and coordinate citizen-based efforts to respond to and recover from disasters using social media and smart communications technologies—an increasingly important dimension of resilience in large scale events (Stern, 2017; Akghar et al, eds, 2017).

32. Hurricane Maria also contains good examples of the ways that leaders at various levels of government engage in competitive attempts to demonstrate empathy and engagement as well as endeavoring to shape the narratives and public perceptions of the event. While President Trump and acting Secretary of Homeland Secretary Elaine Dukes suggested that the response to Maria was effective and a "good news story", the Mayor of San Juan Carmen Yulin Cruz appeared on CNN wearing a black T-shirt with the text "We are dying" creating vivid images that went viral via social and traditional media far beyond the island. Similarly, the tone set by President Trumps combative approach to crisis communication—which included sharp criticism via Twitter of the leadership of Mayor Yulin Cruz and allegations that the Puerto Rican locals were not doing their part with regard to response and recovery—proved highly controversial. [20]

[19] https://blog.npstc.org/2017/10/05/85-of-cell-sites-down-in-puerto-rico/

[20] http://www.cnn.com/2017/09/30/politics/trump-tweets-puerto-rico-mayor/index.html ; http://www.cnn.com/2017/10/03/politics/donald-trump-paper-towels-puerto-rico/index.html ;

33. *Ending and Accounting* refers to the non-trivial task of finding the appropriate timing and means to end the crisis, manage accountability processes, and return to normalcy. Furthermore, attempting to end a crisis prematurely can endanger or alienate constituencies who may still be in harm's way, traumatized, or otherwise continue to be politically or emotionally invested in the crisis. Crises may be particularly difficult to terminate if the operational challenges lead to a so-called *crisis after the crisis* in which serious recriminations—resulting in losses of trust and legitimacy-- are launched against those who failed to prevent, respond to, or recover effectively from a negative event.

34. Critical infrastructure crises, like other forms of crisis, may have different trajectories and different combinations of operational and legitimacy dimensions. Some are "sudden onset" in which a dramatic event such as an earthquake or hurricane causes dramatic damage. Others may demonstrate a "creeping" quality whereby a threat slowly manifests or the functionality of a critical infrastructure slowly degrades for a prolonged period before attracting notice. The water crises which have impacted many cities around the world—from places as diverse as Mexico City and Flint, Michigan and Hoosick Falls, N.Y.—are good examples of vulnerabilities mounting as a result of environmental change, rapid population growth and development, industrial pollution, or unsafe properties of aging infrastructure installations (use of lead pipe in water distribution systems) etc.[21] Similarly, some critical infrastructure crises demonstrate rapid and effective restoration of the pre-crisis *status quo,* while others may exhibit prolonged disruptions of functionality and/or morph into legitimacy crises after the crisis (c.f. Fishbacher-Smith, 2006; Boin et al, 2010). When it comes to critical infrastructure crises, such legitimacy crises may focus on questions such as:

- Why were vulnerable and/or potentially dangerous critical infrastructure systems or components allowed to be used?
- Why were safety margins and measures not more robust?
- Why were safer and/or more reliable alternatives to the failed or vulnerable technologies not used?
- Why were "known" risks and vulnerabilities not addressed more proactively and promptly before and/or during the crisis?
- Why were leaders not more focused on the crisis issue and why did they not provide stronger, more empathetic, and/or more effective leadership?
- Why wasn't the response better coordinated, better resourced, more proactive, more effective, more fair etc?
- Why was the restoration and early recovery not faster, cheaper, more effective and more complete?

35. Why were some groups in society advantaged or disadvantaged (prioritized or neglected) in terms of response and recovery efforts.

