Technological Forecasting & Social Change 103 (2016) 21–33

Contents lists available at ScienceDirect

Technological Forecasting & Social Change

A holistic framework for building critical infrastructure resilience

Leire Labaka *, Josune Hernantes, Jose M. Sarriegi

TECNUN, University of Navarra, Paseo Manuel Lardizabal, 13, 20018 San Sebastian, Spain

ARTICLE INFO

Article history:
Received 1 April 2015
Received in revised form 26 August 2015
Accepted 3 November 2015
Available online 28 November 2015

Keywords:
Crisis management
Critical Infrastructures
Resilience
Resilience policies
Delphi process
Case studies

ABSTRACT

The welfare of society is more and more dependent on the proper functioning of Critical Infrastructures (CIs), and crises that affect CIs usually aggravate their impact on society. Therefore, improving the resilience of CIs is the most important objective of today's crisis managers. Although several resilience frameworks can be found in the literature, their implementation is still incipient and detailed prescriptions for their implementation are lacking. Moreover, some frameworks are only limited to describing the activities performed within the boundaries of the CI, neglecting the role of external agents. This research describes a practical and holistic resilience framework for improving the resilience of CIs taking into account the external agents. The framework is composed of three elements: a set of resilience policies; an influence table that assesses the influence of policies on prevention, absorption and recovery stages; and an implementation methodology that defines the temporal order in which the policies should be implemented. Two empirical studies were undertaken in two CIs to implement this framework. The studies show that the resilience framework helps CIs to diagnose their resilience level, detect areas of potential improvement and complement their risk management approach with a transversal approach to be better prepare to deal with crises.

1. Introduction

Crises derived from similar triggering events occur continuously, but despite the efforts of governments and organizations to develop lessons learned reports and suggest best practices, our ability to effectively implement these lessons learned and best practices seems limited. Although crisis management for future events is improved based on learning from previous incidents, the particular characteristics of every crisis cannot be foreseen. How can crisis managers enhance their preparedness for unexpected events? Crises such as the earthquake in Japan and the subsequent Fukushima nuclear accident (Broad, 2011; Dempsey and LaFraniere, 2011), several power cuts in Western Europe (Andersson et al., 2005; Union for the Coordination of Transmission of Electricity (UCTE), 2004; US–Canada power system outage task force. 2004; Larsson and Danell, 2006), and the eruption of Iceland's Eyjafjallajökull volcano and the resulting air traffic crisis (Hall, 2010; Barr, 2010) have warned us that it is still not possible to anticipate how a crisis may evolve and what protective measures should be established in order to avoid its occurrence. Can we forecast what could occur in the future? Are the characteristics of today's world the same as in the past? Is the current crisis management approach adequate for dealing with today's world crises?

Crisis can be defined as a consequence of an unexpected triggering event that suddenly or by an accumulative process of near misses strikes the entire system (Mitroff and Anagnos, 2000; Pearson and Clair, 1998; Coleman, 2004). Preventing and preparing for something which is unexpected is almost impossible since nobody knows when or how a crisis will occur or what would be affected by the crisis.

To date, crisis managers have been focused on developing specific preparation and response procedures for already identified risks, but they lack sufficient preparation for unexpected situations (Boin et al., 2003; Boin, 2004; Lagadec, 2007). Risk analysis is built on the premise that hazards are identifiable (Risk and Resilience Research Group and Center for Security Studies, 2011; Park et al., 2013). However, nowadays, as it has been shown in the previous crises examples, it is almost impossible to forecast when a crisis would occur and how it would evolve. Furthermore, as today's world is more complex and interconnected than ever before, interactions among Critical Infrastructures (CIs) are more unfamiliar and complex than before, and this makes it difficult to anticipate how an incident that occurs in a CI may affect the rest of the CI network (Gilpin and Murphy, 2008; Turner, 1976; Perrow, 1984). CIs are essential systems for the safety and economic and social welfare of modern society (Min et al., 2007; Oliva et al., 2010; Katina et al., 2014), and therefore crises compound their effects if they affect one or more CIs (Min et al., 2007; Oliva et al., 2010; Laugé et al., 2014; Chang et al., 2007). It is therefore really important that crisis management focuses on improving the safety and reliability levels of CIs (Hämmerli and Renda, 2010).

Several national approaches have been established worldwide such as European Programme for Critical Infrastructure Protection (EPCIP) in Europe (CEU, 2008), National Infrastructure Protection Plan (NIPP) in the US (NIPP. National Infraestructure Protection Plan, 2009), and Critical Infrastructure Resilience Strategy in Australia (Australian

* Corresponding author.
E-mail addresses: llabaka@tecnun.es (L. Labaka), jhernantes@tecnun.es (J. Hernantes), jmsarriegi@tecnun.es (J.M. Sarriegi).

http://dx.doi.org/10.1016/j.techfore.2015.11.005
0040-1625/

Government, 2010). Furthermore, several studies have attempted to analyze the CIs interdependences. Diverse modeling techniques and simulation approaches such as empirical, agent based, system dynamics and, network based approach among others have been used to analyze the CIs interdependences (Ouyang, 2014; Yusta et al., 2011). These modeling approaches have their own particular advantages and disadvantages but all of them have several challenges that they need to overcome. All of them need data to feed into the models but the access to this data is limited and often the accuracy is not sufficient. Most of the approaches limit to model the interdependence between two or a proportion of CIs without taking into account the interdependences among all of them (Ouyang, 2014). The validation is mostly based on feedback from experts and historical data, which might not reflect the reality in the future. In light of these challenges, Ouyang and Yusta et al. (Ouyang, 2014; Yusta et al., 2011) propose to enhance the collaboration and information sharing and to joint effort from the government agencies, research communities and the utility companies to provide the required data and to face the current challenges.

