



S.A.P.I.E.N.S

Surveys and Perspectives Integrating Environment and Society

6.1 | 2013

Vol.6 / n°1 - Resilient Cities

Adding value to critical infrastructure research and disaster risk management: the resilience concept

Claudia Bach, Sara Bouchon², Alexander Fekete, Jörn Birkmann et Damien Serre

Eric Duchemin, Bruno Barroca et Damien Serre (éd.)



Éditeur

Institut Veolia Environnement

Édition électronique

URL : <http://sapiens.revues.org/1626>

ISSN : 1993-3819

Référence électronique

Claudia Bach, Sara Bouchon², Alexander Fekete, Jörn Birkmann and Damien Serre, « Adding value to critical infrastructure research and disaster risk management: the resilience concept », *S.A.P.I.E.N.S* [Online], 6.1 | 2013, Online since 15 July 2014, connection on 30 September 2016. URL : <http://sapiens.revues.org/1626>

Ce document est un fac-similé de l'édition imprimée.

Licence Creative Commons

Perspectives

Adding value to critical infrastructure research and disaster risk management: the resilience concept.

Claudia Bach¹, Sara Bouchon², Alexander Fekete³, Jörn Birkmann¹, Damien Serre⁴

1. United Nation University Institute for Environment and Human Security (UNU-EHS)
Platz der Vereinten Nationen 1, 53113, Bonn
bach@ehs.unu.edu and birkmann@ehs.unu.edu respectively.

2. Risk Governance Solutions S.r.l., Via Fratelli d'Italia, 7, 21052 - Busto Arsizio (VA),
sara.bouchon@riskgovernancesolutions.eu.

3. Institute of Rescue Engineering and Civil Protection,
Cologne University of Applied Sciences/Fachhochschule Koeln,
alexander.fekete@fh-koeln.de.

4. RESCUESolutions SAS, Bagneux, France
damien.serre@rescuesolutions.fr.

Abstract *In recent years, resilience has become a key term in disaster risk management (DRM). Its potential has been mainly discussed with respect to social-ecological systems as well as communities. With respect to Critical Infrastructures (CIs) however, resilience and vulnerability are often used without clear definition and reference to the DRM context. This paper aims to conceptualize vulnerability and resilience for the CI context. Building on socio-ecological approaches, the paper will outline the added value that a more stringent conceptualization of resilience offers for DRM of CIs. After an introduction of CIs and their meaning in the context of DRM (Section 1), the distinct features of the resilience concept and its application in different disciplines are presented (Section 2). Some of the governance challenges associated with the implementation of resilience strategies are presented (Section 3) before conclusions are drawn (Section 4).*

Keywords: Resilience, Critical Infrastructure, Protection, Social-Ecology, Engineering, Concepts, Application.

TABLE OF CONTENTS

1. Introduction
2. From Critical Infrastructure Protection to Resilience
 - 2.1 The resilience concept
 - 2.2 Infrastructure protection: the added value of the resilience concept
 - 2.2.1 CI/human interaction as part of the resilience concept
 - 2.3 Development of Critical Infrastructure Resilience strategies
3. Discussing Critical Infrastructure resilience implementation challenges
 - 3.1 Cooperation and communication among the multiplicity of stakeholders
 - 3.2 Understanding system characteristics
 - 3.3 Integration of citizens into resilience building
4. Conclusion
5. References

1. INTRODUCTION

The recognition of risk as a social construct became one basis for the development of a certain stream of risk assessment methodologies and DRM approaches (e.g. Blaikie *et al.*, 1994; Alexander, 2000; Birkmann, 2013). In this context, different terminologies and concepts such as vulnerability (Birkmann, 2013), sensitivity (Füssel & Klein, 2006), resilience (Paton & Johnston, 2000; Klein *et al.*, 2003; Adger *et al.*, 2005; Cutter *et al.*, 2008) or adaptation and adaptive capacity (Pelling, 2011; Smit & Wandel, 2006) have been developed from related disciplines. Discussions with respect to their delineation, overlap and applicability are ongoing (Cutter *et al.*, 2008; Cardona, 2011; Birkmann, 2013).

Definition and translation of these theoretical concepts into indicators and criteria form an important part of disaster risk assessments and are a priority of the Hyogo Framework for Action (UNISDR, 2007). In this respect, different spheres of interest have been identified that encompass economic, environmental and social dimensions (Cardona & Barbat, 2000; Birkmann, 2013; Cardona, 2011). Defined as "...an asset or part thereof... which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people" (EC, 2008: Article 2a), Critical Infrastructure (CI) can be identified as a cross-cutting topic for all three spheres.

In parallel to these discourses in the DRM community, CIs have gained political importance in the wake of terror attacks in 2001 (World Trade Center), 2004 (Madrid) and 2005 (London) (FMIG, 2009; Her Majesty the Queen in Right of Canada, 2009; HM Government, 2010). These events both shifted the focus of DRM activities and reshaped the CI context, through increasing awareness of the complexity and interrelatedness of infrastructures as socio-technical systems (e.g. Rinaldi *et al.*, 2001; IRGC, 2006; Kröger, 2008; Serre *et al.*, 2013) and the

increasing likelihood of cascading effects reaching beyond geographical and functional borders (Boin & McConnell, 2007; Hémond & Robert, 2012; Lhomme *et al.*, 2013).

The strengthening of infrastructures has been identified as an important field for disaster risk reduction (e.g. UNISDR, 2007). However, CI and DRM terminologies and methodologies have not fully been integrated, resulting in inconsistent labeling, conceptualization and implementation of disaster risk-related CI activities and governance approaches. Accordingly, it is the aim of this paper to apply methodological discussions on DRM conceptualizations to CIs, in order to underline the advantages of the resilience concept for this specific context as well as to discuss potential governance challenges.

2. FROM CRITICAL INFRASTRUCTURE PROTECTION TO RESILIENCE

In the context of DRM, the resilience concept is variously viewed as supplementary to (Gallopín, 2006), overlapping with (Cutter *et al.*, 2008) or the flip-side of (Folke *et al.*, 2002) existing concepts such as *vulnerability*. In the following, we will analyze the specificities offered by the resilience concept as well as its application in the development of strategies.

