Defining Policies to Improve Critical Infrastructure Resilience

Leire Labaka
TECNUN, University of Navarra
llabaka@tecnun.es

Josune Hernantes
TECNUN, University of Navarra
jhernantes@tecnun.es

Tina Comes
University of Agder
Tina.comes@uia.no

Jose Mari Sarriegi
TECNUN, University of Navarra
jmsarriegi@tecnun.es

ABSTRACT

Industrial accidents increasingly threaten society and economy; the increasing exposure and vulnerability of our modern interlaced societies contributes to intensifying their impact. Critical Infrastructures (CIs) have a prominent role, since they are vital for the welfare of the population and essential for the economic growth. As hazards are hard to predict, decision-makers need to implement adequate adaptation and mitigation strategies to improve CI resilience.

Although CI resilience has attracted increasing attention, empirical studies are rare. Research on the implementation of policies aiming at identifying a clear sequence of measures to improve CI resilience is lacking. Therefore, we present a framework to identify resilience policies across four dimensions (technical, organizational, economic and social) and to define the temporal order in which the policies should be implemented. This research provides a framework grounded in our empirical work. Future work will aim at developing quantitative approaches to complement our results.

Keywords

Critical Infrastructure Protection, Resilience, Group Model Building, Delphi Method, Sequential Decision-Making, Vulnerability

INTRODUCTION

Advances in Critical Infrastructures (CIs), such as modern information and communication technologies, smart grids, and better health care systems, have significantly improved societal welfare over the last decades; at the same time our lives and economic prosperity have become dependent on their functioning (Commission of the European Communities, 2005). Therefore, their reliability and safety level should be high. Furthermore, CIs have become increasingly interdependent (Rinaldi, 2004). For example, if a power outage occurs, this crisis can rapidly spreads through other CIs such as health care and transportation causing further disruptions and cascading effects. As CIs are highly interconnected and embedded in a socio-economic system, it is often difficult to predict how a crisis might evolve or what systems would be affected. Moreover, some crises may cross national borders affecting other countries.

Recent natural hazards such as hurricane Sandy in the US or the Typhoon Haiyan in the Philippines have illustrated the vulnerability of our society and CIs (Beck, 2012; Lum and Margesson, 2013; The United Nations Office for Disaster Risk Reduction, 2013). Creating resilient systems, which are able to cope with critical expected and unexpected situations, is essential to deal with these threats. Resilience and vulnerability represent two related approaches to describe the response of systems and actors to changes, which can be trends (such as global warming) or shocks (such as extreme weather events). Their respective origins in ecological and sustainability science, engineering, or risk management explain the continuing differences in the discussions about both terms. In the context of disaster management, the term vulnerability usually refers to the ‘‘*conditions*

determined by physical, social, economic and environmental factors or processes which increase the susceptibility […] to the impact of hazards" (UN/ISDR, 2004).

Regarding resilience, literature provides several definitions regarding this concept. As Moteff (2012, p. 2) states "*There are almost as many definitions of resilience as there are people defining it*". The definitions can be characterized by two different perspectives: some authors define resilience as the capacity to bounce back to a normal state after the impact of a triggering event (Longstaff, 2005; Mileti, 1999; McEntire, 2005) while others expand this definition describing resilience as the capacity to cope with a crisis that as it occurs and to prevent a triggering event to occur (Bruneau et al., 2003; Kahan et al., 2009; Seville et al., 2008; Hollnagel et al., 2006).

We follow the second perspective and define resilience as the capacity of a system to prevent a crisis occurrence and, if an event impacts the system, the capacity of the system to absorb the impact and recover rapidly. Within this definition, the following four resilience dimensions have been distinguished (Bruneau et al., 2003; MCEER, 2008; Zobel, 2010):

- *Technical resilience* refers to the capacity of an organization's physical system to perform sufficiently well when exposed to a hazard event.
- *Organizational resilience* refers to the capacity of crisis managers to make decisions and take actions that avoid a crisis or reduce its impact.
- *Economic resilience* relates to the capacity of the organization to balance the extra costs from a crisis.
- *Social resilience* refers to the ability of society to reduce the impact of a crisis, e.g., help to first responders or act as volunteers.