36. Note that these issues are likely to arise in multiple accountability fora: parliamentary bodies, professional or industry associations or governance bodies, regulatory agencies, courts, and the media. Furthermore, crisis experiences and their

https://www.washingtonpost.com/news/post-nation/wp/2017/10/06/in-puerto-rico-trumps-paper-towel-toss-reveals-where-his-empathy-lies/?utm_term=.c0f8374c0ae1

[21] See e.g. http://www.nejm.org/doi/full/10.1056/NEJMp1601013#t=article ; https://www.nytimes.com/2016/08/31/nyregion/hoosick-falls-tainted-water-hearings.html ; https://www.nytimes.com/interactive/2017/02/17/world/americas/mexico-city-sinking.html

associated accountability processes may profoundly challenge and in some instances destabilize establish practices and patterns of governance (including regulation and divisions of authority and responsibility across sectors and levels of government) with regard to managing critical infrastructure sectors. When critical infrastructure operators and industries are perceived to have been—or determined in a court of law to have been—negligent, strong pressures for change and significant legal and financial liability for operators and other private sector actors may emerge. This can take the form of proposals for increased regulation, incentivizing safety and resilience, heightened operator responsibility for damages, or even withdrawal of the 'permissive consensus" that allows potentially hazardous activities such as nuclear power or process industries involving potentially dangerous chemicals to continue. The Fukushima nuclear accident stemming from the Great Tohuko earthquake and Tsunami (which was another case emphasized in the Geneva Workshop presentations)[22] is a good example, with profound repercussions for the nuclear power industry even in countries on the other side of the world such as Germany (Bernardi et al, 2017).

37. Note that the highly complex systems of critical infrastructure governance entailing various forms and degrees of regulation and legislation, diverse patterns of ownership, different varieties of public-private partnership in place in many countries have profound implications for accountability with regard to critical infrastructure disruption/restoration and crisis management (c.f. Dunn Cavelty and Suter, 2009. Awareness of and outcomes from previous accountability processes should inform preparedness, response, recovery, and post-crisis efforts towards learning and reform (which will be discussed in more detail below).

38. *Learning and changing* requires an active, critical process which recreates, analyzes, and evaluates key processes, tactics, techniques, and procedures in order to enhance performance, safety, capability etc. The learning process has just begun when a so-called lessons learned document has been produced. In order to bring the learning process to fruition, change management / implementation must take place in a fashion that leaves the organization with improved prospects for future success (Boin et al, 2016; Deverell and Olsson, 2009; Stern et al, 2014; Stern, 2015). Note that political and organizational cultural obstacles and various forms of disincentives often prevent effective learning and change from taking place (Stern, 1997).

39. Critical infrastructure disruptions-- like other forms of crisis—provide unique chances for learning and opportunities for change. Latent or unrecognized vulnerabilities and interdependencies manifest themselves in dramatic fashion, providing opportunities for redesign and reform of technical systems, institutional frameworks, tactics, techniques and procedures etc. The abrupt manifestation of urgent and difficult problems can stimulate creative improvisation, new forms and constellations of collaboration and innovation. However, taking advantage of these opportunities requires reflection, inquiry, leadership and resources to identify adaptive lessons (c.f. Heifetz and Laurie, 2001) and translate them into more resilient, reliable effective and legitimately functioning systems for critical infrastructure and crisis management.

40. Hurricane Sandy—which was emphasized in a number of the Geneva presentations—serves as a vivid example:

[22] For T.Okada's briefing on "Infrastructure and Public Service Recovery from Natural Disasters in Japan" see https://www.slideshare.net/OECD-GOV/tomoyuki-okada-japan-6th-oecd-workshop-on-strategic-crisis-management

> *Sandy, the second-largest Atlantic storm on record, affected the East Coast from Florida to Maine, as well as states as far inland as West Virginia, Ohio, and Indiana. The storm made landfall in southern New Jersey on October 29, 2012, battering the densely populated New York and New Jersey region with heavy rains, strong winds, and record storm surges. The storm's effects were extensive, leaving more than 8.5 million customers without power, causing widespread flooding throughout the region, and contributing to acute fuel shortages in parts of New York and New Jersey. The storm damaged or destroyed hundreds of thousands of homes, caused tens of billions of dollars in damages, and killed at least 162 people in the United States.*[23]

41. As noted in the preceding quote, the storm caused severe damage and disruption to multiple critical infrastructure systems in New York and New Jersey including transportation[24], energy (electric power and fuel distribution), water and water systems[25], and provision of health care. Numerous points of vulnerability and challenging problems emerged ranging from the vulnerability of the subway system and the cable installations servicing it to flood damage, cascading interdependencies between electric power and various nodes in the fuel distribution network, and fragility of hospital power backup systems in the face of massive storm surge and flooding (e.g. NYC Langone Medical Center evacuation).[26] Following Hurricane Sandy there have been a large number of after-action reports, inquiries, and research studies about various aspects of the crisis, response, and recovery associated with it. Many of these efforts have focused on or significantly involved critical infrastructure functions and actors and a variety of important lessons have been learned and changes made.[27]

