Resilience of Critical Infrastructures: benefits and challenges from emerging practices and programmes at local level

Paolo Trucco and Boris Petrenj

School of Management, Politecnico di Milano, Piazza Leonardo da Vinci 32, 20133 Milan, Italy

Abstract

Since the beginning of 2010 there has been a boom of Public-Private Partnerships (PPPs) with a goal of Critical Infrastructure Protection and Resilience (CIP-R) and Emergency Management (EM) in North America and partly in Europe and Australia as well. Currently having PPPs as one of the main ways to cope with CI interdependencies through engaging all stakeholders in order to build 'full-spectrum' resilience, it is important to look up to the best practices. Previous research has set the theoretical base of PPPs and claimed their high potential for enhancing CIP-R that is vastly unexploited due to challenges in their establishment and management. It is now necessary to move forward to studying partnerships' practical side – common issues they face, ways to overcome them and concrete benefits they are able to bring. Through studying seven cases, this work compares different PPP approaches and their contribution to CIP-R. The study demonstrates how challenges are faced and solved in an innovative way and how the benefits are reached. It also shows approaches and joint activities that support information sharing and trust building as the main ingredients that hold partners together and enable progress in other aspects, from which both public and private parties may benefit. Starting from the findings and a subsequent analysis within and between the seven cases, the study proposes a framework for the development of regional CIP-R. programmes in the context of a PPP.

Keywords: Critical Infrastructures, Public-Private Partnership, Resilience, Protection, Case study

1. Introduction

An infrastructure is a set of basic facilities, services, and installations that are necessary for the functioning of a community (American Heritage Dictionary of the English Language, 1996) or society, such as electricity, gas and oil production, transport and distribution; communication and transportation systems; water supply; public health; financial and security services, etc. Contemporary societies are increasingly dependent on availability, reliability, correctness, safety and security of many technological infrastructures, commonly referred to as Critical Infrastructure (EC, 2005). A Critical Infrastructure (CI) is an array of assets and systems that, if disrupted, would threaten national security, economy, public health and safety, and way of life (McNally et al., 2007, Hilton, 2006). Concurrently, the importance of infrastructures has skyrocketed as modern societies increasingly rely on their functioning (Ouyang, 2014).

Despite all protection measures, including physical protection of the facilities, surveillance, cyber protection of information and control (SCADA) systems, screening people entering the site, etc., it is impossible to reach risk '0' level. Since the preventive effort itself is not sufficient (cannot be completely reliable or otherwise costs would be unsustainable), more effort is put in enhancing resilience, in order to cope with inevitable events. Counting both high prices of highly reliable preventive efforts and private sector reluctance to invest more in preventing very-low-probability events, despite their expected high-impact, the advantages of resilience-based approaches are reduction of expenses of protection amelioration for certain risk scenarios (which may or may not occur) and improvement of response and recovery activities that cover all hazards (Pursiainen, 2009; Bruijne & Van Eeven, 2007).

CI resilience is emerging as one of the utmost critical issues of this decade. Resilience generally means the ability to recover from shock, insult, or disturbance, and the quality or state of being flexible, and it is used quite differently in different fields (Bouchon, 2006). In the disaster management domain, it is generally defined as "*the capacity of a system, community or society potentially exposed to hazards to adapt, by resisting or changing in order to reach and maintain an acceptable level of functioning and structure. This is determined by the degree to which the social system is capable of organizing itself to increase this capacity for learning from past disasters for better future protection* and *to improve risk reduction measures*" (UN, 2005; p. 9). **Technical resilience** consists of improving the level of resilience of infrastructures (e.g. adding redundancy, geographical isolation, backups, etc.). In its further development, resilience moved towards the

'*full spectrum resilience*' (Boone, 2012) by adopting broader approach including **organizational resilience** (covering strategic, operational, and tactical levels of intra- and inter-organisational coordination and collaboration, addressed across a range of potential impacts) and **societal resilience** (including e.g. preparation of the authority, population and economical world - emergency plans, business continuity plans, evacuation plans, alternative resources).

The US Department of Homeland Security (DHS) in its National Infrastructure Protection Plan (NIPP) defined resilience as "*the ability to resist, absorb, recover from, or successfully adapt to adversity or a change in conditions*". More specifically, **infrastructure resilience** is "*the ability to reduce the magnitude and/or duration of disruptive events. The effectiveness of a resilient infrastructure or enterprise depends upon its ability to anticipate, absorb, adapt to, and/or rapidly recover from a potentially disruptive event*" (NIAC, 2009; p. 8). The NIPP (DHS, 2013) aims to unify Critical Infrastructure and Key Resource (CIKR) protection efforts across the US. It outlines how government and private sector participants in the critical infrastructure community work together to manage risks and achieve security and resilience outcomes. It has evolved from concepts introduced in the initial (DHS, 2006) and revised version (DHS, 2009) until the latest version (DHS, 2013) that focused on partnering for CIP-R. NIPP is supported through supplements in form of tools and resources that can be used for the implementation of specific aspects (such as sector-specific plans, training courses). The Federal Emergency Management Agency (FEMA) made significant efforts to increase the level of private sector collaboration at all levels. FEMA offers a variety of tools to help organizations interested in starting PPPs, such as courses, stories and models of successful partnerships, funding, etc.
The concept of resilience as European strategy had not been mentioned at all either in the 'Green Paper on a European Programme for Critical Infrastructure Protection' (EC, 2005), the Directive Proposal (EC, 2006) or the final Council Directive (EC, 2008; Pursiainen, 2009). The Stockholm Programme (EC, 2009) invited the Council, the Commission, the European Parliament, and the Member States to draw up and implement policies to improve measures for the protection, security preparedness and resilience of critical infrastructure. It also called for Directive 2008/114/EC (EC, 2008) to be analysed and reviewed in order to consider including additional policy sectors. Ultimately, the review of the EPCIP Programme (EC, 2012) called for improved resilience of Critical Infrastructures as a part of comprehensive EU Internal Security Strategy. Most of the EU nations have addressed the issue by developing national CIP-R plans and initiating actions.

On the other side, since interconnected infrastructures largely have a regional scope, their interdependencies and service restoration need to be addressed regionally as well. Local level is where the CIP-R issues are first tackled. Depending on the organization of a country, its population and infrastructure density, 'local' ranges from a big city metropolitan/urban area, parish, region, a few regions acting as one when dealing with CIP-R, all the way to a (small) country. As FEMA Administrator Craig Fugate explained "*We have realized that a federal-centric approach will not yield success and that instead we must collaborate and engage with partners at every level of government as well as the non-profit and private sector.*" (FEMA, 2011; p.2) CI systems are not limited or designed to fit geographical borders. CIP-R resilience is largely cross-border issue in many areas worldwide. Considering diverse and complex aspects and challenges of protection and resilience of CIs including distributed networks, varied organisational structures and operating models, interdependent functions and systems, multi-level authorities, partners, responsibilities, and regulations [5], it is clear that it would not be efficient to tackle CIP-R only from national or regional level. Protecting CIs is a shared responsibility requiring cooperation among all levels of government (national, regional, local) and the involvement of the private sector (DHS, 2009).
In the face of many CI breakdowns current CIP-R approaches have often proved inadequate and with major limitations (Kröger, 2008; Boin & McConnell, 2007). Recent years have brought major governmental initiatives and rapidly increasing number and spectrum of activities all over the world addressing the issues regarding CIP-R. There are pervasive efforts to improve protection and resilience of CIs and ensure their operational continuity in wake of broadened range of hazards and treats. Effective CIP-R depends on numerous stakeholders collaborating at different institutional and operational levels and exchanging information by means of a variety of channels. In this regard, regional initiatives have emerged worldwide as one of the key strategies to deal with CIP-R issues in the context of Emergency Management (EM) and Community Resilience policies. Since the beginning of 2010 there has been a boom of Public-Private Partnerships (PPPs) in North America and partly in Europe and Australia as well, as the main approach for today's practitioners around the world to deal with CIP-R issues. Strong steps are being taken in all the CI sectors to bolster coordination and information sharing across the government-business border, and even more attention should be placed on growing and nurturing PPPs in CIP-R.

PPPs hold great promise to provide resounding value for both government and businesses, but also face significant obstacles that will need to be overcome. Indeed, PPPs come with challenges in their establishment and management so they sometimes fail to perform and bring benefits as expected, a phenomenon that may lead to a fracture between the appearance and the reality of PPPs on CIP-R. This is why the characteristics of the PPP that runs a specific Regional CIP-R Programme have strong influence on the scope, objectives,

activities, and also on the quality of achievements of the programme itself. Recent research has set the theoretical base of Public-Private Partnerships (PPP) and claimed their high potential for enhancing CIP-R that is vastly unexploited due to challenges in their establishment and management. We move forward by studying partnerships' practical side. Through exploratory case study analysis, we try to understand the role and contribution of regional programmes in shaping the contents and results of CIP-R efforts. We identify and consider all the relevant aspect when it comes to these partnerships, such as PPP models, common issues they face, ways to overcome them (good practices in use), alignment with higher level programmes, contribution to information sharing, collaboration and efficiency of crisis response, ability to bring benefits and sustain CI system resilience in general. We sum up all the findings into a framework for the development of regional CIP-R programmes.

The rest of the chapter is organised as follows. Section 2 gives the theoretical background on the topic, related aspects and current developments. In Section 3 we explain the aim of the present study and its methodology. The main findings in form of case studies description and their analysis are presented in Section 4. The cases are summarised, emphasising their common and distinct features and specific activities. Section 5 introduces the framework for the development of regional CIP-R programmes and explains its main parts. The final conclusions are drawn in Section 6.

2. Theoretical background

2.1 Governance issues and approaches to support CIP-R

After the process of privatization and market liberalization during 1980's and 1990's, significant amount of infrastructures passed under ownership of private enterprises. At the same time some public services were being outsourced from the state to private companies. Government's interest, and also obligation, is to ensure providing of essential services that are vital for national security and the well-being of population. On the other hand, the focus of private organizations is on running their business (business continuity) and the security issue is not at the top of their priorities, so there is '*a different sense of urgency in concerning the problem*' among two partnering sides (Dunn-Cavelty & Suter, 2009). Private sector doesn't have funds earmarked for this purpose or is just unwilling to invest more in security. There are exceptions, but in many cases costs of improving security measures or vulnerabilities mitigation outweigh the benefit of reduced risk (Auerswald et al., 2005).

On the other side, every infrastructure disruption, with an outcome of temporary reduction or loss of services, causes significant economical loses and damage to prosperity of the nation. Therefore passing the responsibility for security issues to the private sector is an extremely delicate matter for the government (Percy, 2007). For example the role of the US government during the Deepwater Horizon Oil Spill in Gulf of Mexico (national issue) has been perceived unsatisfactory and criticized by BP Commission for failing to assume leadership and effectively coordinate public and private sector (Heineman, 2011). Government oversight, necessarily accompanied with industry's internal revisions, is needed to adequately reduce risks and effectively prepare to respond in emergencies (National Commission on the BP Deepwater Horizon Oil Spill and Offshore Drilling, 2011).

In situation where control commenced to slowly slip away from the state's hands, a new role for the government presented itself as a possible more effective strategy. In 'meta-governance' approach governments serve as coordinators and stimulators of operators networks (Dunn-Cavelty & Suter, 2009). Another method of resiliency development at both strategic and operational level is through the implementation of Public-Private Partnerships (PPPs). PPPs '*serve as the medium through which that infrastructure functions and protects itself*' (Barnes & Newbold, 2005; p. 1). Protecting and ensuring the resilience of critical infrastructure became a shared responsibility among government and the private sector (PCCIP, 1997). In fact, no single organization has all the necessary resources, relevant information and competence to cope with complex inbound and outbound interdependencies under different accident scenarios (Petrenj, Lettieri & Trucco, 2013), or as US Congress stated: "*Disaster preparedness, mitigation, response, and recovery are efforts that particularly lend themselves to public and private partnerships. In order to effectively respond and recover from an event, the two sectors must work together to protect citizens during a disaster, and help communities rebuild after*" (DHS, 2012). Through its grant program in 2012, DHS has provided supplemental resources to support Public-Private collaboration in order to enhance regional disaster resilience and emergency management.

There is a wide range of PPP forms, characterized by their objectives, models, organization, relationships, leadership, contracts, size, type of actors, etc. While original concept of PPP is project-based and aims to add value and increased efficiency to the specific service, compared to other options such as concluding a more traditional contract (EC, 2005), PPPs with a purpose of collaborative efforts for CI protection and resilience

(in scope of this work) are more programme-oriented (i.e., not limited by time periods) and aimed not at enhancing operational efficiency, but at increasing security and vital service continuity (Dunn-Cavelty & Suter, 2009). Main goals of this kind of partnerships should be quite clear and common – protecting property and lives and ensuring continuity of essential services in the face of a turbulent environment where different types of hazards are present. However, in specific incidents primary objectives can become mismatched. Conflicts can appear about selecting priorities, followed by prioritizing actions and resources.