Thus, in order to improve their resilience level, it is important to implement policies based on these four dimensions. Moreover, as the number of agents involved in crisis management has increased, the involved actors need to be integrated and coordinated. Actually, external stakeholders such as government, first responders and society play also an important role in managing crises (Labaka, 2013). Their adequate preparation is of utmost importance in order to properly deal with crises. Therefore, policies need to be aligned across all actors in order to improve the resilience level of CIs. Beyond this cross-organizational perspective, it is also important to consider the temporal sequence of resilience policies in order to achieve the highest efficiency in their implementation what will help to accomplish a higher resilience level. In light of this situation this research aims to provide a holistic resilience framework to improve the resilience level of CIs, firstly defining the resilience policies that should be implemented and secondly, describing the implementation methodology where the temporal order in which the policies should be implemented is defined.

STATE OF THE ART

There are several theories and frameworks in the literature about improving organizational resilience. High Reliability Organizations (HROs) have been defined as those organizations that operate complex and high-risk technologies and manage to remain accident free for long periods of time (Roberts and Rousseau, 1989; Roberts, 1990). HROs are defined by several characteristics and processes that help them to reach and maintain high reliability levels (Weick and Sutcliffe, 2007; Lekka, 2011). More recently, a research group in New Zealand called "Resilient Organisations" developed a framework to build up the organizations´ resilience level. This framework is composed of thirteen indicators grouped into three attributes: leadership and culture, networks, and change ready (Resilient Organisations, 2012). In the same vein, Parsons describes eight key attributes of organizations to be resilient based on a workshop conducted by Trusted Information Sharing Network´s Community of Interests (Parsons, 2007). However, all frameworks focus on organizational resilience, without providing any information about how to improve the rest of the resilience dimensions (technical, economic, and social). Besides, the principles are very theoretical and they lack to describe the path forward to their implementation in practice.

Johnsen (2010) takes a step forward and describes seven principles based on organizational and technical aspects that organizations need to fulfill to be resilient. Nonetheless, as in the earlier cases, the processes, the order, and transformations required to create resilience building activities are not specified. On the other hand, Cutter et al. (2010) define a set of indicators to evaluate disaster resilience levels and in turn, the efficiency of the established policies that foster the resilience level. However, these policies focus on social resilience and, therefore, they do not provide specific policies for CI providers. Furthermore, little is stated about how to improve these indicators.

Literature provides a broad set of works discussing general characteristics and principles about how to build the CIs resilience level. However, it still lacks a detailed prescription for crisis managers about which activities should be carried out and how resilience principles should be transformed to apply them in practice (Boin and

Van Eeten, 2013; Lekka and Sugden, 2011; Waller and Roberts, 2003). In addition, almost all the principles still focus on activities within the boundaries of the CI, neglecting the role of external agents and their influence on improving the CIs resilience.

Thus, this research aims to present a holistic resilience framework which consists of a list of resilience policies defined taking into account internal and external stakeholders and covering the four resilience dimensions. Additionally, an implementation methodology has also described which identifies the temporal order in which these resilience policies should be implemented to achieve the highest efficiency. This framework has been defined based on empirical data gathered from experts in the field as well as analyzing past major industrial accidents.

RESEARCH METHODOLOGY

The methodology used in this research consists of two main phases: (1) identification of the resilience policies and (2) development of the implementation methodology of the resilience policies.

In order to identify the resilience policies several iterations applying different research methods were carried out. First, a collaborative method called Group Model Building (GMB) was used to gather knowledge from the experts. GMB is a collaborative methodology, which enables integrating fragmented knowledge, initially residing on the minds of different agents, into aggregated models (Richardson and Andersen, 1995). Three workshops were arranged in San Sebastian (Spain) within the context of the SEMPOC European project (Simulation Exercise to Manage Power Cut Crises) in the field of Critical Infrastructure Protection (CIP) during 2009-2011. Fifteen experts from different fields such as energy companies, first responders, and organizations for civil protection, health care and CI protection took part in the process. The workshops provided a wealth of information about the variety of perspectives on crisis management. Additionally, the exercises carried out during these sessions allowed the identification of the stakeholders taking part in the crisis management process, the identification of indicators and their reference modes, and the policies to build the system's resilience level. Hernantes et al. (2012a; 2012b) explain in great detail the activities carried out and the obtained results. As a starting point of our research, eight resilience policies to build the system's resilience level that experts identified during the workshops composed the preliminary version of the resilience policies.