42. At the time of writing (late fall 2017), the experience of the Atlantic Hurricanes of 2017 has not yet been systematically processed via a post-crisis multidimensional after action and research effort of the kind which took place for Hurricane Sandy and some previous major Atlantic storms (e.g. Katrina). The preliminary indications are that important lessons were learned from Sandy and previous cases which informed the proactive crisis management by many governmental actors and critical infrastructure operators with regard to response and restoration efforts with regard to Hurricane Harvey and Irma. However, the much more problematic response and delayed restoration of

---

[23] FEMA (2003) p.iii https://www.fema.gov/media-library-data/20130726-1923-25045-7442/sandy_fema_aar.pdf

[24] For a study of impacts on transportation during and after Hurricane Sandy, see Kaufman et al (2012) available at https://wagner.nyu.edu/files/rudincenter/sandytransportation.pdf

[25] American Waterworks and Wastewater Association WARN (Water and Wastewater Response Network) https://www.awwa.org/Portals/0/files/resources/water%20knowledge/rc%20emergency%20prep/rc%20warn%20situation%20reports/SandyAAR2013.pdf

[26] http://www.nytimes.com/2012/10/30/nyregion/patients-evacuated-from-nyu-langone-after-power-failure.html

[27] See e.g. the integrated New York City report http://www.nyc.gov/html/recovery/downloads/pdf/sandy_aar_5.2.13.pdf ; the integrated FEMA after action report https://www.fema.gov/media-library-data/20130726-1923-25045-7442/sandy_fema_aar.pdf ; U.S. Department of Energy after action report https://energy.gov/sites/prod/files/2013/05/f0/DOE_Overview_Response-Sandy-Noreaster_Final.pdf

critical infrastructure services (e.g. power, fuel, telecommunications, water) to Hurricane Maria in the U.S. territory of Puerto Rico is instructive. Clearly resilience and preparedness for critical infrastructure crisis management can develop in an uneven fashion even in highly developed countries, leaving pockets of particular resilience and particular vulnerability. Contextual factors such as geographic centrality/remoteness, regional economic strength, and robustness or fragility of particular infrastructures, functionality of local governance, coincidence with other simultaneous or near simultaneous events, and not least political will can all impact on response and recovery.

43. While effective production and adaptive implementation of "lessons learned" is very challenging, failure to learn from experience is a recipe for stagnation and perpetuation of vulnerability which may be extremely costly in humanitarian, political, and financial terms for the key actors involved in the governance and operation of critical infrastructure systems. (Boin et al, 2016; Boin and McConnell, 2007).

4. Conclusion: Preparing for Critical Infrastructure Crisis Management

44. Having explored the five crisis management tasks discussed in the previous section, let us conclude this paper by suggesting that a key additional imperative is the broader task of *preparing* for crisis management (Stern, 2013; Boin et.al 2016: chapter 7).

45. *Preparing* refers to the task of creating pre-conditions and dispositions which facilitate collaborative effort as well as effective and legitimate intervention when crises occur as well as during their aftermath. Elements of preparing include activities such as organizing, networking, planning, training and exercising. This generally entails attempting to identify key players and roles likely to be required for effective societal or community response and making sure that each role-player is capable of enacting that role skillfully and in a fashion conducive to not just particularistic but also collective community success. Leadership with regard to this task has a key motivational component—preparedness requires investments in time and resources which compete with other priorities in times of "peace". Ironically, when a crisis is imminent, such as when meteorological experts predict that a hurricane is on its way, motivation tends to be high. However, in such acute preparedness efforts in the face of an escalating event, though the will to prepare may be high, difficult dispositions must be made under crisis-like conditions of uncertainty, time pressure and resource scarcity.