2.2 Hierarchical vs PPP approaches in EM

During the last decades public policy and Emergency Management theorists have increasingly recognised the need for a different approach, rather than traditional hierarchical framework used in normal operating conditions (Comfort, 2007). Hierarchy model works very well under relatively stable and fairly predictable conditions (routine emergencies), with time to plan. On the other hand, when coping with dynamic, complex and largely uncertain events hierarchies tend to break down. Information gets lost due to compression, has to cross many levels which takes too much time and non-functioning link stops information completely (Helbing, Ammoser & Kuhnert, 2006). Obstructed information flow up and down the hierarchy undermines the flexibility, improvisation and urgency expected from crisis responders (Boin, 2005). It is impossible for authorities to control each and every move of first responders, and furthermore, organizational diversity makes it impossible to establish an uppermost hierarchy. Blurred boundaries between public and private sectors also make traditional top-down approach inappropriate.

Ability to handle unanticipated and non-routine events is critical and information processing plays a crucial role for the effectiveness of organizations' response to crisis. As complexity and uncertainty rise, transition to flatter organizational structures is a quick way to increase information processing and keep up to the challenge ahead. Command-and-Control (C2) becomes unreliable and flatter structures become more appropriate. An effective response is flexible and networked, recombining the joint potential of the response network (Boin, 2005). Several tests showed that network teams were overall faster and more accurate in difficult scenarios than hierarchical teams (Boin and McConnell, 2007). Network teams also shared more knowledge in the difficult scenarios, compared with the easier scenarios (Schraagen, Veld & De Koning., 2010). More horizontal and networked organizational structures turned out to be more appropriate to crisis management than classic C2. 'Edge organizations' (Roby & Alberts, 2012) empower the first lines in situations when plans don't work, and authorities should limit themselves to making only critical decisions – decisions only they can make (Boin, 2005). There is no single 'best' approach for each incident, but organizations have to adapt according to the emergency management stage, complexity of the event that they are encountering and environmental characteristics (Lemyre et al., 2011).

Sharing power/authority and even resources is still far from what is the situation in practice and might eventually come up in future as partnerships develop and mature. Even the most of information sharing still occurs through informal channels, relying on acquaintances, personal contacts and connections. Information sharing and coordination of operations is the first step in this direction and basis for establishment higher levels of collaboration, including e.g. pooling of resources, mutual support, and joint decision-making. Beaton et al. (2010) have developed a list of 13 essential collaboration capabilities needed to support actors in their crisis response information sharing (Figure 1).

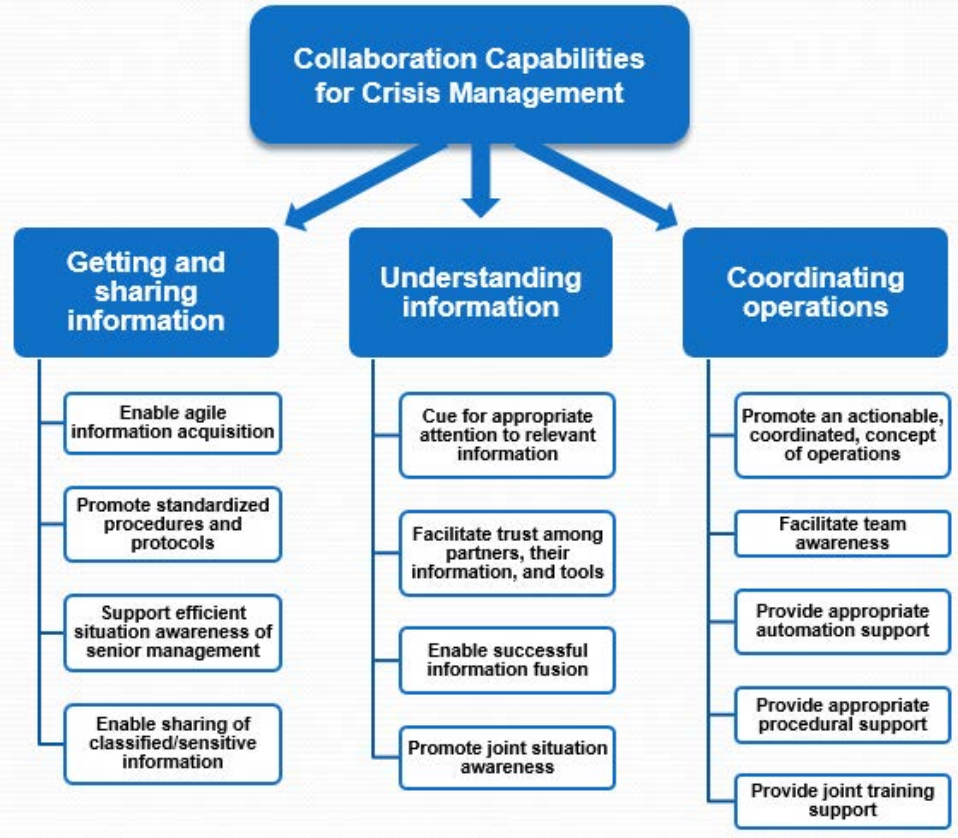

Figure 1: Collaboration capabilities required for crisis management (adapted from [36])

Networks have become prevalent form of multi-organizational governance since they are seen as superior way to deal with malefic problems. Networks consist of legally autonomous organizations that work together to achieve not only their own but collective goals as well. Networks offer enhanced learning and planning, and enough resources and knowledge available to deal with complex problems. However *"some form of governance is necessary to ensure that participants engage in collective and mutually supportive action, that conflict is addressed, and that network resources are acquired and utilized efficiently and effectively"* (Provan and Kenis, 2008, p. 231). Research carried out by Provan and Kenis (2008) presented three ways to govern a network: self-governance, governance by a lead organization and governance by a network administrative organization (NAO). They argue that the successful adoption of a particular form of governance will be based on four key structural and relational contingencies: trust, size (number of participants), goal consensus and the nature of the task (need for network level competencies) – Table 1. Approaches to Inter-Organizational network governance when it comes to CIP-R are defined as (CRN, 2009):

- Meta-governance of identities: Defining Priorities and Strategies
- Hands-on Meta-governance: Network Participation
- Hands-off Meta-governance: Indirect Steering of Networks

Table 1: Key predictors of Effectiveness of Network Governance forms (Provan and Kenis, 2008)

Governance forms	Trust	Number of Participants	Goal consensus	Need for Network-Level Competencies
Shared governance	High density	Few	High	Low
Lead Organization	Low density, highly centralized	Moderate number	Moderately low	Moderate
Network Administrative Organisation (NAO)	Moderate density, NAO monitored by members	Moderate to many	Moderately high	High

Each of the approaches has its advantages and drawbacks. Scholars are aware of the governance form impact to the network functioning and effectiveness as well as on crisis response (Moynihan, 2009), but further analysis should be conducted for a better understanding and assessment of the impact on the information sharing and collaboration forms within CIP-R PPPs.

2.3 The key role of information sharing

Effective Critical Infrastructure Protection and Resilience (CIP-R) is dependable on numerous actors collaborating at different institutional and operational levels and exchanging information by means of a variety of channels. In this regard Public-Private Partnerships (PPPs) have emerged as the most important governance model all around the world to deal with CIP-R issues (Dunn-Cavelty & Suter, 2009). Indeed, PPPs present themselves as a comprehensive way for enhancing proactive risk management through an all-hazard approach, as well as for increasing the effectiveness of responsiveness and recovery by matching complementary skills, expertise and resources from public and private sectors. Arguably, PPPs improve both protection and resilience of interdependent CI systems and enhance all phases of the emergency management cycle and thus are emerging as the new and most promising governance model to develop effective CIP-R strategies (DHS, 2013).

In particular information sharing is nowadays generally recognised as the key element of government and private sector efforts to protect CI (Eckert, 2005). Timely, trusted information sharing and collaboration among stakeholders are crucial within the CIP-R mission (DHS, 2013). NIAC's (2012) extensive analysis concluded that "*information sharing is perhaps the most important factor in the protection and resilience of critical infrastructure*" and that trust is the 'essential glue' to make public-private system work. The US Presidential Policy Directive (PPD-21, 2013) on Critical Infrastructure Security and Resilience aims to enhance coordination, collaboration and information sharing, as well as to encourage and strengthen PPPs.

The European Programme for Critical Infrastructure Protection (EPCIP) sets the overall framework for CIP-R activities in Europe – across all EU States and in all relevant sectors of economic activity.EU is also aiming to strengthen information-sharing on CIP-R between member states by establishing a Critical Infrastructure Warning Information Network (CIWIN), running since mid-January 2013. Information exchange tool should contribute to increasing security in the EU, building trust among relevant stakeholders, standardizing and better integrating national CIP-R programs (EC, 2013).

Partnerships and information sharing are perhaps the most important concepts within the CIP-R mission, according to several authors. However, it remains difficult and complicated to establish trusted relationships and implement information sharing mechanisms effectively (Eckert, 2005; Dunn-Cavelty & Suter, 2009; Natarajan, 2013). From this point of view it is worth investigating PPPs ability to improve information sharing and collaboration and to raise the level of CIP-R. Increased attention should be placed on growing and nurturing CIP-R PPPs and concrete steps are required to bolster these partnerships in order to realize their great promise (Givens & Busch, 2013). Hence it is relevant to examine the characteristics of PPP themselves and assess different factors that could increase benefits of this kind of approach as a whole.

3. Study Methodology

The goal of the CIP-R PPPs is to bring stakeholders together. We can say that the sense of industry–government collaboration (PPPs) activities, in a nutshell is:

- Knowledge and best-practices sharing (information and techniques related to risk management and identification of vulnerabilities/weak-spots, technology to prevent attacks and disruptions, etc.) (Pursiainen, 2009);
- Collaborative risk assessment (vulnerabilities identification, interdependencies mapping and analysis, incident consequence estimation);
- Collaborative crisis/emergency management (collaborative preparation and response to the emergency situations).

We argue that through these collaborative activities, each of which requires building trust and specific type of information shared, resilience and protection of CIs could be enhanced. Here again issues may occur - such as unwillingness to share information, lack of interest for partnering, lack of trust to partners, etc. - so the effort is also directed to overcoming existing barriers.

The overall aim of this study is to conduct a case study analysis to understand the role of different PPP models in shaping the contents and results of regional CIP-R programmes. More specifically, the main purpose is to determine whether well-established PPPs are able to improve crisis response and sustain CI system resilience in general. To this end the paper analyses PPP approach to CIP-R, its strengths, possible weaknesses and contribution to CIP-R at higher levels. It seeks to understand the organization and functioning of PPPs with a goal of CIP-R in different settings, the challenges and issues they are facing for efficient functioning, their contribution to enhanced information sharing and collaboration, as well as to higher level resilience of Critical Infrastructures.

In this study, a *region* is understood as an area that is recognised as such by its stakeholders. A region can be a single or multi-jurisdiction area, portion of a state (or province), or may span national borders. Regions have

established cultural characteristics, and are cemented by common social and economic activities; as such, they are restricted by geographic boundaries and tend to coincide with the service area of the infrastructures that serve them.

With a focus on emerging PPPs at regional level to address CIP-R issues, the questions this study aims to answer are:

- What are the characteristics and the added value of regional Critical Infrastructure Protection and Resilience (CIP-R) strategies and programmes?
- What are successful practices/approaches to support implementation of regional CIP-R programmes?
- What are the expected and perceived benefits of PPP establishment – results achieved? What are the advancements over time, experience and lessons learned?
- How regional CIP-R strategies and programmes are promoted and supported?

Focusing on the main questions, the analysis does not cover merely the basics of partnership but all the aspects that emerged as relevant in practice. We consider each side's (public and private) position, perspective and concerns towards PPP, as well as tools that have been developed in order to satisfy emerging needs and support spectrum of partnership activities.

As the prior research into practical aspects of PPPs with a goal of CIP-R is quite limited, the case method is well suited to the research questions at hand (Benbasat, Goldstein & Mead, 1987; Walsham, 1995). Case research allows a relatively full understanding of the nature and complexity of phenomena and lends itself to exploratory investigations when phenomena are still insufficiently understood (Eisenhardt, 1989; Meredith, 1998; Voss, Tsikriktsis & Frohlich, 2002; Yin, 2003; Seuring, 2008). Case studies are suitable for exploring issues that are too complex for empirical survey or experimental research.