In order to validate the initial list of policies, several previous large-scale crises were analyzed using the multiple case studies method (Yin, 1994). Major nuclear accidents, blackouts, oil spills, mining accidents and air traffic accidents were studied to obtain evidence of the consequences of having a low or high degree of effective implementation of each policy and to complete the initial list of policies. The cases were selected based on the available information and magnitude of the impact. Through this study, the list of policies was improved and the second version of the resilience policies for CIs was developed. This version together with the analysis of past major crises is deeply explained in the following article (Labaka et al., 2013).

However, this second version of the framework still required more corroboration from experts in order to affirm the suitability of the defined policies in other CI sectors. This research applied the Delphi method to refine and to extend the list of the resilience policies. Delphi is a systematic and iterative process for structuring a group communication process in order to obtain a consensus about a complex problem (Dalkey, 1969; Linstone and Turoff, 1975; Okoli and Pawlowski, 2004). Fifteen multidisciplinary experts from different sectors (academics, transport, energy, and first responders) took part in the process. As a result, an improved version of the list of policies was obtained. Labaka (2013) explains in great detail how the Delphi process was carried out, the experts' contribution and the final list of policies. This framework is a holistic framework defined based on the knowledge of multidisciplinary experts with different backgrounds.

Moving to the second phase of the methodology, similarly to the first part, experts´ knowledge was used to obtain information. The survey was chosen as a research method to gather knowledge from the experts about the most convenient order of implementing the policies. A survey consists of a systematic and standardized approach to collect information from a large group of people through questionnaires (Marsden and Wright, 2010; Forza, 2002).

A sample of forty-five experts from all over the world in the field of crisis management and CIs was selected from different sectors such as energy, transport, telecommunications, water, academic, first responders, and national civil protection. We selected a web-tool based questionnaire to perform the survey since it is cheap and easy to use by the experts, it avoids loss of data, and provides the fastest way to answer to the questionnaire.

Before sending the questionnaire to experts, a pilot study was conducted. As a result of the pilot study, changes were made to the formulation of some questions that helped to improve the questionnaire. In order to start the data collection, a cover letter explaining the aim of the research, the general instructions of the survey and the

link to access to the questionnaire were sent to the experts. They had two weeks to answer to the questionnaire. The experts were asked to provide the temporal order in which the policies should be implemented in order to achieve a higher efficiency in their implementation. In total, twenty-five experts from all over the world and from different fields such as transport, energy, water, telecommunications and academic took part in the survey. The developed implementation methodology will be further explained below.

RESULTS: RESILIENCE POLICIES

In total, sixteen resilience policies were defined grouped into four resilience dimensions (technical, organizational, economic and social). Some of them belong to internal resilience, that is, they are implemented to improve the resilience level of the CI where the triggering event occurs and the others belong to external resilience, which refer to the resilience level of the rest of involved agents. In turn, internal resilience has been divided into three resilience dimensions (technical, organizational and economic resilience) whilst for external resilience, four resilience dimensions have been established (technical, organizational, economic, and social). Then, resilience policies have been defined within each resilience dimension (see Table 1) taking into account private and public companies and covering the whole crisis lifecycle (prevention, preparation, response and recovery). Below, the resilience policies are explained.

INTERNAL RESILIENCE		EXTERNAL RESILIENCE	
TECHNICAL RESILIENCE	CI Safety Design and Construction	TECHNICAL RESILIENCE	External Crisis Response Equipment
	CI Maintenance		
	CI Data Acquisition and Monitoring System		
	CI Crisis Response Equipment		
ORGANIZATIONAL RESILIENCE	CI Organizational Procedures for Crisis Management	ORGANIZATIONAL RESILIENCE	First Responder Preparation
	CI Top Management Commitment		Government Preparation
	CI Crisis Manager Preparation		Trusted Network Community
	CI Operator Preparation		Crisis Regulation and Legislation
ECONOMIC RESILIENCE	CI Crisis Response Budget	ECONOMIC RESILIENCE	Public Crisis Response Budget
		SOCIAL RESILIENCE	Societal Situation Awareness

Table 1: Resilience Policies classified by the resilience dimension and the resilience type.