2.1 THE RESILIENCE CONCEPT

The resilience approach was initially used in the fields of psychology (e.g. Garmezy *et al.*, 1984; Rutter, 1985) and ecology (e.g. Holling, 1973), amongst others. In ecology, when considering systemic interactions, the term 'resilience' addresses the ability of ecosystems to absorb fluctuations while persisting. This was a departure from the traditional view that had equated the optimum ecological state with stability—a departure deemed necessary in order to address the behavior of nonlinear systems (Holling, 1973). Socio-ecological resilience research focuses on the relevance of renewal, reorganization and development (Holling, 2001; Gunderson & Holling, 2002; Berkes *et al.*, 2008), arguing that resilience increases the likelihood for desirable pathways under changing and sometimes even unpredictable conditions (Walker *et al.*, 2004; Adger *et al.*, 2005; Folke, 2006). Accordingly, non-linear developments (which might also be generated through infrastructure breakdowns) became part of the analysis (Folke, 2006). The Resilience Alliance defined the term as:

"The ability to absorb disturbances, to be changed and then to re-organise and still have the same identity (retain the same basic structure and ways of functioning). It includes the ability to learn from the disturbance. A resilient system is forgiving of external shocks. As resilience declines, the magnitude of a shock from which it cannot recover gets smaller and smaller. Resilience shifts attention from purely growth and efficiency to needed recovery and flexibility. Growth and efficiency alone can often lead ecological systems, businesses and societies into fragile rigidities, exposing them

to turbulent transformation. Learning, recovery and flexibility open eyes to novelty and new worlds of opportunity.”¹

Counter to this, the *equilibrium approach* to resilience played an important role in many disciplines and has substantially shaped natural resource and environmental management. Traditional engineering resilience approaches often focus on maintaining efficiency and the constancy of a system close to a single steady state (see Holling, 1996 and Table 1). This aspect can also be found in more recent engineering literature stressing the control over the system in order to avoid failure. Vugrin *et al.*, [2010], for example, define CI resilience as:

“Given the occurrence of a particular disruptive event (or set of events), the resilience of a system to that event (or events) is the ability to efficiently reduce both the magnitude and duration of the deviation from targeted system performance levels” (p.82).

According to them, CI resilience comprises two main measurable components: a—the system impact, defined as the difference between general and actual (after event) performance; and b—the recovery effort, encompassing the resources required to restore the functioning to a pre-defined desirable performance level. This engineering driven approach thus neglects the potential for flexibility and change of the system. It relates resilience to the capabilities of systems or networks, elements often expressed in terms such as robustness, redundancy or others (Tierney & Bruneau, 2007). In these approaches, resilience assessments were and still are in many contexts addressing the physical conditions of systems while neglecting different aspects and phases of disaster management (see *e.g.* Hartong *et al.*, 2008, Svensson 2008, Bompard *et al.*, 2009, Rich *et al.*, 2009, Gheorghe and Vamanu 2005 and 2008, Petit *et al.*, 2011, Kröger and Zio 2011, Li *et al.*, 2012).

Table 1: Concepts of resilience in the socio-ecological context

Resilience Concept	Characteristics	Focus on	Context
Engineering resilience.	Maintaining efficiency and constancy.	Deviation from actual performance (often also understood as robustness), recovery effort.	Vicinity to stable equilibrium.
Ecological/ ecosystem resilience and social resilience.	Buffering capacity, withstanding shock, maintaining function.	Persistence, absorb disturbance.	Multiple equilibria, stability landscape.
Socio-ecological resilience.	Interplay, disturbance and reorganization, sustaining and developing.	Adaptive capacity, transformability, learning, innovation.	Integrated system feedback, cross-scale dynamic interactions.

Source: adapted from Folke (2006: 259).

As indicated in Table 1 the resilience concepts used in the socio-ecological context allow for the consideration of systemic feedbacks and cross-scale dynamic interactions as well as (institutional) learning, which can also be transferred to CIs.

2.2 INFRASTRUCTURE PROTECTION: THE ADDED VALUE OF THE RESILIENCE CONCEPT

Applying the concept of resilience as defined in the socio-ecological approach to CIs can be of great value. Shifting the focus away from the maintenance and equilibrium of the infrastructure system towards the delivery of system services and its external relations permits a better consideration of external effects and changes as well as interaction with other systems, in this case society. Gallopín (2006) suggests that the interaction of external and internal processes needs to be considered since stress can be triggered by changes in the system environment, by internal alterations, or both. With respect to CIs, a variety of system challenges can be identified. They include: the increasing (inter-)dependencies of and between infrastructure systems (*e.g.* Rinaldi *et al.*, 2001); technological changes and the integration of smaller into larger systems, thus increasing system complexity and allowing for far-reaching disturbances (Kröger, 2008: 1781); the privatization of infrastructures (Gheorghe *et al.*, 2006: xiv; Kröger, 2008: 178,); the liberalization of markets, leading to an increasing number of actors (Gheorghe *et al.*, 2006: xi ff); and changes in demand patterns (Kröger, 2008; IRGC, 2010). Additionally, changes in system set-up and governance, and global changes including the increasing use of renewable energies, urbanization processes and demographic changes, also shape CI resilience.

Besides these changes, the resilience concept also allows for the consideration of unexpected events such as the 2004 boxing day tsunami, Hurricane Katrina in 2005 or the 2011 Tohoku earthquake and following tsunami. In some cases, unexpected disruptions may occur due to miscalculations in design. The Fukushima earthquake and tsunami for example were both larger than had been anticipated in the design of Japanese power plants (Bunn & Heinonen, 2011: 1580) representing a mismatch of design structures and the spectrum of plausible hazards. Incorporating the resilience concept in this case would ideally have led to the integration of ‘safe failure’ into the design structures, and a higher degree of flexibility to account for a diversity of hazards. In other cases, unexpected disruptions may be the result of cascading effects caused by increasing interdependencies and complexities (Rinaldi *et al.*, 2001; IRGC, 2006; Boin & McConnell, 2007; Kröger, 2008; Hémond & Robert 2012; Lhomme *et al.*, 2013): in this example, the dependency of tsunami height on the magnitude of the earthquake, and the interdependencies of the cooling system with electricity production, water pollution, back-up systems, blocked traffic routes and fire-brigade services. A DRM strategy informed by resilience would specifically design and implement measures that take the interlinkages between different infrastructures into account, as opposed to a DRM strategy that devises a separate strategy or analysis for each system.

¹ <http://www.resalliance.org/index.php/resilience>

Nevertheless, assessment methodologies and measures to address CI disruptions still mainly build on the notion of stability and robustness defined in specific scenarios (e.g. Greenberg *et al.*, 2007; EC, 2009; Reed *et al.*, 2009) while neglecting systemic changes and unexpected events. Although many assessments do encompass multi-hazard approaches, they are still creating blind spots and potential new vulnerabilities by not integrating resilience aspects into their assessments (Perelman, 2006). In this regard, resilience strategies need to incorporate uncertainties (or the so-called 'soft paradigm': Perelman, 2006). In its simplest form, this would mean having a "Plan B" in the event of failure (Tierney & Bruneau, 2007), or a range of options to be taken. Another strategy is to design 'safe failure' or 'graceful degradation' into systems, so that they continue to operate in the event of failure in one or more components (Tyler & Moench, 2012). Another approach is to openly encourage flexibility, for instance, encouraging people to embrace uncertainty rather than insisting on 100% certainty or even a predictable future and security.