Therefore, we decided to adopt an *exploratory-explenatory multiple-case* study research strategy (Yin, 2003) as the most suitable choice, focusing on local PPPs with a goal of CIP-R as the unit of analysis. This approach is suitable for understanding of CIs as one of the biggest and the most complex socio-technical systems in combination with PPPs that are concurrently coping with issues of different nature. The cases were selected for the analysis due to the fact that they are among the leaders in the field (regarded as best practices among practitioners) and at the same time diverse in characteristics and with different focuses (Table 2). We do not use 'extreme cases' but major and representative ones and in this way we partly deal with the issue of generisability. Seven PPPs have been studied, one in Canada (CRP), one in the US (LA BEOC), one operating across the border and covering both Canadian territories and American states (PNWER), and four in Europe (Lombardy region – Italy; Kennemerland Safety Region – The Netherlands; Scottish Government – UK; Øresund cross-border region – Denmark and Sweden). In this way, the diversity of the cases has been assured by means of location, size and main focus. Each individual case presents a complete study where facts are gathered and conclusions drawn. In the further step, using cross-case analysis and being able to look from a broader perspective, we capture some common and distinctive features and thus generalise beyond the influence of location specific factors (e.g. cultural, political characteristics).

Table 2: Cases general features

	Location	Focus	Size/Level	Cross-Border
Copenhagen	Denmark (Europe)	Emergency management	Trans-national region	Yes
Kennemerland (VRK)	The Netherlands (Europe)	Safety and Emergency Management	Safety Region	No
Lombardy	Italy (Europe)	Emergency Management	Administrative Region	No
Louisiana (LA BEOC)	USA	Business continuity and community resilience	State	No
Montreal	Canada	CI Interdependencies identification, assessment and mitigation	Big city – Metropolitan Area	No
Pacific NorthWest Economic Region (PNWER)	USA/Canada	Disaster resilience and Cross-border Emergency Management	Multi-state Economic Region	Yes
Scottish Gov.	UK (Europe)	Critical National Infrastructure Protection and Resilience	Country with separate jurisdiction	No

In order to better analyse and confirm the validity of the findings, multiple sources of data have been used (data source triangulation – Yin, 2003; Denzin, 1989). Source materials for the analysis of the cases included 1) a set of semi-structured interviews with people engaged in PPPs and some partnering organisations (CEOs, Managers, Private Sector Coordinators, Civil protection representatives, etc.); 2) documents, reports, action plans, websites and other publications; 3) participation in meetings, roundtables, focus groups and tabletop exercises; 4) contributions by involved personnel. An overview by cases is given in Table 3.

Semi-structured interviews, being flexible, allow new questions to be raised during the interviews based on the response of the interviewees. Interviews were typically of 30-60 minutes duration and notes were taken during all of them. Besides being a source of data they helped to refine our research questions and led to further rounds of interviews. The rigour and validity of the findings were further ensured (Eisenhardt, 1989; Yin, 2003) through the follow-up interviews with several respondents; reviewing of the case summaries by the interviewees; discussion of the analysis of the cases and research findings with members of some of the studied PPPs. This has been done in order to collect possible missing details, get more comments, clarifications as well as to remove possible misunderstandings and ambiguities.

Table 3: Data sources used

	Interviews	Documentation, Reports, Action Plans, other pub.	Focus groups	Table-top exercise	Website	Contribution to the case description by involved personnel	On site visits
Copenhagen		X			X		X
Kennemerland		X	X			X	X
Lombardy		X	X	X		X	X
Louisiana	X	X			X		X
Montreal	X	X				X	X
PNWER	X	X		X	X		X
Scottish Gov.		X	X		X	X	X

4. Findings

In this section all the seven case studies are described in full, followed by the summary of their goals and objectives (Table 4) and their main practices (Table 5).

4.1 Copenhagen Capital Region

The Copenhagen case study has a specific focus on the Øresund (or Öresund) Region – a transnational region in northern Europe. The region was created after the construction of the Øresund Link that connects Copenhagen (Denmark) and Malmö (Sweden) comprising of a motorway route and a railway route. It was opened in 2000 and is jointly owned by the Danish and Swedish governments. The link is approximately 16 km long comprises a 4 km immersed tunnel, an artificial island, Peberholm, which is 4 km long, and an 8 km cable-stayed bridge (Figure 2). The Oresund Region consists of Southern Sweden (Skania) and Eastern Denmark (Zealand). The region's two centres, Copenhagen on the Danish side and Malmö-Lund-Trelleborg on the Swedish side, both border Øresund. The Øresund link has created one physically connected region of 3.6 million people with interlinked transport systems for Skåne and Zealand, thus turning Copenhagen and Malmö into a new European metropolis.

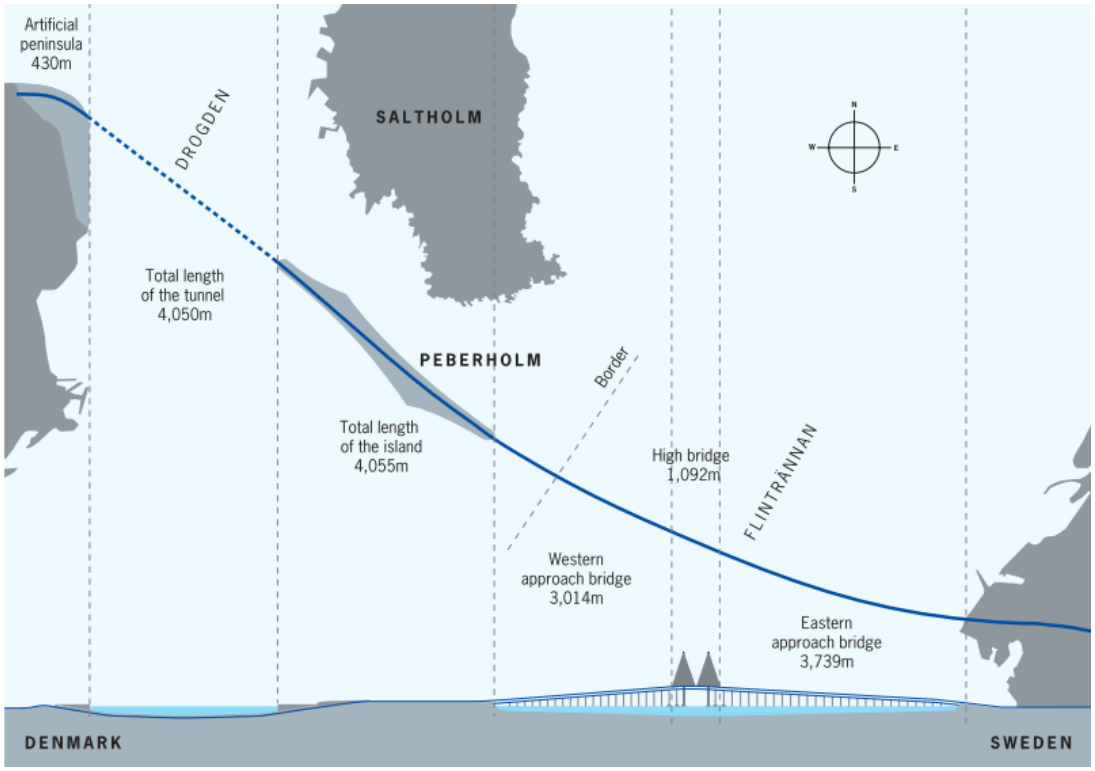

Figure 2: An overview of the Oresund link

The Oresund bridge (7,845m) between Peberholm and Lernacken, which forms the eastern section of the fixed link between Denmark and Sweden, is divided into three main sections: a 3,014m western approach bridge leading from the artificial island to the high bridge, a 1,092m long high bridge and a 3,739m eastern approach bridge between the high bridge and Lernacken on the Swedish coast. The bridge comprises a cable-stayed bridge with a main span of 490m (world's longest cable-stayed bridge for both road and railway), two side spans of 160m each and two approach bridges with 141m spans between the piers.

The Oresund Tunnel is 4,050m long and consists of a 3,510m immersed tunnel under Drogden and two portal buildings of 270m each. Together, these make up the western section of the fixed link between Denmark and Sweden.

Rail traffic is operated by the rail authority, Banedanmark (Rail Net Denmark) and Banverket (the Swedish National Rail Administration), and is monitored by the train stations in Malmo and Copenhagen – Copenhagen Central Station (RFC) and Train Traffic Management in Malmö (DLC).

The Oresund Bridge is owned by the Oresundsbro Konsortiet. Oresundsbro Konsortiet is a client company that was set up on the basis of the agreement of 1991 between the Governments of Denmark and Sweden, jointly owned by the two companies, A/S Oresund and Svensk-Danska Bro-förbindelsen SVEDAB AB. The collaboration between the two companies is laid down in a consortium agreement approved by the two governments. Oresundsbro Konsortiet's primary task is to operate the fixed link across Oresund, including to maintain a high level of accessibility and safety on the link, and to repay the loans raised to construct the Oresund Bridge within a reasonable time frame. Each side is also responsible for the ownership and operations of the land works on their respective sides of the Oresund Bridge. The full organizational structure, as shown in Figure 3 is complex, with the stock of Oresundsbro Konsortiet being equally owned by the Danish holding company A/S Oresund and the Swedish holding company SVEDAB AB, which in turn are controlled by the Danish and Swedish transportation ministries.

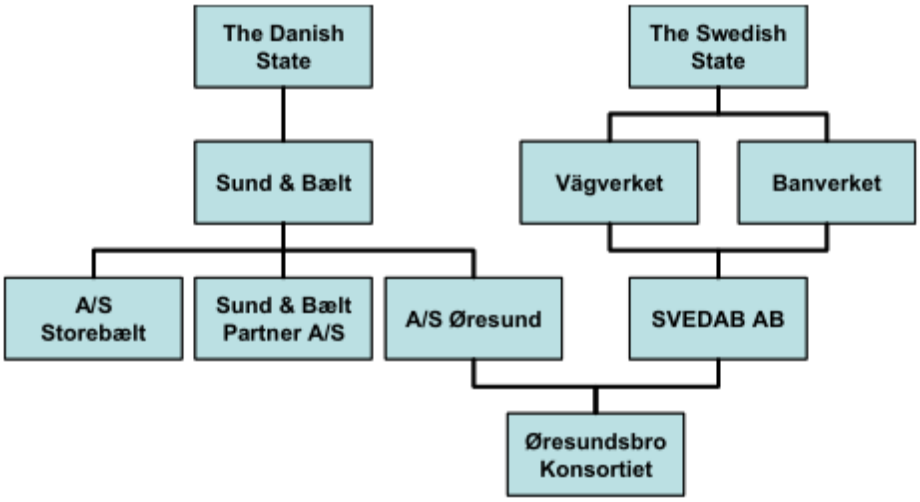

Figure 3: Oresund Bridge organizational structure

"Vägverket" and "Banverket" are the Swedish road and rail authorities, respectively, while "Sund & Bælt" is the Danish authority which oversees the major Danish island linkages. A/S Storebælt acts as a holding company for the Great Belt Fixed Link, much as A/S Oresund does for the Oresund Bridge.

The partnership arrangement (Figure 4) is essentially a public-public partnership between two nations, which assumed full traffic and revenue risk for the project. In order to ensure the safety of the link, the Oresundsbro Konsortiet Company is in partnership with 9 Danish and 6 Swedish agencies, including police, fire, rescue, medical, alarm units and the traffic and rail control agencies. Oresundsbro Konsortiet does not have its own fire brigade or police; it depends on the local authorities for these services. Therefore, it has established a partnership with several agencies from both Swedish and Danish sides to ensure the safety of the link. Involved parties from both Denmark and Sweden include organisations as Police, Fire Brigades, Train and Traffic Control Centres, Hospitals, Alarm Centres, etc. In collaboration with the relevant authorities in Denmark and Sweden, Oresundsbro Konsortiet maintains a comprehensive contingency plan, including an internal crisis response, to handle accidents on the link. The contingency plans are set as a part of the national safety plans of both Denmark and Sweden, and are tested regularly through exercises.