46. On the basis of the literature reviewed above and the results of the Geneva Workshop of June 2017, it is possible to identify a number of target areas for improvement and good practices with regard to improving preparedness and capacity for critical infrastructure crisis management and rapid restoration in the wake of critical infrastructure disruptions in highly developed countries. These include:

- Improving international cooperation and joint-management of critical infrastructure systems.
- Building trust and relationships in support of crisis management across the public, private non-profit divide

- Improving knowledge and understanding of critical infrastructure systems through mapping, modelling, and simulation.
- Reinvigorating critical incident response and recovery planning
- Training and exercises involving key public, private, and non-profit actors at both strategic and operational levels
- Improving accountability and facilitating organizational and inter-organizational learning

47. *Improving international cooperation and collaborative response and recovery of critical infrastructure system*s. As we have seen above, contemporary critical infrastructure systems transcend national boundaries in various ways. Disruptions may originate in physical events occurring in or cyber-attacks launched from on one or more countries, but end up impacting many others. Many natural hazard scenarios—such as extreme terrestrial and space weather events-- can impact critical infrastructures across national boundaries and impact global supply chains. Preventing attacks and limiting the damage of disruptions stemming from natural, man-made, or mixed events often requires rapid, even real-time, exchange of intelligence and system status information as well as expert knowledge. In addition, effective coordination of protective, response, and recovery measures is essential to prevent further cascades of disruption and damage and facilitate rapid restoration (e.g. via effective use of scarce repair capabilities and component resources across countries). This is true not only of power and other energy systems, but also of transportation, and telecommunications.

48. *Building trust and relationships in support of crisis management across the public, private non-profit divide.* A broad set of public, private and non-profit actors share authority, responsibility, capabilities, information, knowledge and resources needed to cope with severe critical infrastructure disruptions and their cascading effects. Though these actors are diverse in many respects, they have significant common interests in mitigating disruptions and promoting rapid restoration of critical infrastructures. Whole society/whole community approaches increasingly in emergency management and resilience-building are highly relevant to improving capacity to cope with critical infrastructure failure as well. Creating opportunities, incentives, and fora for these actors to familiarize themselves and cooperate with each other—before, during, and after crisis events—is extremely valuable. Governments are actively supporting this process in many of the most developed countries (e.g. U.S., UK, Sweden, and Switzerland[28]) via resilience fora, critical infrastructure sector groupings, and other equivalent efforts, though more can be done.

49. *Improving knowledge and understanding of critical infrastructure systems through mapping, modelling, and simulatio*n. As we have seen, critical infrastructure systems are highly complex and dynamic. Such systems and the environments in which they operate evolve and change on an ongoing basis. Human ability to understand and predict outcomes with regard to disruptions and protective interventions with regard to such systems is limited (c.f. Perrow, 1984; Roe and Schulman, 2016) and must be leveraged by investments in efforts to map, monitor and develop deeper understanding of them. Significant advancements of methodology and technology may be harnessed to improve mapping (both geographic and functional) to identify pathways to and from

[28] See e.g. the presentation by M. Henauer at the Geneva workshop. https://www.slideshare.net/OECD-GOV/marc-henauer-switzerland-6th-oecd-workshop-on-strategic-crisis-management

failure and towards rapid restoration. Empirically-based modelling, simulation, and visualization tools can be used to improve reliability and resilience more generally as well as to facilitate effective response and rapid restoration to critical infrastructure disruptions.[29]

50. *Reinvigorating critical incident response and recovery planning*. Emergency planning in many countries has been criticized for a tendency toward unrealistic planning assumptions regarding environmental and system vulnerabilities, magnitude and duration of disruptions, and availability of capabilities and resources (Clark, 1999; Eriksson and McConnell, 2011) as well as for neglecting key actors, stakeholders, and particularly vulnerable populations. Conversely, improved planning for critical infrastructure disruptions will:

- Involve a broader set of public, private, and non-profit actors and stakeholders
- Build on state of the art knowledge of systems, hazards, and interventions informed by mapping, the historical experience base with regard to critical infrastructure crises, and empirically-informed and rigorous modelling and simulation methods and technology (see above).
- Include explicit decision criteria and intervention protocols for proactive system protective measures and planning for the operational and political consequences associated with such measures.
- Consider the impact of interdependencies among critical infrastructure systems (Roe and Schulman, 2016), cascading consequences, and capability degradation stemming from the event itself or protective shut down measures with regard to one or more critical infrastructure systems.
- Thinking bigger and emphasizing "bad" or "worst" case scenarios—the so-called maximum of maximums as it has been labelled in U.S. Federal EMA doctrine—in order to reveal limitations and lay a foundation for adaptive behavior in the face of catastrophic events.
- Depart from conservative assumptions regarding available resources for response and recovery resources.
- Plan explicitly and seek to secure preferential access to resources and capabilities in support of rapid restoration of service.