2.2.1 CI/HUMAN INTERACTION AS PART OF THE RESILIENCE CONCEPT

Many approaches in the disaster risk reduction area are still sector-specific, focussing on the vulnerability of a particular type of system/CI (e.g. Hartong *et al.*, 2008; Svensson, 2008; Bompard *et al.*, 2009; Rich *et al.*, 2009; Gheorghe & Vamanu, 2005, 2008; Petit *et al.*, 2011; Kröger & Zio, 2011; Li *et al.*, 2012). Although the respective research is valuable in order to learn more about the individual system characteristics and potential disaster risk reduction measures, the implications for society are often unclear. However, the operation of CIs determines the functioning of many societies (e.g. FMIG, 2009; DHS, 2009; Cabinet Office, 2010); therefore, a broader perspective is required, that addresses the societal effects. The resilience concept offers the possibility to include societal aspects by taking into account the ability to absorb external shocks². This is specifically relevant as the social effects of an infrastructure breakdown are mainly determined by the level of dependence on an uninterrupted supply, or by the level of preparedness (Toubin *et al.*, 2014). Paradoxically, high levels of supply security lead to complacency within the population and thus an unpreparedness towards potential failures (FMIG, 2009; Reichenbach *et al.*, 2008).

Taking electricity supply failure as an example, not all households and facilities are equally affected. While a shortfall of electricity supply can have life-threatening effects in hospitals (where emergency power supply might be insufficient) (Aghababian, 1994: 773; Klein *et al.*, 2005: 343) and geriatric homes with patients dependent on artificial respiration, a household of middle-aged adults might be relatively unaffected. Additionally, preparedness levels, e.g. with respect to the availability of back-up facilities,

will differ and thus influence overall CI-human resilience.

2.3 DEVELOPMENT OF CRITICAL INFRASTRUCTURE RESILIENCE STRATEGIES

Although the protection of strategically important facilities has always been an important part of national defense strategies (Hellström, 2007; Lauwe & Riegel, 2008), the beginning of the 21st century saw a change in the nature of perceived threats, with natural hazards and terrorism now the focus of security debates (Lauwe & Riegel, 2008). The importance of CI protection escalated through the 2001, 2004 and 2005 terror attacks in New York, Washington, Madrid and London, as well as in response to a number of disasters such as Hurricane Katrina in 2005 or the UK flooding in 2007. Against this changing landscape, societies have become highly vulnerable towards a broad and diffuse spectrum of possible threats (Brunner & Suter, 2008; Her Majesty the Queen in Right of Canada, 2009: 4; HM Government, 2010).

The first generation of policies addressing CI disruptions in this changed threat context was a set of Critical Infrastructure Protection (CIP) strategies. The focus on protection was mainly considered from an all-hazards perspective:

"...the objectives of the EPCIP [European Programme for Critical Infrastructure Protection] will be to continue to identify critical infrastructure, analyse vulnerability and interdependence, and come forward with solutions to protect from, and prepare for, all hazards." (EC, 2004: 8)

The protection was seen as the way to reduce, sometimes to totally eliminate, the vulnerabilities of critical infrastructure systems, mainly seen as the physical assets or components of an infrastructure. In this context, the vulnerability of CIs was defined as a "weakness in the system of the critical infrastructure in itself, which might be exploited, unintentionally or intentionally" (Bouchon, 2006: 80).

Nevertheless, during the last decade, CI disruption issues became more integrated into DRM approaches (see Figure 1). This increase in awareness on the importance of CI resilience, triggered by a variety of events such as the 2003 Northeastern blackout in the US and Canada, Hurricane Katrina in 2005, the 2007 UK flooding as well as the overall awareness of the potential effects of climate change (City of Cape Town, 2006; German Federal Government, 2008), was accompanied by a shift from direct protection and prosecution to a more systemic view of infrastructures in certain countries. It was characterized by the insight that rather than focussing on the protection of certain facilities, the safeguarding of the provision of services should be the primary aim. In particular, the Nordic countries focused on *critical societal functions* (Norwegian CIP Commission, 2006) or *functions vital to society* (Government of Finland, 2006).

² See the Resilience Alliance website: <http://www.resalliance.org/index.php/resilience>

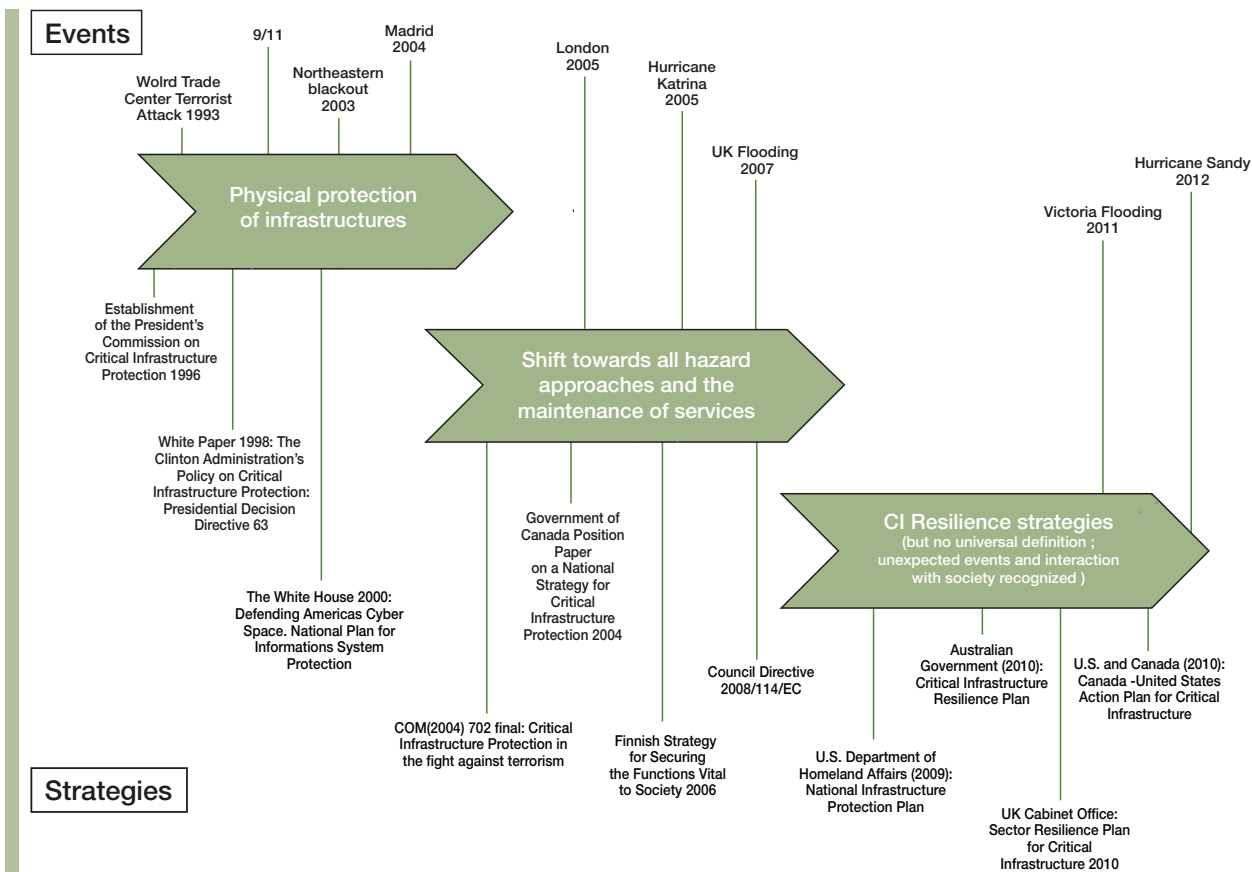


Figure 1: Development of Critical Infrastructure Resilience Strategies. Source: authors.