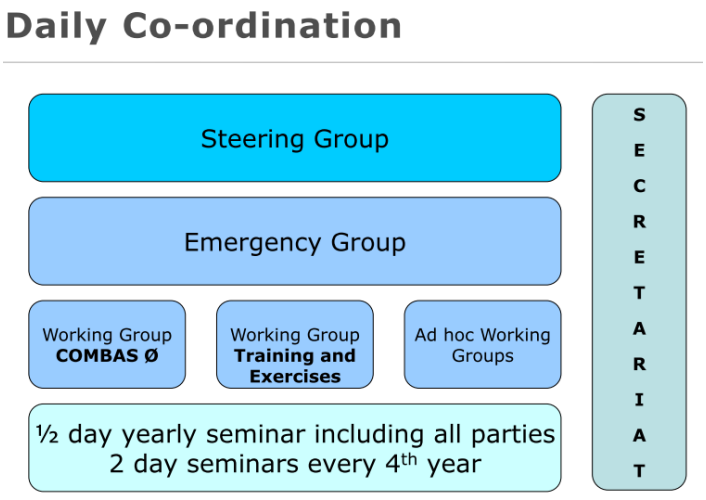

Figure 4: Structure of the partnership

4.1.1 Information Sharing

The main system for sharing information and communication between partners is the Tetra – RAKEL/SINE Gateway System (Figure 5). RAKEL (acronym for radio communications for effective management) is the Swedish national digital communications system (mobile system) used by the emergency services and others in the fields of civil protection, public safety and security, emergency medical services and healthcare. It is used mainly by police, military police, rescue, ambulance services, emergency alarming (RAPS) and local/state

emergency management. RAKEL also helps increase societal preparedness. The system streamlines everyday communications, and enables new ways of working, which increases readiness and with it, ultimately the ability to manage an emergency.

RAKEL is meant to merge all civil protection agencies and organisations into one common forum, increasing information exchanges across organisational and sector boundaries. During the recovery phase of an emergency the system can be used as a tool for monitoring and evaluation, where communications routines and operations can be easily analysed.

Terrestrial Trunked Radio (TETRA) (formerly known as Trans-European Trunked Radio) is a professional mobile radio and two-way transceiver (colloquially known as a walkie-talkie) specification. TETRA was specifically designed for use by government agencies, emergency services, (police forces, fire departments, ambulance) for public safety networks, rail transport staff for train radios, transport services and the military.

TETRA also includes a set of standards developed by the European Telecommunications Standardisation Institute (ETSI) that describes a common mobile radio communications infrastructure throughout Europe.

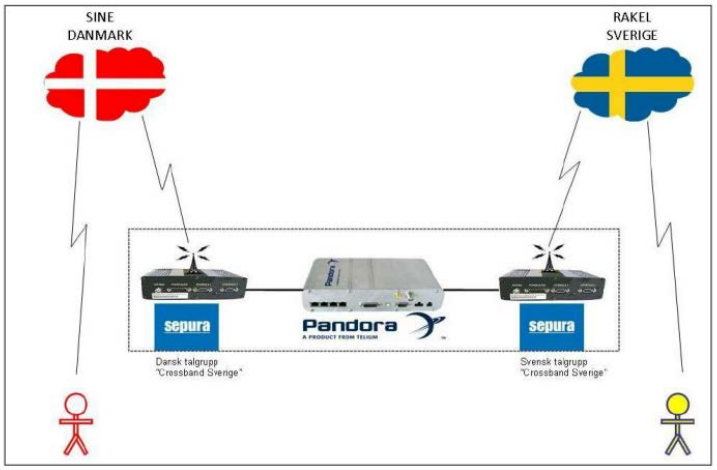

Figure 5: Tetra – RAKEL/SINE Gateway System

4.1.2 COMputer-Based Alarm System Oresundsbron (COMBAS O)

A computer-based alarm system for the Oresund Fixed Link (COMBAS O) has been installed to ensure efficient and rapid alarms to relevant parties and immediately accessible action plans (Figure 6). Information on the location of the accident, type of accident and make of vehicle is entered into the system and immediately passed to the emergency services. Alarms are sent and received, respectively, in Swedish and Danish.

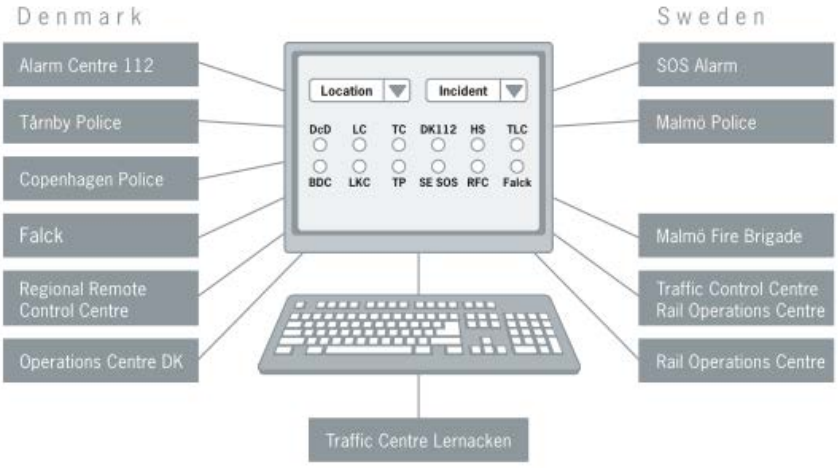

Figure 6: COMBAS O Alarm System

The development of COMBAS O has been crucial for enabling the authorities in the two countries to work efficiently together. Once an operator has keyed in an alarm, COMBAS O will issue a simple order to all

authorities programmed to receive alarms for this type of accident. In order to reduce alarm time and language misunderstandings, the system communicates in both Danish and Swedish. COMBAS O allows all parties to receive the same information and to monitor the rescue work in real time.

4.1.3 Risk Assessment and Emergency Management

Once a year, the Board of Directors presents a report that sets out the company's key risks and specific proposals for handling them. This was done for the first time in 2010 and is updated on an annual basis.

Generally, the emergency response in Denmark has 2 levels: *Municipal (The municipal fire and rescue services) and State (The national fire and rescue services)*. The Danish crisis management organisation is presented in Figure 7.

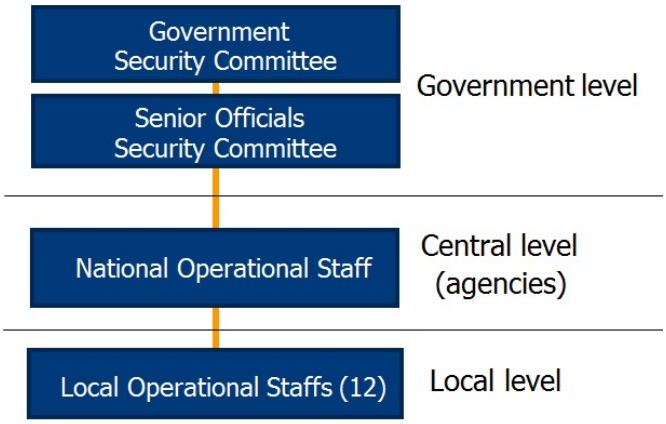

Figure 7: Danish crisis management organisation

Local contingency planning for the Oresund Bridge started three years before the commissioning of the fixed link. The task began with the preparation of a contingency concept which set out existing plans, parties involved in both countries and outlined the framework for a joint contingency plan which could overcome the differences in the two countries (Figure 8). Once the authorities had accepted the concept, detailed planning of the contingency measures could begin.

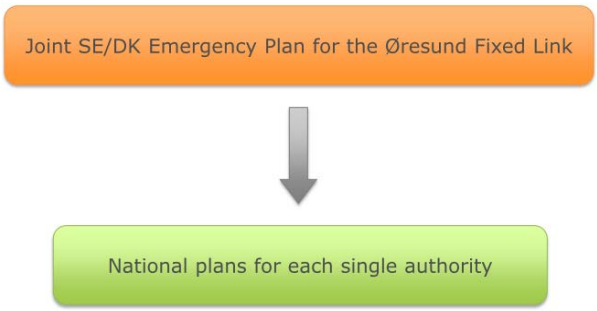

Figure 8: Emergency plans

In collaboration with the relevant authorities in Denmark and Sweden, Oresundsbro Konsortiet maintains a comprehensive contingency plan, including an internal crisis response, to handle accidents on the link. The contingency plans are tested regularly through exercises. The emergency and response plans contain incident level classifications and geographical dimension considerations.

4.1.4 Education

To achieve the contingency objectives, joint training of staff from all relevant authorities and at all levels is required. Oresundsbro Konsortiet has developed an e-learning platform for involved parties (Figure 9), along with trainings and exercises, such as full-scale exercises every 4 year, table-top exercises, small-scale exercises (scenarios) and weekly alerting exercises.

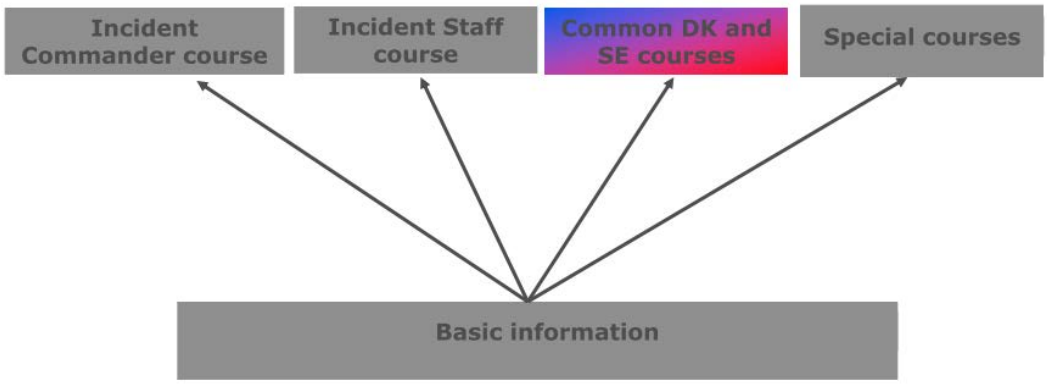

Figure 9: Going towards e-learning

4.2 Kennemerland Safety Region (VRK)

Kennemerland Safery Region (Veiligheidsregio Kennemerland, or shortly VRK) is one of 25 safety regions in The Netherlands. It is situated northwest from Amsterdam, between the city and the North Sea. The region consists of 10 communities with a total population of half a million people (about 3% of the Netherlands' population) and includes Amsterdam's Airport Schiphol (AAS). The geographical area of interest is primarily that within the airport boundary including the city of Amsterdam and nearby municipalities such as Haarlemmermeer. The immediate region is 180 km2 and is host to, and dependent on, a variety of sophisticated and critical infrastructures. The AAS, is a major gateway to and from Europe; it is a key element of the Dutch economy and employment with 64,000 employees on site, plus 290,000 associated jobs nation-wide. The air traffic involves 400,000 flights per annum, carrying more than 50 million passengers and 1.5 million tonnes of cargo, generating 26 billion Euro of the Dutch GNP via 500 companies located at Schiphol. The airport is so important to Dutch society that it has its own crisis planning activity, which sits in relation to its home region's crisis planning activity. It also has its own responders and security services which collaborate with regional responders and security services as required.

In compliance with the 2008 European Directive, the CI sectors in the Netherlands and safety regions have designated the Security Liaison Officers (SLOs), and addressed the obligations regarding Operator Security Plan (OSP) for each potential European Critical Infrastructure (ECI). In addition, the Dutch CIP Contact Point has been set up as a priority, so that the actual implementation of the directive can be channelled through the CIP contact point.

The partnership within VRK is not formed as a single entity or organisation, and in fact operates through a series of PPPs whereby some of the partners are involved for different purposes. Within this complex mix of partners there are 13 public and 6 private organisations of several kinds (medical services, fire services, AAS, National Rail Company, Air Traffic Control and KLM Airlines). Specific plans exist for several Critical Infrastructures in each safety region – the following case of Schiphol Airport CIP-R is only one of the localized partnership, used as illustration. The specific goals and objectives of the partnership are determined by the Statute. In summary, the objectives aim to deliver CIP-R through assurance of conformance with legal instruments, maintenance of the PPP for planning and crisis management, assessment and updating of plans, and conduct of exercises to prove the practical viability and value of such plans.

The public-private partnership between the Safety Region of Kennemerland and Amsterdam Airport Schiphol was formalized in 2007, and builds upon the pre-existing partnerships between AAS and parts of the present Safety Region. Until 2010, the responsibility for responding to crises and disasters were within the local governments. In 2010, according to the law regarding the safety regions, these responsibilities were transferred from the local level to the regional level of government called *Safety Regions*. Therefore, Safety Regions are responsible for CIP-R issues and crisis response at the regional level, while Mayors are responsible for public order and for crisis response at the local (municipality) level. All levels of government work together with critical infrastructure owners/operators to ensure a sufficient level of protection at their respective levels.

4.2.1 History

In 2007 the so-called territorial congruence (territoriale congruentie) took place. The Ministry of Internal Affairs (Binnenlandse Zaken en Koninkrijksrelaties - BZK) which was then responsible for disaster management and fire safety, decided it was more efficient for the police, fire and ambulance services to work together when they covered the same working areas.