51. Training and exercises involving key actors-- at both strategic and operational levels—from government, critical infrastructure operators, and other key private and non-profit sector stakeholders.[30] Government and critical infrastructure operator leaders should take steps to make sure that they and their team members, other key subordinates, and counterparts from essential partners are educated, trained, and exercised in preparation for critical infrastructure crisis management.[31] When facing major crises,

[29] https://www.slideshare.net/OECD-GOV/dr-georgios-giannopoulos-jrc-6th-oecd-workshop-on-strategic-crisis-management

[30] This draws on chapter four of OECD (2015) *The Changing Face of Strategic Crisis Management* and the discussion of the 2017 Geneva workshop. See also Stern (2013).

[31]For example, the US. Department of Homeland Security Critical Infrastructure Protection and Resilience Toolkit contains expercise planning resources to help operators develop table top exercises. https://www.oecd.org/governance/toolkit-on-risk-governance/goodpractices/page/uscriticalinfrastructureprotectionandresiliencetoolkit.htm#tab_description

partnership between strategic leaders and "professionals" inside and outside of government is essential. This means that political leaders who are not "professionals" must be educated as to the nature of critical infrastructure crisis management, informed of what is required of them in scenarios and contingencies involving (the risk of) significant disruption to critical-infrastructure systems, familiarized with relevant crisis planning and organization, and equipped to engage effectively in meaningful communicative interaction with others inside and outside of their organizations. Individual and collective crisis management skills are best acquired and honed through hands-on practice in simulated as well as real world incidents and crises. There are a wide variety of powerful instructional designs and techniques (both traditional and technology enhanced) suitable for critical infrastructure crisis management training and exercises.[32] Instructional designs and techniques should be consciously chosen and explicitly adapted to the goals and purposes of a given training or exercise for maximum positive impact.

52. *Improving accountability and enabling organizational and inter-organizational learning.* Critical infrastructure failures raise significant issues of political, legal and financial accountability. Divisions of labor and responsibility continue to vary greatly across countries and sectors and ambiguities and gaps persist, contributing to sub-optimal resilience and sub-optimal preparedness for response and rapid restoration. As noted above public, private, and non-profit sector actors participating governance and operation of critical infrastructure systems are subject to multiple forms of accountability and must be prepared to answer questions not only in Congress (or Parliament), but also literally in court and in the metaphorical "courts" of (social) media and public opinion.

53. Disruption of critical infrastructure systems by definition may be costly in lives, treasure, as well as in organizational (and in many cases personal) trust and legitimacy. As a result, it is imperative to learn the lessons of experience. Doing so effectively requires fostering a culture of safety and resilience in which information is shared and performance before, during, and after crises subjected to benchmarking and critical scrutiny. Temptations to withhold "embarrassing" information and white wash sub-par performances should be resisted in favor of systematic and methodologically informed inquiry and vigorous and forward-looking implementation of measures to address preparedness gaps and shortcomings.

[32] See e.g. the description of the Dutch VITEX exercise presented by Mutsaers. https://www.slideshare.net/OECD-GOV/jeroen-mutsaers-netherlands-6th-oecd-workshop-on-strategic-crisis-management

5. References and Resources [Preliminary]

Akgar, B, A. Staniforth, and D. Waddington eds. (2017) Application of Social Media in Crisis Management. Cham, Switzerland: Springer.

Alberts, D. S., & Hayes R.E. (2003) Power to the Edge. Washington, D.C.: Command and Control Research Program.

Austin, L. L., Liu, B. F., & Jin, Y. (2014). Examining signs of recovery: How senior crisis communicators define organizational crisis recovery. Public Relations Review, 40(5), 844–846. https://doi.org/10.1016/j.pubrev.2014.06.003

Baubion, C. (2013) OECD Risk Management: Strategic Crisis Management. OECD Working Papers on Public Governance 23. Paris: OECD.