CI Safety Design and Construction

This policy refers to the safety level of CI to avoid a crisis occurrence and to absorb the magnitude of the impact efficiently. Having safety sub-systems and redundant components and sub-systems allow preventing a crisis occurrence and ensuring the functioning of the CI (Bruneau et al., 2003; Johnsen, 2010). However, having a complex system with many additional redundant and safety systems makes it difficult to manage and control its functioning (Perrow, 1984; Leveson et al., 2009; Sagan, 2004). Therefore, when designing the CI, it is important to reduce complexity and tight relationships. Internal and external audits should also be carried out to ensure the proper functioning of the CI.

CI Maintenance

Not only should the CI be well designed and built, but high quality maintenance activities must also be performed periodically in order to guarantee a high level of reliability of the infrastructure. Having a good level of maintenance helps to withstand incidents and also reduces the magnitude of the impact and the time to recover.

CI Data Acquisition and Monitoring System

Having systems to monitor the state of the CI would help to ensure its proper state. Setting up the required

sensors to gather information from the CI and installing adequate software to monitor the CI performance are some of the main activities that should be carried out in order to achieve a high implementation level of this policy.

CI Data Acquisition and Monitoring System

Having systems to monitor the state of the CI would help to ensure its proper state. Setting up the required sensors to gather information from the CI and installing adequate software to monitor the CI performance are some of the main activities that should be carried out in order to achieve a high implementation level of this policy.

CI Crisis Response Equipment

This policy refers to the emergency equipment that the CI should have when a crisis occurs to absorb the impact and ensure the safety of the workers at the CI. Emergency equipment should be reliable to ensure its proper functioning when it is required and should be available to be able to use it when a crisis occurs.

CI Organizational Procedures for Crisis Management

This policy corresponds to the preparation and the capacity of the organization to deal with crises and incidents as well as the ability to coordinate with external stakeholders such as government and first responders. CIs should develop crisis management and coordination procedures with external stakeholders in order to have the response actions and the responsibilities of each worker well defined before a crisis occurs.

CI Top Management Commitment

Top managers should be committed to the resilience building process and they have to promote a resilience-based culture, attitudes and values within the CI. They are responsible for deploying resources to promote the workers' commitment and training and to establish the required technical measures to prevent a crisis occurrence and absorb the impact.

CI Crisis Manager Preparation

Crisis managers' preparation corresponds to the capacity of crisis managers to detect early warning signals, communicate to the stakeholders and analyze triggering events to propose new preventive measures for the future. In addition to this, managers also have to develop their sensemaking capacity (Gilpin and Murphy, 2008), which refers to be ability to understand an unexpected event, adapt to it, and make the correct decisions in a stressful situation and without complete information.

CI Operator Preparation

Operators at the CI must be adequately trained prior to the occurrence of a crisis so they know how to respond when a crisis does occur. Operators should take training courses to know the response procedures and protocols and develop their response and coordination abilities (Resilient Organisations, 2012). Operators should also be committed with the safety of the company since they can help detecting early warning signals and avoiding a crisis occurrence (Resilient Organisations, 2012).

CI Crisis Response Budget

When a triggering event occurs, monetary resources are needed to absorb the impact and recover to the initial state as soon as possible. CIs should have monetary resources set aside in order to cover repairs and replacements just after the triggering event happens and until an acceptable level of performance that guarantees society's welfare is achieved (Resilient Organisations, 2012).

External Crisis Response Equipment

External stakeholders such as first responders, government and society should also have reliable and adequate equipment to cope with crisis. Furthermore, having redundant equipment would ensure the availability of this

equipment when a component or a subsystem gets damaged. CIs should advise external stakeholders about the required equipment, especially when specific equipment is needed. In case of a severe crisis, equipment could also be gathered from foreign countries.

First Responder Preparation

This policy refers to how first responders (fire fighters, emergency units, policemen, military, etc.) are prepared to face a crisis. Prior to the occurrence of a crisis, they should be trained to know how to absorb and bounce back from a crisis and learn about the special characteristics of their closest CIs in order to be able to properly respond when a crisis occurs. Actions such as how to act in dangerous environments and how to organize themselves and coordinate with each other need to be defined before a critical event takes place.

Government Preparation

The government should be well prepared for crisis management. The government should be aware of the possible incidents that could lead to a big crisis and should be committed to the crisis management process. The government should develop response procedures and acquire leaderships and communication skills to manage and inform properly in case of a crisis (Carrel, 2000; Boin, 2009). Furthermore, members of the government are also responsible for coordinating efficiently the network of stakeholders involved in the absorption and recovery activities (Carrel, 2000; Boin, 2009).