Given the unforeseen nature of crises and the complex structure of CI networks, mitigation efforts established beforehand may often be inadequate or not even desirable when dealing with crises and their cascading effects (Gilpin and Murphy, 2008; Wardekker et al., 2010). Assessing the magnitude of the hazard may be unknowable and forecasting the joint probability of the occurrence of two or more major events simultaneously may be even harder (Park et al., 2013). Therefore, improving cooperation between the CI and external stakeholders and developing a crisis awareness culture within the organizations have become the most promising alternatives for crisis managers (Van de Walle and Turoff, 2008). To be able to face crisis situations, it is essential that their occurrence be prevented and specific response plans be developed; it is equally crucial that an adaptive behavior plan also be adopted (Gilpin and Murphy, 2008; Wardekker et al., 2010; Weick and Sutcliffe, 2007; Elwood, 2009; Boin and McConnell, 2007). Lindblom (1959) outlined this approach in a 1959 paper. He explained that decisions cannot always be made using a "scientific" process where complete knowledge of all relevant variables is known nor can the optimized solution be obtained. As Turoff et al. (2009) point out, when unexpected events occur and there is not enough information or a previously established plan is not adequate for handling the situation, decisions made by crisis managers are subjective and involve a limited number of alternatives that rely on expert knowledge and past experience.

In this context, resilience has become an essential concept in the field of crisis management and critical infrastructure protection (Hämmerli and Renda, 2010; Boin and McConnell, 2007; De Bruijne, 2006; De Bruijne and Van Eeten, 2007). Resilience goes beyond traditional risk management methods by not only defining policies for facing expected events but also by taking into account unexpected events (Risk and Resilience Research Group and Center for Security Studies, 2011). Both approaches, risk management and resilience, must be combined to adequately cope with crises (Park et al., 2013). Although there are several definitions in the literature regarding the concept of resilience (Manyena, 2006; Moteff, 2012), our research defines resilience as the ability of a system to prevent the occurrence of a crisis and the capacity to absorb the impact and recover to the normal state rapidly and efficiently when a crisis does occur.

In operationalizing resilience, this paper presents a holistic resilience framework for CIs that supports crisis managers in diagnosing and improving a CI's resilience level. Although there are several studies regarding the analysis of CI interdependences (Ouyang, 2014; Yusta et al., 2011; Eusgeld et al., 2011), only a few address the relationships that exist between a single CI and external response stakeholders such as first responders, government and society (Yusta et al., 2011). Therefore, this framework focuses on a single CI, including the external stakeholders potentially involved in a crisis at this particular CI. This research does not analyze the interdependences that exist among different CIs. The framework is composed of three main elements: a set of resilience policies, an influence table where the influence of each resilience policy on the three resilience lifecycle stages (prevention, absorption and recovery) is assessed, and an implementation methodology which identifies the temporal order in which the resilience policies should be implemented to achieve the highest effectiveness in the implementation process. Moreover, two case studies were carried out in order to implement this framework in practice. We conclude by drawing some conclusions about the experiences of applying the framework.

2. Resilience dimensions, characteristics and principles

The literature contains several definitions of resilience as well as several dimensions, characteristics and principles that define this concept. Some authors break resilience down into four dimensions (Bruneau et al., 2003; Multidisciplinary Center for Earthquake Engineering Research (MCEER), 2008; Zobel, 2010; Gibson and Tarrant, 2010):

- Technical resilience: this refers to the ability of the organization's physical system to perform properly when subject to a crisis.
- Organizational resilience: this refers to the capacity of crisis managers to make decisions and take actions that lead to a crisis being avoided or to at least reducing its impact.
- Economic resilience: this refers to the ability of the entity to face the extra costs that arise from a crisis.
- Social resilience: this refers to the ability of society to lessen the impact of a crisis by helping first responders or acting as volunteers.

Alternatively, some authors set the following characteristics as the main features of resilience (Bruneau et al., 2003; Multidisciplinary Center for Earthquake Engineering Research (MCEER), 2008; Zobel, 2010): robustness, redundancy, resourcefulness, and rapidity. Brunsdon and Dalziell (2005) propose that resilience can be broken down into two components: vulnerability and adaptive capacity. Vulnerability refers to the ease with which an organization is pushed into a new state and adaptive capacity is the ability to cope with that change. In turn, McEntire (2001) defines vulnerability as "the degree of risk, susceptibility, resistance and resilience level of the system". Vulnerability is dependent not only on the magnitude of the hazard and exposure of the system to an event, but also on the capacity of the system to resist and absorb the impact (McEntire, 2001; Francis and Bekera, 2014).

The literature also presents several resilience frameworks and principles for improving the resilience level of CIs. 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 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 organizations' resilience level. This framework is composed of thirteen indicators grouped under three attributes: leadership and culture, networks, and change ready (Resilient Organisations. Resilience Indicators. 2012). In the same vein, Parsons describes eight key attributes of organizations that are 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).

Johnsen (2010) takes a step forward and describes seven principles based on the organizational and technical aspects that organizations need to fulfill to be resilient. Francis and Bekera (2014) propose a resilience assessment framework based on the three resilience capacities: absorptive capacity, adaptive capacity and restorative capacity. A four step process (system identification, vulnerability analysis, resilience