Some recent documents include resilience terminology in strategic approaches (City of New York, 2013; Cabinet Office, 2010; Scottish Government, 2011; Australian Government, 2010; DHS & Public Safety Canada, 2009; Her Majesty the Queen in Right of Canada, 2009; NIAC, 2009). However, in others the resilience approach is not referred to (e.g. EC, 2008) or is used in a misleading way in what should be referred to as protection strategies (e.g. The White House, 2013). This is astonishing not only since the scientific debate has been well developed, but because resilience-based approaches have been found to be substantially less expensive than investments into structural updates (de Bruijne & van Eeten, 2007: 24). Although resilience aspects such as education and training or specific response and recovery efforts are integrated into some strategies (e.g. DHS, 2009), *societal* resilience encompassing efforts and planning activities of communities and businesses is frequently neglected (Boin & McConnell, 2007: 54 ff; Pursiainen, 2007: 31 ff). Finally, most CI DRM strategies still fail to integrate insecurities and to explicitly address the potential unexpectedness of events. In this respect, the development of more comprehensive and integrated resilience approaches taking into account different spatial and content-related levels (e.g. changes in socio-technical landscapes, patchworks of standards and regimes or action of individuals) are needed (Hellström, 2007). Although some guidelines take these aspects into account (e.g. TISP, 2006; TNO, 2011), a variety of challenges remain for regional, national and local strategies (Balsells *et al.*, 2013; Toubin *et al.*, 2014).

3. DISCUSSING CRITICAL INFRASTRUCTURE RESILIENCE IMPLEMENTATION CHALLENGES

Having looked into the development of CI resilience strategies, the variety of nomenclature is striking and increases the challenges in implementing resilience strategies such as 1—cooperation and communication among the multiplicity of stakeholders, 2—understanding system characteristics, and 3—the integration of citizens into resilience building.

3.1 COOPERATION AND COMMUNICATION AMONG THE MULTIPLICITY OF STAKEHOLDERS

In the field of CI strategies, the main challenge raised by governance is related to the need to involve very different types of stakeholders: the population, public authorities (from different jurisdictions), private operators, operators from different sectors, the media, *etc.*. This need has been articulated in the concept of network governance proposed by Suter (2011). Each group of stakeholders has its own interests, and hence its own understanding of what it means to achieve resilience. Potential conflicts may arise, for instance when business interests are not compatible with public security. The role of the State with respect to CIs changes when liberalization or privatization occurs: it can no longer directly influence the setup and governance of the CI system, but rather has to focus on setting framework conditions for production processes

and markets and subsequently organizing and moderating negotiations between different stakeholders (Abbate, 1999; de Bruijne & van Eeten, 2007; Monstadt, 2008; Toubin *et al.*, 2014). The provision of CI services is, however, mainly in the hands of privately organized operators.

The collaboration between the different stakeholders requires adequate collaboration schemes, where each group of stakeholders feels that its own interests are taken into account (win-win situations). The need for cooperation was already identified by the President's Commission on Critical Infrastructure Protection (PCCIP) (1997). Such public-private partnerships (PPPs) are already operational, for instance, in Scotland, where the regional Critical Infrastructure Strategy is based on a Critical Infrastructure Partnership Framework between Government and those responsible for the critical assets "...to minimise disruption to any part of that infrastructure or to any of our communities living and working across Scotland" (Scottish Government, 2011: 27). In the case where the interests of each group of stakeholders are not taken on board, the strategy elaborated may compromise the achievement of the expected results, as in the example of the 2008 European Directive on European Critical Infrastructure (ECI). The Directive defined security measures to be implemented by the ECI operators; however, the operators had little input on the accuracy of these measures, whose implementation they had to pay for (Bouchon, 2011). This was one of the main factors triggering a revision of the Directive. Resilience measures should thus be the result of a participative process to ensure better acceptance.

In the case of Norway, CI resilience is achieved through measures implemented by responsible owners, taking into account the needs defined by their customers, and on the basis of goals, expectations and regulations defined by the responsible authorities, within a system of risk governance defined by the government (Thomassen, 2012). However, adequate governance models to achieve CI resilience in different contexts remain to be developed. The main challenges in this regard include: the identification of the right number of stakeholders (not too few, not too many); the types of collaboration process to be developed (e.g. protocols, informal discussions, exercises, *etc.*); and the degree of formalization of this process (policies with a normative goal vs. processes based on a voluntary, informal, or horizontal way of collaboration).

If CIR stakeholder collaboration is to prove efficient in addressing the resilience and protection issues (Bouchon & Dimauro, 2012; Bouchon *et al.*, 2012), it is fundamental that the interest of participants be maintained by taking into account their needs and perspectives, and also that the necessary funding be generated. New synergies and innovative co-financing strategies, involving the participation of both public and private actors, need to be explored in this regard.

The adoption and the development of adequate technologies and communication systems are particularly relevant to CI Resilience collaboration processes: they are the key factors to secure the exchange of information. Large, monolithic and

costly integrated platforms are not in line with the needs of authorities and operators. On the contrary, technological innovations should be directed to gain opportunities for economy of scale and investment sustainability, thanks to modular interoperable and reconfigurable solutions.

A key element of successful stakeholder collaborations is communication between the stakeholders (IRGC, 2006). Communication is principally a question of defining responsibilities, roles, duties and obligations with respect to specific procedures and crisis situations. The challenges of CI governance already substantial in business as usual, scenarios against the background of liberalized markets and the privatization of the provision of services (Kröger, 2008) are only intensified in times of crisis when specific needs arise but responsibilities and cooperation potential remain unclear. For example, Hurricane Katrina showed that the disaster management mechanisms in place were not sufficient, despite the fact that new strategies had been implemented after 9/11 (Wise, 2006). Although the unexpected breakdown of communications technology played an important role in turning the natural hazard into a disaster situation, confusion about responsibilities and the interaction of departments and officials contributed significantly (*ibid.*: 304). Since communication always involves the exchange of information, it is important to address the type of information that can be exchanged (e.g. intelligence or commercially sensitive information) and technical questions related to the information exchange, such as protection measures, secure information sharing platforms and their limitations in DRM.

Finally, decision-making processes also pose a challenge to resilience building. This encompasses decision-taking as well as the financing, implementation and monitoring of decisions taken. It is also necessary to determine how decisions can be taken. For example, who should make decisions regarding resilience levels and acceptable risks? Ensuring the delivery of certain infrastructure services during times of crisis necessarily implies the prioritization of available resources; however, the criteria under which such prioritization processes can be organized, and who should make such decisions, remain unclear. Public discussion about possible limits of protection and target levels of risk can contribute to addressing this challenge and could serve as a stimulus for multi-stakeholder communication about risks (Fekete *et al.*, 2012; Fekete, 2012).