Boin, A., & McConnell, A. (2007). Preparing for Critical Infrastructure Breakdowns. Journal of Contingencies and Crisis Management, 15(1), 50–59. https://doi.org/10.1111/j.1468-5973.2007.00504.x

Boin et al (2005/2016) The Politics of Crisis Management: Public Leadership Under Pressure. New York: Cambridge University Press.

Brown, G., Carlyle, M., Salmerón, J., & Wood, K. (2006). Defending critical infrastructure. Interfaces, 36(6), 530–544. https://doi.org/10.1287/inte.1060.0252

Clarke, L. (1999) Mission Improbable: Using Fantasy Documents to Tame Disasters. Chicago: University of Chicago Press.

Clinton, W. J. (1996). Executive order 13010-critical infrastructure protection. Federal Register, 61(138), 37347–37350.

De Bruijne, M., & Van Eeten, M. (2007). Systems that should have failed: critical infrastructure protection in an institutionally fragmented environment. Journal of Contingencies and Crisis Management, 15(1), 18–29.

Dunn-Cavelty, M., & Suter, M. (2009). Public-Private Partnerships are no silver bullet: An expanded governance model for Critical Infrastructure Protection. International Journal of Critical Infrastructure Protection, 2(4), 179–187. https://doi.org/10.1016/j.ijcip.2009.08.006

Editor, S., & Pham, H. (2013). Risk and Interdependencies in Critical Infrastructures, (December 2012). https://doi.org/10.1007/978-1-4471-4661-2

Egan, M. J. (2007). Anticipating future vulnerability: Defining characteristics of increasingly critical infrastructure-like systems. Journal of Contingencies and Crisis Management, 15(1), 4–17.

Eriksson, K. & A. McConnell (2011) Contingency planning for crisis management: Recipe for success or political fantasy?, Policy and Society, 30:2, 89-99, DOI: 10.1016/j.polsoc.2011.03.004

Fischbacher-Smith (2006)

Holeguin-Veras, J. et al (2012) On the unique features of humanitarian logistics. Journal of Operational Research 30(7-8), 494-506 https://doi.org/10.1016/j.jom.2012.08.003

Klijn, E.-H., & Teisman, G. R. (2003). Institutional and Strategic Barriers to Public—Private Partnership: An Analysis of Dutch Cases. Public Money and Management, 23(3), 137–146. https://doi.org/10.1111/1467-9302.00361

Labaka, L. ., Hernantes, J. ., Comes, T. ., & Sarriegi, J. M. . (2014). Defining policies to improve critical infrastructure resilience. ISCRAM 2014 Conference Proceedings - 11th International Conference on Information Systems for Crisis Response and Management, (May), 429–438. Retrieved from http://www.scopus.com/inward/record.url?eid=2-s2.0-84905833913&partnerID=40&md5=b93ff6d1024ecff53cd36f7eed5373ac

Linnenluecke, M. K., Griffiths, A., & Winn, M. (2012). Extreme weather events and the critical importance of anticipatory adaptation and organizational resilience in responding to impacts. Business Strategy and the Environment, 21(1), 17–32. https://doi.org/10.1002/bse.708

Lundberg, J., Törnqvist, E., & Tehrani, S. N. (2012). Resilience in sensemaking and control of emergency response. International Journal of Emergency Management, 8(2), 99. https://doi.org/10.1504/IJEM.2012.046009

Lynne Genik, P. C. (2013). An Overview of Pilot Projects in Support of Critical Infrastructure Resilience.

Macaulay, T. (2008). Critical Infrastructure. https://doi.org/10.1201/9781420068368.ch1

Mohammed, J. R., & Qasim, J. M. (2012). Comparison of One-Dimensional HEC-RAS with Two-Dimensional ADH for Flow over Trapezoidal Profile Weirs. Statewide Agricultural Land Use Baseline 2015, 1(6), 1–32. https://doi.org/10.1017/CBO9781107415324.004

Moteff, J., & Ave, I. (2004). CRS Report for Congress Received through the CRS Web Risk Management and Critical Infrastructure Protection : Assessing , Integrating , and Managing Threats , Vulnerabilities and Consequences. Risk Management. Retrieved from http://www.fas.org/sgp/crs/RL32561.pdf

Moteff, J., & Parfomak, P. (2004). CRS Report for Congress Received through the CRS Web Critical Infrastructure and Key Assets. Time, 19. Retrieved from http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA454016

Koraeus, M and E. Stern (2013) "The Crisis Management-Knowledge Management Nexus" in Akhgar and Yates eds. Strategic Intelligence Management. London: Butterworth-Heinemann.