Amsterdam Airport Schiphol is in the municipality of Haarlemmermeer, and the regional fire services and disaster management then the responsibility of the fire services of Amsterdam. The police services, however, was the responsibility of Kennemerland, while the medical services were provided by the health organization (GGD) that worked not only for Haarlemmermeer, but also for other municipalities in the area.
Because the regional police of Kennemerland had the same working area as the prosecution district, the BZK decided that it was more efficient if the regional fire services of Kennemerland took over fire control and disaster management. The medical services would then be provided by a new health organization (GHOR) for the whole region of Kennemerland.
The present Safety Region Kennemerland (Veiligheidsregio Kennemerland – VRK) is now formed out of the regional fire service, plus the medical/health service.
The first task of the VRK was to organize the disaster management and crisis response of the municipality of Haarlemmermeer, including Amsterdam Airport Schiphol. VRK also began to organize that for other municipalities in the region, as well as addressing the large/complex risks such as those related to Tata Steel, seaworthy cargo and cruise ships over the North Sea Channel to and from the harbours of Amsterdam, large public events and a critical/vital infrastructure with a number of important roadways and railways including multiple tunnels.
VRK deployed its new Safety Bureau whose primary task is the preparation and support of the multidisciplinary crisis response tasks of the Safety Region. The Safety Bureau provides the planning, facilities support, training, exercise and evaluation of the main crisis response structure of the Safety Region.
To ensure alignment between the stakeholders, liaison and support was seconded to the Safety Bureau.
Another important step was the arrangement of a joint co-located dispatch centre for the police, ambulance and fire services in the region of Kennemerland.
In 2010, new legislation revised arrangements between fire services, medical services and disaster management. The mayors remained responsible, but now as one board. The new legislation is more focussed on modern crisis response instead of classical disaster management.
Within the above background, things changed in the public-private partnership between Amsterdam Airport Schiphol and the public emergency services, but the basis remains.

4.2.2 Public-private partnership – operational levels

The cooperation between Amsterdam Airport Schiphol and the Safety Region Kennemerland is based on activities at specific levels:

- Dispatch centres
- Executive/operational level (regular/daily incident response)
- Crisis response

4.2.3 Dispatch Centres

Amsterdam Airport Schiphol has its own coordination centre where all the business processes of the airport are coordinated, supported and aligned. Its own dispatch centre for the airport fire and the medical service is part of that centre. In case of small incidents this centre can deploy the airport fire and the medical service on its own. The joint dispatch centre of the safety region monitors these deployments. The dispatch systems are connected, as are the alert (P2000) and communication systems (C2000).

4.2.4 Operational Partnerships

In case of escalation or need for support, the joint dispatch centre of the safety region will deploy additional units. For example, the airport medical service can provide first aid but is by legislation not permitted to transport patients to a hospital. An ambulance of the safety region has to take it over. In the case of escalation of a fire or accident, a duty officer of the safety region and additional regional units will be deployed to the scene. The preparation and execution of the fire and medical services at the airport are organized in close cooperation between the private services of the airport and the public services of the safety region. This ensures alignment between planning and procedures, equipment of vehicles, materials, training and exercise.

4.2.5 Crisis response

In case of an incident that disrupts the business processes of the airport, the Operations Manager of Amsterdam Airport Schiphol can take over the coordination of that incident and will assemble a management committee with representatives of the involved business partners. Amsterdam Airport Schiphol has prepared

this in its own incident response plan. An example is a major disruption of the luggage handling system that will lead to delays of incoming and outgoing flights. But in the case of a major/complex fire or accident, the coordination is the responsibility of the safety region. The safety region ensures systematic crisis response through its regional crisis response plan, and a subset of that plan addresses incidents at the Schiphol Airport through formulation of a specific crisis response plan for the Schiphol area. The main scenarios addressed are:

- airplane crash (at or nearby the airport),
- hazardous materials incident at Aircraft Fuel Supply (large storage tanks) or at KLM Engineering & Maintenance (large storage of chemicals),
- incident in the railway underpass (underground platforms with switch lanes).

4.2.6 Steering and administrative groups Schiphol

The administrative management of the specific crisis response plan for the Schiphol area has links with activities such as training and exercises, management of the facilities (crisis response centre with systems) and judgement of evaluations (as a PDCA-circle).
To align this, a steering and a management group are instituted. The *management group* comprises tactical representatives of involved partners, both public and private. The *steering group* comprises strategic representatives under chairmanship of the mayor of Haarlemmermeer.

4.2.7 Most Recent Public Lesson

The main task of the Safety Region Kennemerland is to organize the crisis response in the municipality of Haarlemmermeer and Schiphol airport. A major test was seen in February 2009 when a large passenger plane crashed in farmland just before the landing strip (early touchdown). The cooperation between private services of Amsterdam Airport Schiphol and public services of the Safety Region Kennemerland was very successful, as confirmed by evaluations and investigations.
Points for improvement emphasised after-care of passengers and relatives. Before the municipality could get responders to the site, public care was organized by citizens, supported by motorists of the nearby motorway and farmers of the nearby farms. This form of self-reliance was a signal to all municipalities in the Netherlands to change its public care in case of crisis to facilitate the needs of the public rather than control it.

4.3 Lombardy Region

Lombardy (*Lombardia* in Italian) is one of the 20 Italian regions, located in the north. A sixth of Italy's population lives in Lombardy (around 10 million citizens) and it accounts for around 20% of Italy's GDP, making it the most populous and richest region in the country and one of the richest in Europe. It has a constant population growth, a highly developed infrastructure system and hosted the Expo 2015.

To establish a risk-informed policy making process, the Regional Administration launched in 2007 a four-year research programme named "PRIM -Integrated Regional Program for the mitigation of major risks" (Lombardy Region, 2007). The aim of the programme was the identification of the most critical areas, following an all-hazard approach, the expected impacts on population and economic activities, and the related prevention and mitigation actions. The programme allowed developing a multi-risk assessment methodology that integrates information with different degree of accuracy into a limited set of leading indicators.
The continuous development of high-value services characterizing the Lombardy region society, one of the most industrialized in Europe, deeply relies on complex infrastructure systems. Considering the results of its first study in 2007, it became evident that hazards identified over the territory, not only can threat the citizen life, but can also cause severe disruptions of infrastructure service continuity inducing wide cascading effects. As a consequence, following the release of the EC Directive 114/EC (2008), the Lombardy Region Administration decided to set up a preliminary study to investigate CI vulnerability and to assess current emergency practices in the sector.

It emerged that there is a great potential for an increase in the flow of shared information regarding criticality and accidents which can increase efficiency of the invested resources and also bring an improvement in the security level. The objective of the Lombardy region policy in CIP/R is therefore not to add new mechanisms or control processes, but to **promote and advance collaborative processes**. In light of this logic, from 2010 Lombardy Region has launched a program of activities aimed at defining a model of integrated and shared management, capable of supporting a higher level of collaboration within the processes of prevention, risk monitoring and emergency management related to regional CIs. The program was named "Programma Regionale per la Collaborazione ed il Coordinamento nella Sicurezza delle Infrastrutture Critiche (PReSIC)".

In December 2010 a Memorandum of Understanding was signed by 18 operators of energy and transport CIs operating in the Lombardy region.

The key elements that define the scope of the PPP in Lombardy are (Figure 10):

- evolution of the governance processes, decision-making and operational resilience of regional CIs;
- maintaining a continuous process and shared identification and monitoring of threats, vulnerabilities and consequent risk analysis;
- definition of procedures and protocols for the exchange of information and operational interaction between all the actors involved;
- studying the most appropriate technologies, enabling the operating model of reference and able to guarantee security of access and protection of information.

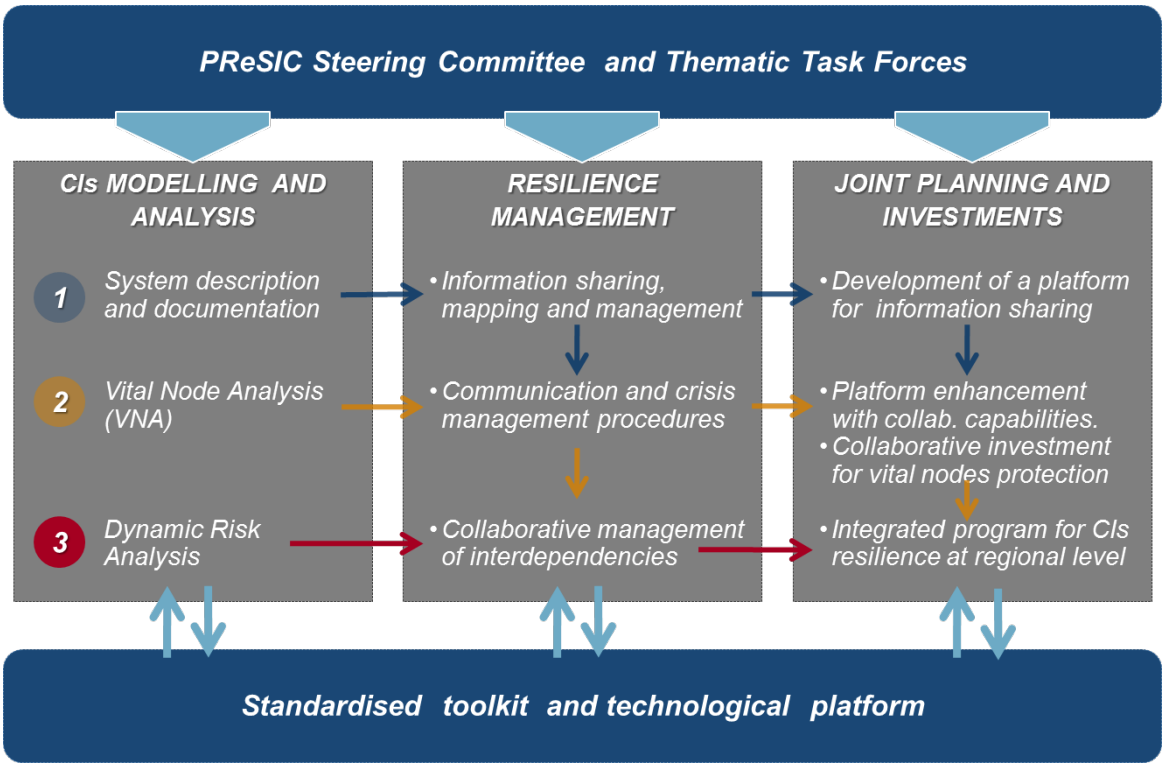

Figure 10: Roadmap for the development and evolution of PReSIC

PReSIC strategy and objectives call for a deep involvement of public and private CI operators. Since this is clearly the most challenging point of the programme, several resources and means of collaboration has been mobilized.

4.3.1 Mapping of emergency management processes and vital node analysis

The preliminary study, carried out by a team of academics and consultants, provided a complete picture of the actual status of the vulnerability of regional infrastructural nodes and the corresponding emergency management processes adopted by the most important CI operators. More specifically the study focused on:

- Carrying out a census of the critical nodes of major regional transport (road, rail, air and underground) and energy (electricity, gas and fuels) infrastructures; globally more than 200 regional nodes have been identified and documented;
- Analysis of the accidents influencing regional CIs and creating a series of historical cases;
- Mapping the organizational models and operational processes of emergency management of the main CI operators active in the region.

The scientific and technical team of PReSIC offered a constant support to operators in preparing and gathering useful information, mainly by means of document analysis, FMECA-like (Failure Mode Effect and Criticality Analysis) questionnaires, direct interviews and process mapping tools.

Thanks to the implementation of a functional model of the regional infrastructural system a systematic vital node analysis has been carried out (Trucco, Cagno, & De Ambroggi, 2012) and returned a ranking list of most critical nodes and clusters of nodes. The functional model is also normally used to support scenario analysis (Cagno, De Ambroggi & Trucco, 2011) and to evaluate resilience strategies (Petrenj & Trucco, 2014) proposed by specific Thematic Task Forces (TTF).

4.3.2 Thematic Task-Forces (TTF)

TTFs represent the backbone of the PReSIC programme implementation; they are established and coordinated by a higher level PPP Governance Committee which is formed by the managing directors from all of the organizations that signed the MoU.

So far three TTF have been established starting from January 2011, one focused on mapping of the information flows and communication channels among actors, another focused on developing collaborative procedures for coping with major meteorological events (e.g. heavy snowfall) and the third one to set up collaborative activities in case of large blackout events.