3.2 UNDERSTANDING SYSTEM CHARACTERISTICS

A second governance challenge that is closely related to communication between stakeholders is related to the collection of relevant information to characterize the CI systems and their interdependencies. Stakeholders need to understand their dependence on certain CI services as well as their own role in the functioning of other infrastructure services. Such system characteristics can be identified in a hazard independent manner with the help of scenarios.

Some cases show that building PPPs, as mentioned above,

creates a trusted environment for information exchange that allows better understanding of the system characteristics. Examples have been developed in the Netherlands (Luijckx et al., 2003), Canada (Robert & Morabito, 2010), in Scotland, or in Lombardy, Italy (Bouchon et al., 2012). In this last example, transportation and energy operators, in collaboration with the regional Civil Protection authorities, started working in 2009 to increase their knowledge of the existing interdependencies characterizing the Transportation and Energy critical systems for the Lombardy Region: on the basis of questionnaires, direct interviews and process mapping, operators were requested to provide information about critical infrastructures nodes, accident and service disruption events, maintenance, and crisis management internal processes and systems in order to understand fallout effects. A simulation of functional vulnerabilities and interdependencies has also been developed to support the programme activities (Trucco et al., 2011; Cagno et al., 2011). As a result of these cooperation efforts, the Lombardy Region Authorities have developed an emergency communication and information-sharing framework. The operators contributed to the identification of the relevant communication flows and channels under different emergency conditions and type of events. For example, in the scenario of heavy snowfall, the operators could state the kind of information they needed (e.g. very precise meteorological predictions), the information they could provide (particularly information that could have an impact for the other operators) and the role they expected the regional crisis management centre to play (e.g. to communicate with the public).

3.3 INTEGRATION OF CITIZENS INTO RESILIENCE BUILDING

A third important point that needs to be considered in the context of CI resilience building is the incorporation of civil society. In this regard, citizens should be understood to be consumers and tax-payers, and thus stakeholders. It is therefore fundamental to communicate the CI decisions to be taken, particularly those decisions that concern the communities.

Since CI resilience should focus on maintaining the provision of certain infrastructure services, it is important to have information about specific dependencies (with respect to citizens but also regarding public facilities such as hospitals, transport systems, etc.). At the same time, it is equally important to view citizens as active contributors towards civil protection. For example, the principle underlying the Australian approach to CIR is that “communities are the heart of the resilience process” (Duckworth, 2012). For people to prepare for and respond to emergencies, people must understand the risks they live with. When they understand the risks, they need to be empowered to take action to deal with them. Governments cannot make people resilient, but they can help by providing information and ongoing support (e.g. Cabinet Office, 2013). Building resilience is a “bottom-up” process and governments as well as regional authorities need to agree on a communication framework to inform and engage people about risk. Although everyone must take into account the possibility of deficiencies in deliveries of services on which they are critically dependent, this is one

area in which the State should assume greater responsibility (Duckworth, 2012). Accordingly, analysis of how top-down and bottom-up approaches can be matched is required.

Community resilience including the bottom-up approach is not a new concept, and has in fact been widely applied in the DRM community (Magis, 2010; Cutter *et al.*, 2008; Paton & Johnston, 2000, 2006; Tobin, 1999), for example with respect to empowerment, education, access to institutions and resources (Edwards, 2009). With respect to the failure of CIs, however, the concept has only recently been applied.

Citizens can not only improve their own resilience by these measures but also serve as a source of information for civil protection agencies. People can provide relevant information to allow first responders to identify what is happening, where the priorities are, and what types of resources need to be mobilized. This may entail, for instance, analyzing information circulating among social networks, although this raises the question of validating and guaranteeing the accuracy of the information (e.g. Australian Emergency Management Institute, 2013).

4. CONCLUSION

The term ‘resilience’ is increasingly used for CI-related DRM strategies. However, it is applied in a variety of contexts and scales, often without a clear and stringent definition. This results in confusion around its meaning, so that it becomes difficult to understand what is meant when a resilience strategy is presented. This failure to clearly define the concept may mean that the actions and activities deriving from it fail to increase resilience. With respect to society and CIs, resilience strategies need to integrate the potential failure of infrastructure services instead of focussing only on their robustness and reliability. Relating resilience to concepts used in the DRM community and specifically to aspects of socio-ecological resilience facilitates the interrelation of technical systems while taking into account unexpected events—at least from a theoretical point of view. In order to operationalize a resilience framework for CIs towards natural hazards, further research is required. Although some current research projects address the general question of conceptualizing resilience in different contexts (e.g. the FP7 project EmBrace) and some valuable examples have been presented, for instance by TISP (2006), the operationalization potential for the CI context remains vague.

The implementation of resilience strategies by concrete measures and monitoring activities remains a challenge. In this regard, indicators of the efficiency of resilience strategies would be needed to evaluate results and to benchmark different approaches in order to generate arguments in favor of appropriate action. Difficulties in collecting and updating relevant data and information (Trucco *et al.*, 2011, Robert & Morabito, 2010) are an obstacle to progress in this area. Technical solutions establishing a trustable and secure environment to exchange data and other information among different operators such as policy makers and operators can

thereby facilitate the implementation of resilience strategies. Some first attempts have been made by Bruneau *et al.* (2003).

Finally, additional research with respect to bridging different temporal and spatial scales in resilience strategies is required. While operators consider operational business timeframes, governments and political decision makers follow a political and electoral timeframe. These timeframes differ from the lifespan of infrastructure systems or the timeframe of technical and technological changes. The superposition of these timeframes requires further analysis, while different fields—such as land use planning, emergency management or infrastructure development—take place at different spatial scales, which also have to be integrated.