Nye, D. (2010) When the Lights Went Out: A History of Blackouts in America. Cambridge, MA: MIT Press.

OECD (2015) The Changing Face of Strategic Crisis Management. Paris: OECD Press.

Ouyang, M. (2014). Review on modeling and simulation of interdependent critical infrastructure systems. Reliability Engineering and System Safety, 121, 43–60. https://doi.org/10.1016/j.ress.2013.06.040

Parker (2014) Complex Negative Events and the Diffusion of Crisis: Lessons from the 2010 and 2011 Icelandic Volcanic Ash Cloud Events Geografiska Annaler. DOI: 10.1111/geoa.12078

Pelfrey, W. V. J. S., Pelfrey, W. V. J. S., & Information, C. (2010). Sensemaking in a Nascent Field : A Conceptual Framework for Understanding the Emerging Discipline of Homeland Security. The Homeland Security Review, 4(3).

Roe, E. and Schulman, P. (2016) Reliability and Risk: The Challenge of Managing Interconnected Infrastructures. Stanford, CA: Stanford Business Books.

Roehrich, J. K., Lewis, M. A., & George, G. (2014). Are public-private partnerships a healthy option? A systematic literature review. Social Science and Medicine, 113, 110–119. https://doi.org/10.1016/j.socscimed.2014.03.037

Rosenthal, U., Charles, M. T., & Hart, P. T. (1989). Coping with crises: The management of disasters, riots, and terrorism. Springfield: Charles C Thomas Pub Ltd.

Santella, N., Steinberg, L. J., & Parks, K. (2009). Decision making for extreme events: Modeling critical infrastructure interdependencies to aid mitigation and response planning. Review of Policy Research, 26(4), 409–422. https://doi.org/10.1111/j.1541-1338.2009.00392.x

Smith, L. (2012). School Leadership in Times of Crisis. School Leadership and Management, 32(1), 57–71.

Stern, E. (2017a) "Crisis Management, Social Media, and Smart Devices" in Akghar et al. eds. Applications of Social Media in Crisis Management. New York: Springer.

Stern, E. (2017c) "Unpacking and Exploring the Relationship between Crisis Management and Social Media in the Era of 'Smart Devices" Homeland Security Affairs Journal.

Stern, E. ed. (2014) Designing Crisis Management Training and Exercises for Strategic Leaders. Stockholm: Swedish National Defense College (SNDC).

Stern, E. et al (2014) "Post-Mortem Crisis Analysis: Dissecting the London Bombings of July 2005" Journal of Organizational Effectiveness 1(4)

Stern, E (2013) "Preparing: The Sixth Task of Crisis Leadership". Journal of Leadership Studies 7(3):51-57.

Stern E. (2003)"Crisis Studies and Foreign Policy Analysis: Insights, Synergies, and Challenges" International Studies Review 5:183-202.

Tanaka, H. (2006). Thank you for using the University at Albany's Interlibrary Loan Service, 30. https://doi.org/10.1680/udap.2010.163

Weick, K. E. (1993). The collapse of sensemaking in organizations: The Mann Gulch disaster. Administrative Science Quarterly, 628–652.

Weick, K. E. (1993). The Collapse of Sensemaking in Organizations: The Mann Gulch Disaster. Administrative Science Quarterly, 38(4), 628–652. https://doi.org/10.2307/2393339

Weick, K. E., Sutcliffe, K. M., & Obstfeld, D. (2005). Organizing and the Process of Sensemaking. Organization Science, 16(4), 409–421. https://doi.org/10.1287/orsc.1050.0133

Zimmerman, R. (2004). Decision-making and the vulnerability of interdependent critical infrastructure. Conference Proceedings - IEEE International Conference on Systems, Man and Cybernetics, 5, 4059–4063. https://doi.org/10.1109/ICSMC.2004.1401166

Annex A. Appollo's Fury Exercise [to be added].

https://www.slideshare.net/OECD-GOV/prof-eric-stern-exercice-6th-oecd-workshop-on-strategic-crisis-management