The primary objective of the first TTF – focused on the mapping of multi actor information flows during disaster management – was to increase the effectiveness and operational efficiency thanks to a greater standardization of communication flows and channels among actors in the regional system (Figure 11). The first analysis and the final documentation of information exchanges has been carried out using a web-based application tool developed for this specific need and constantly accessible by all the actors involved in the PPP. From the work of the roundtables it is evident preference of the operators to increase information exchanges in the future, although not necessarily for collaborative purposes, but primarily for informational purposes. The operators feel the need to increase the volume of communication, or at least improve its effectiveness, to increase a common operational picture. NATO Architecture Framework (NATO, 2007) was used as the standard for presenting operational models of the socio-technical systems. NAF views used in this research include, but are not limited to, the following: High-Level operational concept description (NOV-01) used to describe the 'big picture' through geographical location, operational elements, their connections and interactions; Operational Node Connectivity Description (NOV-02) used for graphical presentation of the nodes that need to exchange information; Operational information requirements (NOV-03) for identification and description of all information exchanges; Organizational relationship chart (NOV-04) to presents the key actors and their relationships; System interface description (NSV-01) to illustrate and describe systems and interfaces that enable exchange of information identified in NOV-03.

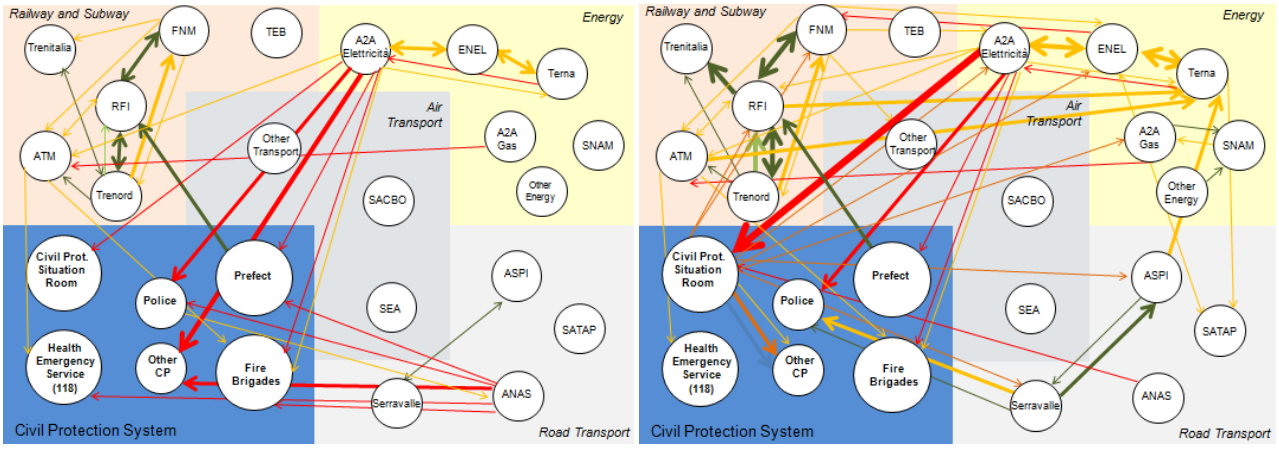

Figure 11: Information flows before (left) and after (right) PPP establishment (Operation context: service interruption of a generic CI)

As for TTFs focused on specific accident scenarios, they adopt the same methodological approach, substantially organised into three steps:

- Development of vulnerability and resilience studies;
- Identification of best practices and innovative solutions for risk mitigation through collaboration between actors, where opportunities for enhancing information sharing are particularly investigated and promoted;
- Design, validation and implementation of collaborative emergency plans.

4.3.3 Towards an integrated platform for information sharing during emergencies

There is an ongoing effort in Italy to support the collaborative plans between CI operators by release of an information sharing application. In this regard, the integration of CI operators and first responders is necessary to improve information sharing and collaborative processes in the planning and management of emergencies. Requirements are defined in the context of infrastructure systems and civil protection of the Lombardy region.

Lombardy Region and Ministry of Research are funding the development of application modules designed to play a key role within an information platform, realized in SOA (Service Oriented Architecture) logic. It aims to improve operational management of emergencies, technologically and functionally support Network Enabled Operations (NEO) and identify coherent strategies in terms of PPPs that would enable new models of governance and investments for CIP/R.

Innovative solutions are being developed at different levels:

- Standardization of information content based on: i) extension / adaptation of standard protocols already existing in the field of Civil Protection, such as Tactical Situation Object (TSO) (Henriques & Rego, 2008); ii) automatic translators to ensure the specificity of glossaries adopted by each operator.
- Development of shared ontology and algorithms for semi-automatic generation of operational information from the data available in the IT systems of each CI operators
- Prediction of vulnerability and domino effects through Pattern Recognition Algorithms, applied to the information exchange process, and discrete event simulation, both powered by real-time operational data;
- Adoption of technological and architectural features that ensure interoperability, easy customization and reconfiguration, access security and resilience to emergency

4.4 Louisiana

Louisiana is a state located in the southern region of the United States, by the Gulf of Mexico, with a surface area of about 135,000 km^2 (1.35% of all US territory) and a population of around 4.65 million (1.45% of total US population). According to the US Department of Commerce, the Gross State Product of Louisiana in 2013 was about 253.6 billion dollars that accounted for around 1.5% of US total GDP. The main cities are Baton Rouge (the capital) and New Orleans –the largest city and a major US port. Louisiana is the only state in the U.S. with political subdivisions (local governments) named 'parishes', which are equivalent to counties.

Louisiana is often affected by tropical cyclones, thunderstorms, and is very vulnerable to strikes by major hurricanes, particularly the lowlands around and in the New Orleans area. New Orleans was catastrophically affected when the Federal levee system failed during Hurricane Katrina in 2005. It was the costliest natural disaster, as well as one of the five deadliest hurricanes, in the history of the US.
Another major event was the Deepwater Horizon Oil Spill in Gulf of Mexico (2010). It was a national issue that is considered the largest accidental marine oil spill in the history of the petroleum industry and the worst environmental disaster America has ever faced.

The Louisiana Business Emergency Operations Center (LA BEOC) is a joint partnership between Louisiana Economic Development (LED), the Governor's Office of Homeland Security and Emergency Preparedness (GOHSEP), the National Incident Management Systems & Advanced Technologies (NIMSAT) Institute at the University of Louisiana at Lafayette and the Stephenson Disaster Management Institute (SDMI) at Louisiana State University. The LA BEOC has been recognized by FEMA as a best practice model for PPPs. It was launched in 2010 to support the coordination of activities and resources of businesses and volunteer organizations in Louisiana and across the nation. The four institutions are equipped with an IT system that enables them communicate between themselves. It is operated as a state-of-the-art facility on the LSU (Louisiana State University) campus, the development of which was supported with in-kind donations of technology and software and cash donation by major national and Louisiana based businesses. LA BEOC doesn't own any resources to give or land to private sector, nor is there a lot of decision making inside LA BEOC - it is getting the information and forwarding to who needs it. There are 30 seats at LA BEOC for representatives of business associations, each of whom have outreach to all of their members.

The mission of the LA BEOC in support of any major disaster is to focus on providing situational awareness and resource support, supporting community recovery, mitigation, and economic stabilization. Its goal is to improve response and self-sufficiency, reduce reliance on FEMA, and maximize business, industry and economic stabilization. It is operated as a state-of-the-art facility on the LSU (Louisiana State University) campus, the development of which was supported with in-kind donations of technology and software and cash donation by major national and Louisiana based businesses. LA BEOC doesn't own any resources to give or

land to private sector, nor is there a lot of decision making inside LA BEOC - it is getting the information and forwarding to who needs it. There are 30 seats at LA BEOC for representatives of business associations, each of whom have outreach to all of their members.

Loss of one or a few critical infrastructure services significantly affects functioning of private businesses causing multiple ripple effects. Establishment of the LABEOC had a goal of mitigating disaster effects and consequences supporting state private businesses continuity. It consists of temporary finding alternative ways of providing essential services until the infrastructure functioning has been recovered. Besides improving business resilience and survivability, it is also important since:

- **Incentivizes new companies to enter the state market** - if the state is willing to help businesses during an emergency and make them safer, it is a good image and motivation for other companies to enter the market.
- **Brings economic benefits in two ways**
  - Through money saving – local goods and services are significantly cheaper than the ones requested from federal level
  - Every local purchase supports the state economy through tax income
- **Citizens are more satisfied** using local products and services that they are accustomed to.

LABEOC model offers an improved crisis communication with state EOC:

- **Private businesses have who to contact and request help** – LA BEOC is handling requests that are not going to be considered if asked directly to state.
- **Communication B2B** – many needs are satisfied locally by making bond between different business, matching ones needs and others resources or services, and thus making benefits for both sides without engagement of the public authorities
- **Serves as filter for information between businesses and state government** – State EOC was getting overwhelmed by phone calls and requests from individual businesses. LA BEOC liaison at the State EOC is able to receive the request and needs that are not fulfilled on local level and address them in an appropriate way.
- Information on the state of infrastructures collected by government office (reliable) is wrapped as 'situational awareness report' and is sent to LA BEOC for use.
- The private sector participants with positions in LA BEOC support the activities of the state EOC – utilize their relationships to source goods and services needed, and capture damage assessment critical to assisting the state in developing accurate situation awareness and economic impact assessments.

During emergencies everything starts local – city or parish. In many cases business need something that cannot be supplied locally. Businesses are registered from all over the state, so in case of an incident in one area businesses from other parts are able to help. The NIMSAT Institute has developed a web portal for the LA BEOC where businesses are asked to register with the state before a disaster and identify any products or services they might provide to assist communities in the state that have been affected by a disaster. Communication with neighbouring states is on a higher level and in charge of the state.

4.4.1 "Big business-small business" Emergency Management Mentorship program

In January 2012, FEMA announced a new campaign "Small Business is Big" and made an effort to help small businesses, often lacking the resources and knowledge, to be better prepared for all-hazards disasters. The need for improvement of businesses resilience is strongly supported by the statistics from the Institute of Business and Home Safety (*25% of all businesses do not reopen after a major disaster*) and the U.S. Chamber of Commerce (*when a business does not have a formal emergency plan in place the figure rises to 43%*) (NIMSAT, 2012).

"Big Business – Small Business" is an innovative effort in the area of PPPs that engages big businesses, willing and able to mentor, with the small ones helping them to strengthen their disaster preparedness and reduce recovery time. Private-private partnership model is voluntary based and promotes proactive (whole-community) emergency management approach. ***Why is this programme important and what are the mutual benefits?*** Big businesses benefit from strengthening their supply chains (where small businesses are often located), raising reputation and positive branding. Small businesses get an opportunity to learn about resilience/business continuity, get missing resources and adopt best practices from experienced leaders who have been through disasters and know what it takes to survive. Considering the social and economic importance of SMEs it creates a great contribution to community resilience. Businesses also build beneficial long-term relationships that round this win-win environment. "Big business-small business" platform has been launched by NIMSAT institute in June 2012.

4.4.2 CI/KR interdependencies and risk analyses

The NIMSAT Institute seeks to advance the understanding of risk faced as a nation due to the interdependencies between various Critical Infrastructure/Key Resources (CI/KR) assets, the dependency of various public and private sector supply chains on these assets, and the consequences of disruptions to the way of life regardless of the cause or location of disruption. The main activities in this direction include:

- **Critical Infrastructure Consequence Analysis** – The NIMSAT Institute, the National Infrastructure Simulation and Analysis Center (NISAC) of the US DHS, Sandia National Labs, and the LA-1 Coalition collaborated on the assessment of the national consequences of disruptions to Louisiana's energy corridor (Port Fourchon / Louisiana Offshore Oil Port / Grand Isle/ Louisiana Highway 1).
- **Infrastructure Surveillance and Risk Assessment** – The NIMSAT Institute is working with the Louisiana Office of Coastal Protection and Restoration (OCPR), in the development of a state-of-the art Intelligent Flood Protection Monitoring, Warning and Response System (IFPRMWRS) at strategic locations within levee systems in the New Orleans region. This system will include the ability to monitor and warn of undesirable performance that could lead to catastrophic consequences.

4.5 Montreal Metropolitan Community

Montreal is the largest city in province of Quebec and the second largest city of Canada with 4 million citizens (11% of total population of Canada) that covers a small portion of the country (about 4250 km^2). According to the Quebec Institute of Statistics, Montreal Metropolitan Community's GDP in 2013 was around 161 billion dollars which accounts for about 9% of the total GDP of Canada.