Trusted Network Community

Creating a network of stakeholders (CI owners, regulators, government, etc.) in which agents involved in a crisis can trust each other to share experiences and lessons learned may improve their crisis management knowledge and the number of collaboration agreements to help in crisis prevention and resolution (Ruffner et al., 2010; Snyder and de Souza Briggs, 2003; Wenger et al., 2002; Resilient Organisations, 2012). These networks should promote research in the field of CI protection and safety to improve CIs resilience level.

Crisis Regulation and Legislation

This policy refers to the maturity level and compliance level of the regulations and laws. Having well defined and updated regulation and legislation results in more safe and better prepared infrastructures to avoid a crisis occurrence and to better handle it. Furthermore, the regulations and laws should be regularly updated and reviewed to identify responsibilities in case a crisis occurs.

Public Crisis Response Budget

As in the case of the CI Crisis Budget, public institutions should have a pool of money set aside in case a crisis occurs, in order to help the stakeholders and society. This extra funding allows organizations, society and first responders to obtain resources within a reasonable time. Monetary resources will allow performing activities, repairing and rebuilding damaged physical systems and compensating the affected CIs and people.

Societal Situation Awareness

Not only should the government and first responders prepare to handle crises but society can also play an important role in a crisis resolution. The situation awareness and commitment of society towards avoiding a crisis occurrence reduces crisis probability and reduces the magnitude of the impact, with better ability to respond (Resilient Organisations, 2012; Shaw et al., 2009). Furthermore, the collaboration and information that society can provide may be crucial to enhance crisis management.

RESULTS: IMPLEMENTATION METHODOLOGY OF THE RESILIENCE POLICIES

The resilience policies are closely related each other since some of the policies require others prior implementation to be efficiently applied. Moreover, due to scarce resources and time pressure not all the policies should be implemented at the same moment since some of them take longer to have effect than others. Therefore, this research has developed an implementation methodology to establish the temporal order in which the policies should be implemented to achieve the highest efficiency in the implementation of these resilience policies in practice.

Defining the exact order in which the policies should be implemented is not an easy task since policies are interdependent and some effects may take long to be observed. After analyzing the results provided by experts we concluded that there are some policies that need to be implemented at the beginning of the process since they are required for the implementation of others. In turn, others are placed in the last positions as they necessarily must be built on previous policies. Finally, there are also some policies which require others implementation but they also affect in the efficiency of others. Therefore, in order to achieve more realistic and coherent results, we divided the implementation process into five stages. Although each policy starts its implementation in one phase, afterwards, the policies should continue developing over time. Table 2 illustrates the implementation methodology of the resilience policies divided into five main stages.

First Stage

There are two policies that are the driving forces to begin, promote, and encourage the improvement of resilience in CIs. First, having a safely designed and built infrastructure is essential to improve the resilience of CIs. Second, the commitment of top management towards the resilience building process is vital to allocate resources, promote a resilience based culture, and increase the engagement of the workers.

Second Stage

Two new policies would be added to the previous ones in the second stage. Not only CI needs to be well designed and built but maintenance activities should also be carried out to ensure the reliability of the components and CIs and avoid the accumulation of errors. Therefore, *CI maintenance* policy should start its implementation in this second stage. Together with technical issues, *CI Organizational Procedures for Crisis Management* should also be developed to properly manage crises. Internally, the CI should prepare to be able to deal with a crisis. Guidelines about what activities should be carried out, responsibilities of each worker and coordination procedures with external stakeholders should also be established to better handle crises.