REFERENCES

- Abbate, J. (1999). From control to coordination: new governance models for information networks and other large technical systems. In: Coutard, O. (Ed.) *The Governance of Large Technical Systems*, pp. 114-129. London: Routledge.
- Adger, W.N., T.P. Hughes, C. Folke, S.R. Carpenter & J. Rockström (2005). Social-ecological resilience to coastal disasters. *Science* 309: 1036-1039.
- Aghababian R., C.P. Lewis, L. Gans & F.J. Curley (1994). Disasters within hospitals. *Annals of Emergency Medicine* 23: 771-777.
- Alexander, D. (2000). *Confronting Catastrophe. New Perspectives on Natural Disasters*. Edinburgh: Dunedin Academic Press..
- Australian Emergency Management Institute (2013). *National strategy for disaster resilience: community engagement framework, Handbook 6*. Commonwealth of Australia, Attorney General's Department. Archived by WebCite at: <http://www.webcitation.org/6Q3f6rtlk>.
- Australian Government (2010). *Critical infrastructure resilience strategy*. Archived by WebCite® at: <http://www.webcitation.org/6Q3g53aFs>
- Balsells, M., B. Barroca, J. Amdal, Y. Diab, V. Becue & D. Serre (2013). Analysing urban resilience through alternative stormwater management options: application of the conceptual Spatial Decision Support System model at the neighbourhood scale. *Water Science and Technology* 68(11): 2448-2457.
- Berkes, F., J. Colding & C. Folke (Eds.) (2008). *Navigating Social-Ecological Systems: Building Resilience for Complexity and Change*. Cambridge: Cambridge University Press.
- Birkmann, J. (2013). Measuring vulnerability to promote disaster resilient societies: Conceptual frameworks and definitions. In: Birkmann, J. (Ed.) *Measuring Vulnerability to Natural Hazards: Towards Disaster Resilient Societies*, 2nd Edition, pp. 9-79. Tokyo: United Nations University Press.
- Blaikie, P., T. Cannon, I. Davis & B. Wisner (1994). *At Risk: Natural Hazards, People's Vulnerability, and Disasters*. London: Routledge.
- Boin, A. & A. McConnell (2007). Preparing for critical infrastructure breakdowns: the limits of crisis management and the need for resilience. *Journal of Contingencies and Crisis Management* 15(1): 50-59.
- Bompard, E., R. Napoli & F. Xue (2009). Analysis of structural vulnerabilities in power transmission grids. *International Journal of Critical Infrastructure Protection* 2(1-2): 5-12.
- Bouchon, S. (2006). *The vulnerability of interdependent critical infrastructures systems: epistemological and conceptual state of the art*. EUR 22205 EN. Ispra: Institute for the Protection and Security of the Citizen/European Commission.
- Bouchon, S. (2011). *Critical Infrastructures Identification: Reflexion about the European case*. PhD Thesis, Université de Nanterre Paris-X, France.
- Bouchon, S. & C. Dimauro (2012). Resilience: insights into the role of critical infrastructures disaster mitigation strategies. *Journal of Land Use, Mobility and Environment* 5(3): 103-117.
- Bouchon, S., C. Dimauro & P. Trucco (Eds.) (2012). *Proceedings of the 1st International Workshop on Regional Critical Infrastructure Protection Programmes: Main issues, Experiences and Challenges*, Milan, 17-18 November 2011. Milan: Lombardy Region. Archived by WebCite® at: <http://www.webcitation.org/6QPKwA22z>.
- Bruneau, M., S.E. Chang, R.T. Eguchi, G.C. Lee *et al.* (2003). A framework to quantitatively assess and enhance the seismic resilience of communities. *Earthquake Spectra* 19(4): 733-752.
- Brunner, E.M. & M Suter (2008). *An inventory of 25 national and 7 international critical information infrastructure protection policies*. International CIIP Handbook 2008/2009. Zurich: Center for Security Studies, ETH Zurich.
- Bunn, M. & O. Heinonen (2011). Preventing the next Fukushima. *Science* 333: 1580-1581.
- Cabinet Office (2010). Strategic framework and policy statement on improving the resilience of critical infrastructure to disruption from natural hazards. March 2010. London. Archived by WebCite® at: <http://www.webcitation.org/6Q2U9cifz>
- Cabinet Office (2013). *The role of local resilience forums: a reference document. The Civil Contingencies Act (2004), its associated Regulations (2005) and guidance, the National Resilience Capabilities Programme and emergency response and recovery*. Civil Contingencies Secretariat, July 2013 (V2). London. Archived by WebCite® at: <http://www.webcitation.org/6Q3gBXBuR>
- Cagno, E., M. De Ambroggi & P. Trucco (2011). Interdependen-

cy analysis of CIs in real scenarios. In: Berenguer, C., A. Grall & C. Guedes Soares (Eds.) *Advances in Safety, Reliability and Risk Management: ESREL 2011*, pp. 2508-2514. London: CRC Press.

Cardona, O.D. (2011). Disaster risk and vulnerability: notions and measurement of human and environmental insecurity. In: Brauch, H.G., U. Oswald Spring, C. Mesjasz, J. Grin *et al.* (Eds.) *Coping with Global Environmental Change, Disasters and Security: Threats, Challenges, Vulnerabilities and Risks* pp. 107-122. Berlin: Springer.

Cardona, O.D. & A.H. Barbat (2000). *El Riesgo Sísmico y su Prevención. [Earthquake risk and prevention.]* Cuaderno Técnico no.5. Madrid: Schneider Electric.

City of Cape Town (2006). Framework for adaptation to climate change in the city of Cape Town (FAC⁴T). Report submitted to City of Cape Town: Environment Resource Management, August 2006. Archived by WebCite® at: <http://www.webcitation.org/6Q3ggPs1j>

City of New York (2013). *A stronger, more resilient New York*. A PlaNYC report. URL: http://s-media.nyc.gov/agencies/sirr/SIRR_singles_Lo_res.pdf.

Cutter, S.L., L. Barnes, M. Berry, C. Burton *et al.* (2008). A place-based model for understanding community resilience to natural disasters. *Global Environmental Change* 18: 598-606.

De Bruijne, M. & M. van Eeten (2007). Systems that should have failed: Critical Infrastructure Protection in an institutionally fragmented environment. *Journal of Contingencies and Crisis Management* 15: 18-29.

DHS [U.S. Department of Homeland Security] (2009). *National Infrastructure Protection Plan. Partnering to enhance protection and resiliency*. Archived by WebCite® at: <http://www.webcitation.org/6QRhJzY8f>

DHS [U.S. Department of Home Affairs] & Public Safety Canada (2010). *Canada-United States Action Plan for Critical Infrastructure*. Archived by WebCite® at: <http://www.webcitation.org/6QRhFDyes>

Duckworth, M. (2012). *The resilience journey: the importance of people and communities at times of disaster*. Keynote speech at the 2nd International Workshop on Regional Critical Infrastructure Resilience, 15 November 2012, Edinburgh, UK.

EC [European Commission] (2004). *Communication from the Commission to the Council and the European Parliament: Critical Infrastructure Protection in the fight against terrorism*. COM(2004) 702 final. Brussels, 20th October 2004. Archived by WebCite® at: <http://www.webcitation.org/6QRhOqN7Q>

EC [European Commission] (2008). Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the

need to improve their protection. *Official Journal of the European Union* L 345: 75-82.

EC [European Commission] (2009). Principles of multi-risk assessment: interactions amongst natural and man-induced risks. Project report EUR23615. Brussels: EC. Archived by WebCite® at: <http://www.webcitation.org/6Q2OpmqPY>

Edwards, C. (2009). *Resilient Nation*. London: DEMOS. Archived by WebCite® at: <http://www.webcitation.org/6Q3hRrFQ1>

Fekete, A. (2012). Safety and security target levels: opportunities and challenges for risk management and risk communication. *International Journal of Disaster Risk Reduction* 2: 67-76.

Fekete, A., P. Lauwe & W. Geier (2012). Risk management goals and identification of critical infrastructures. *International Journal of Critical Infrastructures* 8(4): 336-353.

FMIG [Federal Ministry of the Interior of Germany] (2009). National strategy for critical protection (*CIP Strategy*). Berlin: FMIG. Archived by WebCite® at: <http://www.webcitation.org/6Q2Titf7U>

Folke, C. (2006). Resilience: the emergence of a perspective for social-ecological systems analyses. *Global Environmental Change* 16(3): 253-267.