The Great Ice Storm in 1998 (strongly hit eastern Ontario, southern Quebec and parts of the US) brought into focus the need for all stakeholders to work together, form partnerships and toil spirit of full collaboration. It also raised awareness of the possible consequences of damaged infrastructure in Canada. At this point Federal and Provincial Acts stated that (Lecomte, Pang & Russell, 1998):

- emergency operations are most effective when managed at the lowest level of government
- the response structure should be built upon permanent organizations
- coordinated support from government (federal and provincial) should come from their external partners
- intervention must respect the responsibilities of the participants
- the response and recovery structure must be flexible enough to accommodate all circumstances

In the period after the storm a few of the regional organisations in Quebec decided to give money for the university research on interdependencies. Subsequently, in 2004, a grant from the Natural Sciences and Engineering Research Council of Canada and Public Safety and Emergency Preparedness Canada (now Public Safety Canada) was given to 6 universities/teams across Canada for a Joint Infrastructure Interdependencies Research Program (JIIRP), where Centre risque & performance (CRP) of École Polytechnique de Montréal was assigned to study interdependencies and domino effects.

At the provincial level, in 2008 Quebec launched a government initiative to increase the resilience of its essential systems. Coordinated by the Civil security of Quebec (Organisation de la sécurité civile du Québec - OSCQ), initiative focused primarily on maintaining or restoring the functioning of essential systems to an acceptable level despite any failures that might occur. OSCQ resilience subcommittee's mandate was to mobilize the owner and operators of CIs, whether private or public, to build partnerships, and to ensure the coherence and complementarity of the preventive and preparatory measures envisaged by the stakeholders. CRP of the École Polytechnique de Montréal was asked to give support by consolidating the theory of organisational resilience, establishing a common set of terms and developing a method to evaluate resilience.

4.5.1 Interdependencies and domino-effects study

The ***preventive approach*** (Robert, Morabito & Quenneville, 2007) adopted by the CRP implies the proactive risk management. It emphasizes the anticipation of harmful consequences and establishing a bilateral communication of risk among CIs that interact within a single socioeconomic environment. In order to anticipate the consequences caused by potential failure, and take into account the changing status of the CIs, *coordinative space* must be set up, where it could be possible to share information relevant for planning efficient, effective and realistic protective measures. The preventive approach deliberately focuses on anticipation and effective, targeted communication of the relevant information in order to protect populations

by reducing the domino effects generated by interdependencies. Advantages of the preventive approach include cooperation, communication, anticipation, planning and continuous risk management.

Consideration of the consequences rather than the causes of failures (***consequence-based risk management approach/ All-hazard approach***) leads to the vulnerability assessment of the entities making up an environment. At the same time, it allows ranking of the employment of emergency measures based on the acceptability of the potential consequences. It leads people in charge to better prepare for the risks related to interdependencies among CIs, but calls for initial evaluation of interdependencies in order to estimate a) possible domino effect in case of a disruption, and b) users that have to be informed, so the protective measures could be put in place on time.

As CRP experienced, there were four main barriers for information sharing at the point of interdependency identification and analysis:

- **Confidentiality –** Dissemination of information may represent an additional vulnerability for a network. While security reasons are concern for every organization when it comes to sharing confidential information, competition was problem only in certain sectors. This was not an issue for water and gas operators since they are unique in the region. On the other side, in telecommunication sector situation was significantly different since more enterprises were competing over the market.
- **Interpretation –** Managers of a system are the only ones able to interpret correctly information regarding their system. Receiving a basic level ('raw') information/data makes it prone to misinterpretation by the managers, leads them to analysis that is not good (since they are not experts), to come up with a wrong conclusion and make errors when taking action. (e.g. creating the maps without the key to read them, or without a clear idea how to use them.)
- **Value and property –** Acquisition and management of information is costly. Organizations are not ready to share their information if they do not receive something in return. A lot of the infrastructural systems had been laid underground many years ago and they exact position/location as well as their structural condition (status) is not always precisely known (sometimes even unknown). These data have an intrinsic market value. The acquisition of information requires human and technological resources, and after, there are costs of managing and updating the data on the systems.
- **Update –** The data of an organization are numerous. The update is complex and must be done continuously. Only the organization itself can perform this task efficiently.

How did CRP cope with these issues? Since geographical data are essential dimension in order to properly target and coordinate actions in the field, CRP has developed an innovative flexible cartography approach (Robert and Morabito, 2010) in which, rather than representing infrastructures, represents location sectors in which the consequences of the resource failures are synthesized. Approach with flexible representation allows for a targeted intervention while preserving the confidentiality of information. The size of the sectors used may vary based on needed analysis detail level, geographical zone studied, and the level of confidentiality CI managers wish to maintain. In this specific case, where the methodology has been applied in downtown Montreal, the study zone has been divided into 1 square-km sectors.

Subsequently, a modelling, mapping, decision and planning assistance tool, DOMINO, was developed. It is a prototype of a system for managing interdependencies and analyzing domino effects (Figure 12). DOMINO uses a flexible cartography approach to locate system infrastructures and simulate domino effects, ensuring at the same time data confidentiality (agreements had been signed with partners). The online database is organized in that way that each organization has a password protected access to its own private section of the database where they can manage the information they are sharing, used for domino effects analysis. Module that contains the results of the simulations (analysis of domino effects) is available for all systems including the Civil Security Center of the City of Montréal.

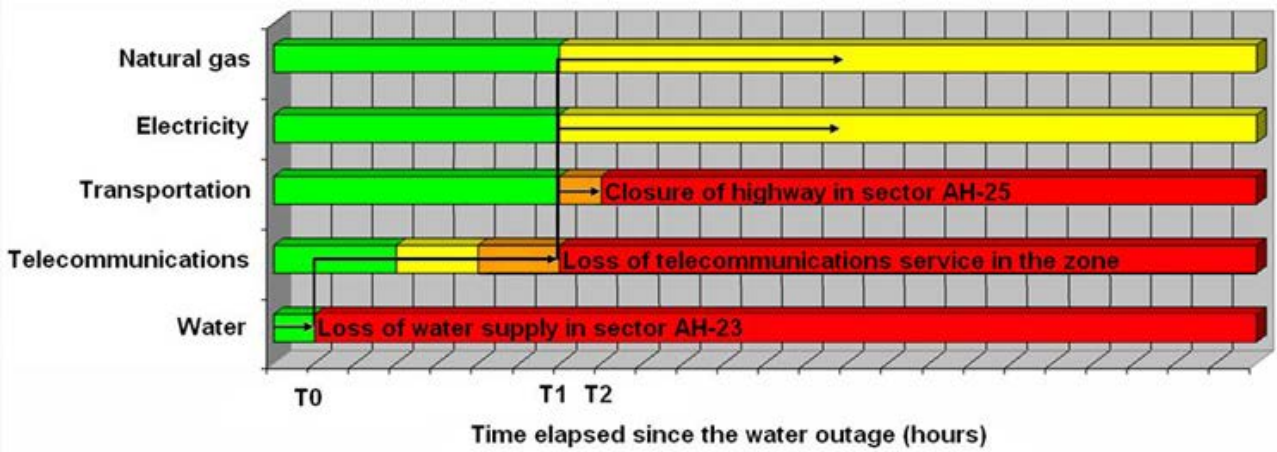

Figure 12: An example of DOMINO simulation (Robert, de Calan, & Morabito, 2008)

In cases of high sensitivity, confidential geographical information needed for identifying anticipated impacts of geographic interdependencies in some sectors is exchanged in the interaction only between system owners, without unnecessary sharing it with other members. Once the meeting is over, each participant takes away the strategic and confidential information related to its system. Thus, this is only a temporary pooling of information, though a vital one to enable the subsequent analysis. This approach for confidential information protection can be also used during the actions aimed at mitigation of vulnerability. Where points of high vulnerability have been identified through functional and/or geographical interdependencies analysis, involved organizations are left to work together to find a possible improvement. Their activities can include technical or organizational changes, changes in flow and use of primary and alternative resources, etc. After mutual activities are finished operators can come back to partners, so the information about the interdependencies can be updated and used for simulation. The presented tool works in the manner of Early Warning System (EWS). EWSs are generally composed of four inter-related key elements: risk knowledge, monitoring and warning service, dissemination and communication and response capability (UN/ISDR, 2006), and since it addresses only the first three key elements it is not a real EWS but more system able to make a good mobilization of the resources – so can be defined as *Early Mobilization and Cooperation System*. The future development should include utilization in the real-time environment – during the response phase of EM.

4.5.2 Role and involvement of the Civil Protection of Montreal metropolitan area

The Organization of Civil Protection of Montreal metropolitan area (OSCAM) is activated when a disturbing situation represents a significant risk to the life and health security of the population. How does the OSCAM mobilization works? It must first make an assessment process and analysis of the situation based on available information. Several tools (telemetry stations, weather alerts, number of 911 calls, etc.) allow them to gather information on various events that are occurring, or may occur. According to the situation, the coordinator of emergency preparedness will determine if one goes to standby, alert or intervention mode. Each alert level corresponds to a different level of mobilization (used to determine who will be mobilized) that are also different from one risk from another. Different indicators, are established by the people who are directly involved in the risk – experts in the domain. The indicators are constantly followed and when the threshold is reached (defined for every risk) mobilization starts. If there are no specific indicators the coordinator will always have the final say.

OSCAM is able to reach each people who run (are responsible for) each major infrastructure. They can get in touch with anybody who is involved in municipality at any kind of level. Automatic phone system can call each stakeholder or its replacement very quickly. Message will reach to every phone number and email until somebody answers and acknowledges that he will report on duty. System is automatic so it sends very short situation update, and tells what actions OSCAM requires – to come to work, or to get ready to be able to come to work in a few hours. Every municipal stakeholder has pre-defined missions, so there are standard pre-planned procedures (who does what) that people would have to follow in the event of a disaster. If there is a risk that has no specific plan, then it will be the emergency responders on the scene that will determine if they are overwhelmed or if they need emergency measures to give them special powers.

Coordination centre – half of the room are people who are in touch with the people in the field (fire department, police department, ambulance, representative from public health, representative of public transport) – on the other side there are people in charge of gathering information, people in charge of financial aspects, logistics,

elected people, people in charge of communications – each of members is just in touch with his entire team in a different room. Representatives of each infrastructure operator have their own centre and communication with representative – liaison agent who has power to make decision. Collecting information that would facilitate strategic decisions is the responsibility at the center. Collected situational awareness information is transferred to the coordinator who then decides who he wants at the table. Decisions are made based on the impact on the population. Not how to fix a damaged infrastructure but how to minimise the impact on the surrounding population. At the emergency coordination center the site is handled but also the consequences on the rest of the population. It's easier to make a decision when persons from very different backgrounds/or different organizations are together, having a multi angle on things to consider (e.g. Doctor, toxicologist, CBR specialist, surveillance – all talking to each other and making wiser decisions). The fire department is responsible for rescue operations.

The role of *Civil Security Center* is to coordinate among all the stakeholders in the city region. One of its responsibilities is to make special arrangements with external suppliers/stakeholders in the event of a disaster. The provincial level has very similar missions that could provide support if needed.

Sometimes, during the planning phase, it takes a lot of time to get information at that time but when they get into intervention there are never problems for getting any kind of information. It always remains a challenge when new players/personnel (due to promotions/retirements) come to play, but once they get to know people from OSCAM and why the information is needed - it gets easier. They're always afraid that OSCAM is going to ask some technical aspects/information, which it doesn't, only if they have something going on in the sector that OSCAM needs to know about.

In the tabletop exercises emphasis was made on the **importance to work together before, during and after a disruption event**. During exercises it easy for an organization to say something that they might not be able to deliver in real life. "*We get to know people; we get to make them think about what they just said; we get to make them realize what they would be responsible for delivering if that would really happened*", said Michel Bonin (Civil Security Center– City of Montréal) about the exercise benefits. "*We have established very close network of people – strategic intelligence – who talk a few times a week on any kind of subject, usually by a conference call. We've been working together so often and so long that now we know exactly what we can expect in a real emergency.*"

There are two basic ways to measure success (evaluate improvements):

- In preplanning every year report card is given for every person responsible for a mission – to evaluate his level of preparedness;
- After every kind of intervention debriefing is always made – out of the debriefing come recommendations – one person will be responsible to make follow ups to those recommendations. There are not many interventions but we still they get better every time – lessons are learned.

4.6 Pacific North-West Economic Region

Pacific NorthWest Economic Region (PNWER) is a statutory public/private non-profit created in 1991 by five US states (Idaho, Montana, Oregon, Washington and Alaska) and five Canadian jurisdictions (British Columbia, Alberta, Yukon, Saskatchewan and Northwest Territories) focused on issues impacting the economy of the Pacific NorthWest. State/jurisdiction governments understood that there are regional impacts that don't stop at borders but impact everyone, and realized as well that each of the governments had influence only within their own borders. By establishing PNWER as a statutory non-profit they are able to cross the borders, get all the people together and have a collective approach to tough issues. It is also much easier to make consistent government decisions. Nothing will adversely impact the economic vitality of the region – that is the essence of what is PNWER all about.