	Resilience Dimensions	Resilience Policies	1st stage	2nd stage	3rd stage	4th stage	5th stage
INTERNAL RESILIENCE	TECHNICAL RESILIENCE	CI Safety Design and Construction					
		CI Maintenance					
		CI Data Acquisition and Monitoring System					
		CI Crisis Response Equipment					
	ORGANZIATIONAL RESILIENCE	CI Organizational Procedures for Crisis Management					
		CI Top Management Commitment					
		CI Crisis Manager Preparation					
		CI Operator Preparation					
	ECONOMIC RESILIENCE	CI Crisis Response Budget					
EXTERNAL ERSILIENCE	TECHNICAL RESILIENCE	External Crisis Response Equipment					
	ORGANIZATIONAL RESILIENCE	First Responder Preparation					
		Government Preparation					
		Trusted Network Community					
		Crisis Regulation and Legislation					
	ECONOMIC RESILIENCE	Public Crisis Response Budget					
	SOCIAL RESILIENCE	Societal Situation Awareness					

Table 2: The Implementation Methodology of the Resilience Policies

Third Stage

In this step, five new policies are introduced. First, *CI Data Acquisition and Monitoring Systems* should be implemented through the infrastructure to gather information about the state of the infrastructure and be able to anticipate any incident. Second, *CI Crisis Response Equipment* has also to be acquired in order to be able to absorb the impact and ensure the safety of the workers. Third, the *CI Crisis Manager Preparation* is introduced in this step since they are the ones responsible for detecting early warning signals, analyzing them and communicating to the corresponding person. They are continuously aware of any possible incident and they have the responsibility for preparing the organization to perform efficiently in face of a crisis. Fourth, the *Government Preparation* should be improved since the government also plays an important role in crisis management. It has the authority and the capacity to increase the external entities' awareness and commitment towards resilience building process and it can afford resources to acquire equipment and help in the crisis resolution. Fifth, together with the fourth policy, the government and its public entities should develop *crisis regulations and laws* in order to establish the minimum requirements that CIs need to ensure their safety and high reliability. It is worth noting that these last two policies should be constantly improved and provided with feedback.

Fourth Stage

CI Operator Preparation, *CI Crisis Response Budget*, and *First Responder Preparation* policies are implemented in this stage. Once the top management is committed, the crisis management procedures are established, and crisis managers are well prepared, operators should be prepared to face crises. They receive training courses and make some table-top exercises and emergency drills to improve their crisis management skills and awareness. Furthermore, CIs have to set aside some monetary resources or contract for insurance to be able to absorb the extra costs that arise from a crisis. Externally, the preparation of first responders must be improved to ensure their proper response in case of a crisis.

Fifth Stage

Finally, in this stage, the last external policies are implemented. In order to be able to respond appropriately it is important that external entities have reliable and sufficient response equipment (*External Crisis Response Equipment*). Furthermore, a *Trusted Network Community* has to be created where stakeholders share information and experiences with other involved agents and improve their crisis management knowledge. The *Public Crisis Response Budget* is also improved in order to have monetary resources to be able to respond to crises. Finally, the *Societal Situation Awareness* is enhanced since society can help to handle a crisis or also avoiding its occurrence or at least not making it worse. Society should be aware about the crisis occurrence and prepared to cope with crises in the most efficient way.

CONCLUSIONS, LIMITATIONS AND FUTURE RESEARCH

This research proposes a holistic framework to improve the resilience level in CIs that is grounded in our empirical findings. Future work will start from the specifics of each CI sector, which has its own features and therefore, differences may appear in the implementation methodology, i.e., setting the temporal order in which the policies should be implemented. Therefore, it would be interesting to particularize the implementation methodology defined in this research for each CI sector (energy, health and transport among others) in order to analyze similarities and differences among sectors.

Moreover, the time scope of each implementation phase is currently not specified. Besides, the phases might have unequal lengths: some policies, it might take weeks, months or years to develop it. As time passes, however, new developments and trends can occur requiring an update and re-prioritization. Furthermore, (direct and indirect) cause-effect relations among the resilience policies should be established to provide more insights about which policies require others prior implementation or if one policy can start its development in a following stage without finishing the development of the policies defined in the previous stage.

The proposed implementation methodology will therefore be extended in future: we aim to complete and validate it with further research by adopting other methodologies such as sequential decision making methods to determine the temporal order. While the research presented in this paper assumes that decision makers address isolated, i.e. single decision problems that can be solved independently from one another, in future we will extend this methodology by focusing on interdependent decisions. This comprises interdependencies across

different actors and organizations as well as temporal interdependencies as outlined in (Comes, 2013).

Therefore, our research will continue validating and completing the implementation methodology (i) by particularizing the implementation methodology to each CI sector, (ii) by gathering information about measures or conditions that define the end of each stage, and (iii) by applying other research methods to define the relations between implementation policies and environment that determine requirements of each policy.