Folke, C., S. Carpenter, T. Elmqvist, L. Gunderson *et al.* (2002). *Resilience and sustainable development: building adaptive capacity in a world of transformations*. Scientific Background Paper on Resilience for the process of The World Summit on Sustainable Development on behalf of The Environmental Advisory Council to the Swedish Government. April 2002. Stockholm: Environmental Advisory Council.

Füssel, H.-M. & R.J.T. Klein (2006). Climate change vulnerability assessments: an evolution of conceptual thinking. *Climatic Change* 75: 301-329.

Gallopin, G.C. (2006). Linkages between vulnerability, resilience, and adaptive capacity. *Global Environmental Change* 16: 293-303.

Garmezy, N., A.S. Masten & A. Tellegen (1984). The study of stress and competence in children: a building block for developmental psychopathology. *Child Development* 55: 97-111.

German Federal Government (2008). *Deutsche Anpassungsstrategie an den Klimawandel. [German strategy for adaptation to climate change.]* Decided by the Federal Cabinet on December 17, 2008 Archived by WebCite® at: <http://www.webcitation.org/6Q3haRrRU>

Gheorghe, A.V. & D.V. Vamanu (2005). Reading vulnerability in phase portraits: an exercise in probabilistic resilience assessment. *International Journal of Critical Infrastructures* 1(4): 312-329.

- Gheorghe, A.V. & D.V. Vamanu (2008). Quantitative vulnerability assessment of Critical Infrastructures: watching for hidden faults. *International Journal of Critical Infrastructures* 4(1/2): 144-152.
- Gheorghe, A.V., M. Masera, M. Weijnen & L. De Vries (2006). *Critical Infrastructure at Risk. Securing the European Electric Power System*. Dordrecht: Springer.
- Government of Finland (2006). *The strategy for securing the functions vital to society*. Government Resolution 23.11.2006, prepared by The Security and Defence Committee. Archived by WebCite® at: <http://www.webcitation.org/6Q3hh1csj>
- Greenberg, M., N. Mantell, M. Lahr, F. Felder & R. Zimmerman (2007). Short and intermediate economic impacts of a terrorist-initiated loss of electric power: case study of New Jersey. *Energy Policy* 35: 722-733.
- Gunderson, L.H. & C.S. Holling (Eds.) (2002). *Panarchy: Understanding Transformations in Human and Natural Systems*. Washington DC: Island Press.
- Hartong, M., R. Goel & D. Wijesekera (2008). Security and the US rail infrastructure. *International Journal of Critical Infrastructure Protection* 1: 15-28.
- Hellström, T. (2007). Critical infrastructure and systemic vulnerability: towards a planning framework. *Safety Science* 45: 415-430.
- Hémond, Y. & B. Robert (2012). Evaluation of state of resilience for a critical infrastructure in a context of interdependencies. *International Journal of Critical Infrastructures* 8(2/3): 1-18.
- Her Majesty the Queen in Right of Canada (2009). *Action plan for critical infrastructure*. Archived by WebCite® at: <http://www.webcitation.org/6QRhtYqx3>.
- HM Government [Her Majesty's Government] (2010). *A strong Britain in an age of uncertainty: the national security strategy*. Presented to Parliament by the Prime Minister by Command of Her Majesty. London: The Stationery Office Limited. Archived by WebCite® at: <http://www.webcitation.org/6QRhxaIGZ>.
- Holling, C.S. (1973). Resilience and stability of ecological systems. *Annual Review of Ecology and Systematics* 4: 1-23.
- Holling, C.S. (1996). Engineering resilience versus ecological resilience. In: Schulze, P. (Ed.). *Engineering Within Ecological Constraints*, pp. 31-44. Washington DC: The National Academies Press.
- Holling, C.S. (2001). Understanding the complexity of economic, ecological, and social systems. *Ecosystems* 4: 390-405.
- IRGC [International Risk Governance Council] (2006). *Managing and reducing social vulnerabilities from coupled critical infrastructures*. White paper. Geneva: IRGC.
- IRGC [International Risk Governance Council] (2010). *Emerging risks: sources, drivers and governance issues*. Concept note. Revised version, March 2010. Geneva: IRGC.
- Klein, K.R., M.S. Rosenthal & H.A. Klausner (2005). Blackout 2003: preparedness and lessons learned from the perspectives of four hospitals. *Prehospital and Disaster Medicine* 20(5): 343-349.
- Klein, R.J.T., R.J. Nicholls & F. Thomalla (2003). Resilience to natural hazards: how useful is this concept? *Global Environmental Change Part B: Environmental Hazards* 5(1-2): 35-45.
- Kröger, W. (2008). Critical infrastructures at risk: a need for a new conceptual approach and extended analytical tools. *Reliability Engineering and System Safety* 93: 1781-1787.
- Kröger, W. & E. Zio (2011). *Vulnerable Systems*. London: Springer.
- Lauwe, P. & C. Riegel (2008). Schutz Kritischer Infrastrukturen: Konzepte zur Versorgungssicherheit. [Critical infrastructure protection: concepts for security of supply.] *Informationen zur Raumentwicklung* 1/2: 113-125.
- Lhomme, S., D. Serre, Y. Diab & R. Laganier (2013). Assessing the resilience of the urban networks: a preliminary step towards more flood resilient cities. *Natural Hazards and Earth System Sciences* 13: 221-230.
- Li, Q., J. Sun & J. Fan (2012). Seismic vulnerability assessment through explicit consideration of uncertainties in structural capacities and structural demands. *International Journal of Structural Engineering* 3(1/2): 27-36.
- Luijff, E., H. Burger & M. Klaver (2003). Critical infrastructure protection in the Netherlands: a quick-scan. In: Gattiker, U.E. (Ed.) *EICAR 2002 Conference Best Paper Proceedings* (ISBN: 87-987271-2-5). Copenhagen: EICAR.
- Magis, K. (2010). Community resilience: an indicator of social sustainability. *Society & Natural Resources: An International Journal* 23(5): 401-416.
- Monstadt, J. (2008). Der räumliche Wandel der Stromversorgung und die Auswirkungen auf die Raum- und Infrastrukturplanung. [The spatial change of the power supply and the impact on the spatial and infrastructure planning.] In: Moss, T., M. Naumann & M. Wissen (Eds.). *Infrastrukturnetze und Raumentwicklung: Zwischen Universalisierung und Differenzierung [Infrastructure Networks and Spatial Development: Between Universalization and Differentiation]*, pp. 187-224. Munich: Oekom.
- NIAC [National Infrastructure Advisory Council] (2009). *Critical infrastructure resilience: final report and recommendations*. September 8, 2009. Archived by WebCite® at: <http://www.webcitation.org/6QRi1SkGQ>.