REFERENCES

1. Beck, C., 2012. Critical Infrastructure Resilience: What we can learn from hurricane Sandy, *Security Center - Center for National Policy.* Available at: http://cnponline.org/ht/d/ViewBloggerThread/i/40897/pid/35636.
2. Boin, A. (2009) The new world of crises and crisis management: Implications for policymaking and research, *Review of Policy Research*, 26, 4, 367-377.
3. Boin, A. and Van Eeten, M.J.G. (2013) The Resilient Organization, *Public Management Review*, 15, 3, 429-445.
4. Bruneau, M., Chang, S., Eguchi, R., Lee, G., O'Rourke, T., Reinhorn, A., Shinozuka, M., Tierney, K., Wallace, W. and von Winterfelt, D. (2003) A framework to quantitatively assess and enhance seismic resilience of communities, *Earthquake Spectra*, 19, 733-52.
5. Carrel, L.F. (2000) Training civil servants for crisis management, *Journal of Contingencies and Crisis Management*, 8, 4, 192-196.
6. Comes, T. (2013) Robust emergency management strategies: Providing support for sequential decisions, *Proceedings of 46th Hawaii International Conference On System Sciences (HICSS 46)*, Mauii, Hawaii.
7. Commission of the European Communities (2005) *Green Paper on a European Programme of Critical Infrastructure Protection*, Brussels.
8. Cutter, S.L., Burton, C.G. and Emrich, C.T. (2010) Disaster Resilience Indicators for Benchmarking Baseline Conditions, *Journal of Homeland Security and Emergency Management*, 7, 51.
9. Dalkey, N. (1969) An experimental study of group opinion, *Futures*, 408-426.
10. Forza, C. (2002) Survey research in operations management: a process-based perspective, *International Journal of Operations & Production Management*, 22, 2, 152-194.
11. Gilpin, D.R. and Murphy, P.J. (2008) *Crisis Management in a Complex World,* Oxford University Press, Oxford.
12. Hernantes, J., Labaka, L., Laugé, A. and Sarriegi, J.M. (2012a) Group Model Building: A collaborative modelling methodology applied to Critical Infrastructure Protection, *International Journal of Organizational Design and Engineering*, 2, 1, 41-60.
13. Hernantes, J., Labaka, L., Laugé, A. and Sarriegi, J.M. (2012b) Three complementary approaches for crisis management, *International Journal of Emergency Management*, 8, 3, 245-263.
14. Hollnagel, E., Woods, D.D. and Leveson, N. (2006) *Resilience Engineering: Concepts and Precepts,* Ashgate.
15. Johnsen, S.O. (2010) Resilience in risk analysis and risk assessment, *Critical Infrastructure Protection*, Springer, Berlin.
16. Kahan, J.H., Allen, A.C. and George, J.K. (2009) An Operational Framework for Resilience, *Journal of Homeland Security and Emergency Management*, 6, 1.
17. Labaka, L. (2013) *Resilience Framework for Critical Infrastructures*, University of Navarra, San Sebastian.
18. Labaka, L., Hernantes, J., Laugé, A. and Sarriegi, J.M. (2013) Enhancing Resilience: Implementing Resilience Building Policies against Major Industrial Accidents, *International Journal of Critical Infrastructures*, 9, 1/2, 130-147.
19. Lekka, C. (2011) *High reliability organizations: A review of the literature*, Health and Safety Executive, United Kingdom.
20. Lekka, C. and Sugden, C. (2011) The successes and challenges of implementing high reliability principles: A case study of a UK oil refinery, *Process Safety and Environmental Protection*, 89, 6, 443-451.
21. Leveson, N., Dulac, N., Marais, K. and Carroll, J. (2009) Moving beyond normal accidents and high reliability organizations: a systems approach to safety in complex systems, *Organization Studies*, 30, 2-3, 227-249.
22. Linstone, H.A. and Turoff, M. (1975) *The Delphi Method: Techniques and Applications,* Addison-Wesley Pub. Co., Boston, M.A., USA.
23. Longstaff, P.H. (2005) *Security, Resilience, and Communication in Unpredictable Environments Such as Terrorism, Natural Disasters, and Complex Technology,* Harvard University, Cambridge MA.
24. Lum, T. and Margesson, R. (2013) *Typhoon Haiyan (Yolanda): US and International Response to Philippines Disaster*, Congressional Research Service.