- Norwegian CIP Commission (2006). *Protection of critical infrastructures and critical societal functions in Norway*. Report NOU 2006:6 submitted to the Ministry of Justice and the Police by the government appointed commission for the protection of critical infrastructure on 5th of April 2006 Archived by WebCite® at: <http://www.webcitation.org/6Q3huvEYC>
- Paton, D. & D. Johnston (2000). Disasters and communities: vulnerability, resilience and preparedness. *Disaster Prevention and Management* 10(4): 270 - 277.
- Paton, D. & D. Johnston (Eds.) (2006). *Disaster Resilience: An Integrated Approach*. Springfield: Charles C. Thomas.
- Pelling, M. (2011). *Adaptation to Climate Change: From Resilience to Transformation*. London: Routledge.
- Perelman, L.J. (2006). *Shifting security paradigms. Toward resilience*. CIPP Working Paper 10-06. Arlington, VA: George Mason University. Archived by WebCite® at: <http://www.webcitation.org/6Q2PYzlz>
- Petit, F., W. Buehring, R. Whitfield, R. Fisher & M. Collins (2011). Protective measures and vulnerability indices for the Enhanced Critical Infrastructure Protection Programme. *International Journal of Critical Infrastructures* 7(3): 200-219.
- PCCIP [President's Commission on Critical Infrastructure Protection] (1997). *Critical foundations: protecting America's infrastructure*. The Report of the President's Commission on Critical Infrastructure Protection, October 1997. Washington: PCCIP. Archived by WebCite® at: <http://www.webcitation.org/6Q3iBqPud>
- Pursiainen, C. (Ed.) (2007). *Towards a Baltic Sea region strategy in Critical Infrastructure Protection*. Nordregio Report 2007: 5. Stockholm: Nordregio (Nordic Center for Spatial Development). Archived by WebCite® at: <http://www.webcitation.org/6Q3iG90hh>
- Reed, D.A., K.C. Kapur & R.D. Christie (2009). Methodology for assessing the resilience of networked infrastructure. *IEEE Systems Journal* 3(2): 174-180.
- Reichenbach, G., H. Wolff, R. Göbel & S. Stokar von Neuforn (2008). *Risiken und Herausforderungen für die öffentliche Sicherheit in Deutschland: Szenarien und Leitfragen*. Grünbuch des Zukunftsforums Öffentliche Sicherheit. [Risks and challenges for public security in Germany: scenarios and questions. Green Paper of the future forum public safety.] Berlin: Zukunftsforums Öffentliche Sicherheit. Archived by WebCite® at: <http://www.webcitation.org/6Q2UfyJeG>
- Rich, E., J.J. Gonzalez, Y. Qian, F.O. Sveen, J. Radianti & S. Hilten (2009). Emergent vulnerabilities in Integrated Operations: a proactive simulation study of economic risk. *International Journal of Critical Infrastructure Protection* 2(3): 110-123.
- Rinaldi S.M., J.P. Peerenboom & T.K. Kelly (2001). Identifying, understanding and analyzing critical infrastructure interdependencies. *IEEE Control Systems Magazine* 21 (6): 12-25.
- Robert, B. & L. Morabito (2010). An approach to identifying geographic interdependencies among critical infrastructures. *International Journal of Critical Infrastructures* 6(1): 17-30.
- Rutter, M. (1985). Resilience in the face of adversity. Protective factors and resistance to psychiatric disorder. *The British Journal of Psychiatry* 147: 598-611.
- Scottish Government (2011). *Secure and resilient: a strategic framework for critical national infrastructure in Scotland*. Edinburgh: The Scottish Government. Archived by WebCite® at: <http://www.webcitation.org/6Q3iPsVtR>
- Serre, D., B. Barroca & R. Laganier (2013). *Resilience and Urban Risk Management*. New York: CRC Press.
- Smit, B. & J. Wandel (2006). Adaptation, adaptive capacity and vulnerability. *Global Environmental Change* 16(3): 282-292.
- Suter, M. (2011, November). *PPP models for CIP implementation at regional level*. Paper presented at the 1st International Workshop on Regional Critical Infrastructure Protection Programmes: Main Issues, Experiences and Challenges, 17-18 November 2011, Milan, Italy.
- Svensson, G. (2008). Mutual and interactive vulnerability in supply-chain dyads. *International Journal of Logistics Economics and Globalisation* 1(2): 123-140.
- The White House (2013). *Critical infrastructure security and resilience*. Presidential Policy Directive/PPD-21, February 12, 2013. Archived by WebCite® at: <http://www.webcitation.org/6Q3iVRiUP>
- Thomassen, E. (2012, November). *Critical Infrastructure Resilience: the Norwegian approach*. Paper presented at the 2nd International Workshop on Regional Critical Infrastructure Resilience, 15 November 2012, Edinburgh UK.
- Tierney, K. & M. Bruneau (2007). Conceptualizing and measuring resilience. A key to disaster loss reduction. *TR News* 250(May-June): 14-17.
- TISP [The Infrastructure Security Partnership] (2006). *Regional Disaster Resilience: A Guide for Developing an Action Plan*. Reston, Virginia: ASCE [The American Society of Civil Engineers. Archived by WebCite® at: <http://www.webcitation.org/6Q3ia2Lo4>
- TNO [Toegepast Natuurwetenschappelijk Onderzoek] (2011). *RECIPE [Recommended Elements of Critical Infrastructure Protection]: Good Practices Manual for Policy Makers in Europe*. TNO. Archived by WebCite® at: <http://www.webcitation.org/6Q3ieefLF>

Tobin, G.A. (1999). Sustainability and community resilience: the holy grail of hazards planning? *Global Environmental Change Part B: Environmental Hazards* 1(1): 13-25.

Toubin, M., R. Laganier, S. Gomez, Y. Diab & D. Serre (2014). Improving the conditions for urban resilience through interdependencies identification and collaborative learning between Parisian urban services. *Journal of Urban Planning and Development*, ASCE (in press).

Trucco, P., E. Cagno & M. De Ambroggi (2011). Dynamic functional modelling of vulnerability and interoperability of Critical Infrastructures. *Reliability Engineering and System Safety* 105: 51-63.

Tyler, S. & M. Moench (2012). A framework for urban climate resilience. *Climate and Development* 4(4): 311-326.

UNISDR [International Strategy for Disaster Reduction] (2007). *Hyogo Framework for Action 2005-2015: building the resilience of nations and communities to disasters*. Extract from the final report of the World Conference on Disaster Reduction (A/CONF.206/6). Geneva: United Nations. URL: http://www.ISDR.org/files/1037_hyogoframeworkforactionenglish.pdf

Vugrin, E.D., D.E. Warren, M.A. Ehlen & R.C. Camphouse (2010). A framework for assessing the resilience of infrastructure and economic systems. In: Gopalakrishnan, K. & S. Peeta (Eds.) *Sustainable and Resilient Critical Infrastructure Systems*, pp. 77-116. Heidelberg: Springer.

Walker, B.H., C.S. Holling S.R. Carpenter & A.P. Kinzig (2004). Resilience, adaptability and transformability in social-ecological systems. *Ecology and Society* 9(2): 5.

Wise, C.R. (2006). Organizing for homeland security after Katrina: is adaptive management what's missing? *Public Administration Review* May/June: 302-318.