25. Marsden, P.V. and Wright, J.D. (2010) *Handbook of survey research,* Emerald Group Publishing, United Kingdom.
26. McEntire, D.A. (2005) Why vulnerability matters: Exploring the merit of an inclusive disaster reduction concept*, Disaster Prevention and Management*, 14, 2, 206-222.
27. Mileti, D. (1999) *Disasters by Design: A Reassessment of Natural Hazards in the United States,* Joseph Henry Press, Washington, DC.
28. Moteff, J.D. (2012) *Critical Infrastructure Resilience: The Evolution of Policy and Programs and Issues for Congress*, Congressional Research Service, US.
29. MCEER (2008) *Engineering Resilience Solutions*, University of Buffalo, USA.
30. Okoli, C. and Pawlowski, S.D. (2004) The Delphi method as a research tool: an example, design considerations and applications*, Information and Management*, 42, 15-29.
31. Parsons, D. (2007) *National Organisational Resilience Framework Workshop: The Outcomes*, Mt Macedon Victoria, Australia.
32. Perrow, C. (1984) *Normal Accidents: Living with High Risk Technologies,* Princeton University Press, New Jersey, USA.
33. Resilient Organisations, , Resilience Indicators. . Available: http://www.resorgs.org.nz/Content/what-is-organisational-resilience.html.
34. Richardson, G.P. and Andersen, D.F. (1995) Teamwork in group model building*, System Dynamics Review*, 11, 2, 113-137.
35. Rinaldi, S.M. (2004) Modeling and simulating critical infrastructures and their interdependencies*, Proceedings of 37th Hawaii international conference on system sciences*, Washington DC, USA.
36. Roberts, K.H. (1990) Some Characteristics of one type of High Reliability Organization*, Organization Science*, 1, 2, 160-176.
37. Roberts, K.H. and Rousseau, D.M. (1989) Research in nearly failure-free, high-reliability organizations: having the bubble*, Engineering Management, IEEE Transactions on*, 36, 2, 132-139.
38. Ruffner, J.W., Brodie, A.C., Holiday, C.L. and Isenberg, T.H. (2010) Selecting and Utilizing Metrics for an Internet-Based Community of Practice*, Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, Nevada, U.S.
39. Sagan, S.D. (2004) The Problem of Redundancy Problem: Why More Nuclear Security Forces May Produce Less Nuclear Security*, Risk Analysis*, 24, 4, 935-946.
40. Seville, E., Brunsdon, D., Dantas, A., Le Masurier, J., Wilkinson, S. and Vargo, J. (2008) Organisational resilience: Researching the reality of New Zealand organisations*, Journal of business continuity & emergency planning*, 2, 2, 258-266.
41. Shaw, R.S., Chen, C.C., Harris, A.L. and Huang, H.J. (2009) The impact of information richness on information security awareness training effectiveness*, Computers & Education*, 52, 1, 92.
42. Snyder, W.M. and de Souza Briggs, X. (2003) *Communities of Practice: A New Tool for Government Managers*, IBM Center for The Business of Government, Virginia, U.S.
43. The United Nations Office for Disaster Risk Reduction, (November 2013) , Supertyphoon Haiyan "A turning point" for disaster risk management. . Available: http://www.unisdr.org/files/35452_2013no30haiyanformatted.pdf.
44. UN/ISDR (2004) *Living with risk: a global review of disaster reduction initiatives*, New York and Geneva.
45. Waller, M.J. and Roberts, K.H. (2003) High reliability and organizational behavior: finally the twain must meet*, Journal of Organizational Behavior*, 24, 7, 813-814.
46. Weick, K.E. and Sutcliffe, K.M. (2007) *Managing the Unexpected: resilient performance in an age of uncertainty,* Calif.: Jossey-Bass, San Francisco.
47. Wenger, E., McDermott, R.A. and Snyder, W.M. (2002) *Cultivating communities of practice: A guide to managing knowledge,* Harvard Business School Press, Boston, Massachusetts.
48. Yin, R.K. (1994) *Case Study Research: Design and Methods,* Sage publications, Thousand Oaks, CA.
49. Zobel, C.W. (2010) Representing perceived tradeoffs in defining disaster resilience*, Decision Support Systems*, 50, 2, 394-403.