The first initiative to address regional infrastructure security issues was the creation of The Partnership for Regional Infrastructure Security in November 2001 and launch of the Regional Disaster Resilience and Homeland Security Program with the goal of improving the Pacific Northwest's ability to withstand and recover and to protect its CIs from all-hazards disasters. PNWER has, through its Center for Regional Disaster Resilience (CRDR), coordinated public and private critical infrastructures and key businesses stakeholders to examine interdependencies and cascading impacts resulting from different disasters. It also coordinates several regional 'sector councils' including cyber security, banking and finance, livestock health, energy, fusion center info sharing, etc. CRDR is committed to working with states, provinces, territories, and communities to develop regional public-private partnerships, develop action plans, and undertake pilot projects and activities to further this important mission. PNWER also provides training, education and developing tools, technologies, and approaches that build on existing capabilities, in order to secure interdependent infrastructures and improve all-hazards disaster preparedness and resilience. PNWER was listed as a best

practice for working with other states and provinces to address critical infrastructure security issues in the NGA's Governors Guide to Homeland Security (in March 2007) and also referenced in the National Infrastructure Protection Plan (NIPP) as the model for bringing the public and private sectors together to address critical infrastructure protection issues (in July 2009).
The Washington State Fusion Center (WSFC) is a unified counterterrorism, "all crimes," fusion center, incorporating agencies with intelligence, critical infrastructure, public safety and preparedness, resiliency, response and recovery missions. The WSFC is Washington State's single fusion center and concurrently supports federal, state, tribal agencies and private sector entities, regional and local law enforcement, public safety and homeland security by providing timely, relevant and high quality information and intelligence services.

4.6.1 NWWARN information sharing platform

One of the major achievements was the development of a regional alert and warning system named 'Northwest Warning, Alert and Response Network' (NWWARN), to encourage cross-sector information sharing. NWWARN project started in 2004 as a joint project between Federal Bureau of Investigation (FBI), DHS and PNWER, with assistance of regional CI operators as well as key business and government managers with responsibilities for security, preparedness, strategic planning, emergency management, response and recovery from all disasters and terrorism threats. DHS planned to use it for its own needs but never completed its implementation, so it was finally built as a notification platform adjusted to PNWER needs by MyStateUSA (Idaho). It is now the communication backbone of the Washington State Fusion Center (WSFC), routinely used for two-way communications with around 3000 CI/KR stakeholders.

Inside NWWARN platform information is shared through gatekeepers – experts in a particular infrastructure (water, electric utilities, shipping, defence industries). Gatekeepers are the trusted sources of information within an infrastructure, designed primarily to approve members within their infrastructure to be added to the system. Any of the gatekeepers could inquire with another gatekeeper for information on something that they need to know. Proprietary business information that can be very confidential is not needed in this kind of exchange, but mainly information on facilities and interdependencies with other systems.

Suspicious activity report had been identified as a gap and this capability was added to the platform afterwards. Social media integration enables to directly push information to Twitter or Facebook, while capability to draw information in (integrate e.g. *Google crises/alerts*) relies on crowdsourcing mechanisms to collect information. Ability to see in real time what kind of information is being posted online gives better situational awareness picture. Next big step would be to create a portion of NWWARN as a business operation center tool – in order to have a single source of information for business community to get and request information during crises. Businesses want accurate information from one place – informative to make decisions about their businesses.

In a nutshell, the goal of information sharing to help protect regional/national infrastructures, communities and the public has been achieved by:

- Maximizing near real-time, two-way sharing of situational information without delay
- Providing immediate distribution of critical information to the members who need to act on it
- Providing a place for members and non-members to submit suspicious activity reports to the FBI and Washington State Fusion Center
- Using commonly used, popular mediums for disseminating messages (phone calls, emails, text messages,etc.)

4.6.2 CIP Task Force and Blue Cascades Exercise Series

Information sharing and collaboration are a matter of relationships and trust – virtually never works, but physically – meeting people and building trust.

PNWER established the ***CIP Task Force*** – initiated coordination of regional Critical Infrastructure Protection (CIP) managers from the states and provinces as well as federal partners (Department of Homeland Security, Department of Defense, the Department of Energy, the U.S. Army Corps of Engineers, etc.) to build relationships with one another, share information and best practices on a regular basis, and thus increase infrastructure and community resilience. This coordination has led to many states and provinces sharing CIP plans and training and exercise opportunities and has helped build regional trust.

Blue Cascades Exercise Series have been developed to explore infrastructure interdependencies, at the same time building relationships and trust – supporting NWWARN use. Since 2002, PNWER has held six exercises addressing variety of topics (e.g. cyber security, earthquake recovery, pandemics, supply chain

resilience), each designed by stakeholders and reflecting regional concerns. Blue Cascades has become a model for bringing together public and private sector stakeholders to discuss cascading impacts across the region. It has been mostly about "who to talk to and about what, when something happens". Recovery and mitigation activities are often topics that don't get enough attention in other kind of venues, so having the opportunity to get into the recovery and restoration side of it (in a Blue Cascades type of exercise) is important to move everybody forward. Blue Cascades offer an opportunity to discuss about emergency plans with various types of jurisdictions and companies (like Boeing, Microsoft), decide on the best practices from each of the type of approach, implement best practices and modify own plans. One of the main outcomes of the exercises is that everyone ended up with much more comprehensive plans than individual departments or jurisdictions could create on their own. After each exercise, stakeholders assist in developing an action plan to address the issues uncovered during the exercise. Results of the exercises are kind of a roadmap – identify key areas to think about in planning and sometimes have specific topics that are necessary to make the region more resilient. Exercises have resulted in lessons learned and a lot of jurisdiction recovery plans that have not even had a thought in the past.

4.7 Scottish Government

Scotland is a country and a part of the United Kingdom that covers the northern third of the Great Britain. With a population of around 5.3 million (8.3% of UK population) and a total surface area of 78,800 km^2 (one third of UK area), Scotland is a rather small country. According to the Scottish Government website, the Scotland's GDP in 2013 was about 245.3 billion dollars that is about a tenth of the UK total GDP.

The flooding in England and Wales during the summer of 2007 was a timely point when it was acknowledged that Critical National Infrastructure (CNI) in Scotland is both critical to Scotland and the wider UK, and therefore, appropriate plans and strategies must be developed, involving all levels of the Government to protect the UK CNIs. Towards this aim, *Preparing Scotland* was established as the guidance to responders assisting them in planning, response and recovery. It is aimed to establish good practice based on professional expertise, legislation and lessons learned from planning for and dealing with major emergencies at regional and local levels. It is set out as a hub and spokes model; the hub, including philosophy, principles, governance structures and regulatory guidance and the spokes a range of detailed guidance on specific matters such as caring for people, mass fatalities and communicating with the public. '*Secure and Resilient*' is one of the spokes of Preparing Scotland, available publically in summary form and, reflecting its security status, available in full to relevant responders and organisations involved in the operation, protection and resilience of CIs. Secure and Resilient seeks to implement the UK National Security in relation to Critical National Infrastructure in Scotland. It sits under and meshes with the UK National Security Strategy, the UK CONTEST Strategy and the UK Critical National Infrastructure Protection Framework. It is intended to describe in more detail the Scottish Government contribution to these UK strategies including aims, responsibilities and delivery arrangements. It also clarifies areas where Scottish Government leads (on devolved matters) and areas which are reserved where Scottish Government aims to work closely in support of Whitehall departments.

The main unit devoted to CIP-R in Scotland is the Critical Infrastructure Resilience Unit (CIRU). CIRU works closely with relevant colleagues from within Scottish Government, the Cabinet Office and CNI Site Operators, in order to ensure that effective and appropriate resilience arrangements are in place across the devolved sectors in Scotland.

Table 4: Summary of Goals and Objectives of the cases

Local CIP-R Programme	Mission and Goals	Objectives
Copenhagen Capital Region	▪ Own, operate and maintain the railway and the entire motorway and the land works on both sides of the bridge ▪ Maintain a high level of accessibility and safety on the link ▪ Repay the loans raised to the construction of the link within a reasonable time frame	▪ Provide an efficient, safe and accessible traffic facility with minimum impact on the environment ▪ Provide fast, safe and reliable passage across Oresund at competitive prices ▪ Develop, implement and update a joint Danish-Swedish contingency plan ▪ Repay the bridge's loans within 30 years after its opening (1991) with most of the revenue deriving from road traffic ▪ Achieving financial stability in a long-term perspective
Kennemerland Safety Region	To deliver CIP-R through: ▪ Assurance of conformance with legal instruments, ▪ Maintenance of a public and private partnership for planning and crisis management, ▪ Assessment and updating of plans, ▪ Conduct of exercises to prove the practical viability and value of such plans.	▪ To ensure legal conformance of the regional disaster plan so as to maximize public safety and security. ▪ Preparation of measures concerning prevention of, and response to disasters and serious accidents in the municipality, and so the partnership aims to ensure CIP-R conforms to and benefits from regional safety planning. ▪ Establishing an emergency plan in compliance with the legal provisions of combating accidents and disasters to maximize safety and security. ▪ Assessment and updating of the crisis plan. ▪ Conduct exercises at least once every two years to demonstrate and test the emergency planning
Lombardy Region	▪ Evolution of the governance processes, decision-making and operational resilience of regional CIs; ▪ Maintaining a continuous process and shared identification and monitoring of threats, vulnerabilities and consequent risk analysis; ▪ Definition of procedures and protocols for the exchange of information and operational interaction between all the actors involved; ▪ Studying the most appropriate technologies, enabling the operating model of reference and able to guarantee security of access and protection of information	▪ Characterisation of the critical nodes of major regional transport and energy infrastructures; globally more than 200 regional nodes have been identified and documented; ▪ Analysis of the accidents influencing regional CIs and creating a series of historical cases; ▪ Development of vulnerability and resilience studies based on specific quantitative simulation tool; ▪ Design, validation and implementation of collaborative emergency plans; ▪ Standardization of communication among the actors – mapping information relevant and communication channels, dealing with interoperability and security of IS.
Louisiana	▪ To create a disaster resilient business community by building from current preparedness efforts, thereby helping Louisiana businesses to become more disaster resistant and able to support the various response and recovery efforts of the State and local community. ▪ To improve disaster preparedness, response and self-sufficiency, reduce reliance on FEMA, and maximize business, industry and economic stabilization. ▪ To Provide support in any major disaster - focus on providing situational awareness and resource support, supporting community recovery, mitigation, and economic stabilization.	▪ Facilitating bi-directional communication of critical information between the State and private sector and promote the resumption of normal business operations; ▪ Enhancing participation by businesses and non-profit organizations in disaster management efforts ▪ Joint trainings and exercises with the public and private sectors; ▪ Economic assessment of events impact to major State economic drivers and the resulting impacts to regional, State, and national economies; ▪ Maximizing the use of Louisiana businesses and national private sector resources and distribution capabilities to provide needed emergency response products and services; ▪ Supporting the coordination of voluntary donations from businesses through the Voluntary Organizations Active in Disaster (VOADs) and individuals.
Montreal Metropolitan Community	The Centre Risque & Performance (CRP) is dedicated to the study of interdependencies between critical infrastructures. In concert with partners from the public and private sectors, its mission is to integrate risk and resilience evaluation into the management mechanisms of industrial and governmental systems.	▪ Developing a methodology of interdependency modelling and evaluation ▪ Creating operational planning tools of emergency measures. ▪ Validating and integrate the CRP tools into day-to-day professional activities of network administrators. ▪ Training highly qualified personnel in the risk management and analysis field, in organizational resiliency and interdependency evaluation.
Pacific NorthWest Economic	▪ To improve the Pacific Northwest's ability to withstand and recover and to protect its critical infrastructures from all-hazards disasters	▪ Developing and conducting regional infrastructure interdependencies initiatives focused on various threat scenarios that include regional cross-sector/cross discipline workshops and exercises;

Region (PNWER)	▪ To coordinate regional Sector Councils, public and private critical infrastructures and key businesses stakeholders to examine interdependencies and cascading impacts resulting from different disasters. ▪ To develop regional public-private partnerships. ▪ To provide training, education and developing tools, technologies, and approaches to secure interdependent infrastructures and improve all-hazards disaster preparedness and resilience.	▪ Seeking funding and other resources to support regional pilot projects and other activities and to enable State and local agencies to address regional preparedness needs; ▪ Overseeing the implementation of priority projects and activities in a cost-effective, timely and ethical manner; ▪ Conducting outreach and develop and facilitate seminars, workshops, and targeted exercises to raise awareness and test the level of preparedness. ▪ Communicating stakeholder validated regional disaster resilience recommendations to State and provincial governments and policymakers.
Scottish Government	▪ Lead the way in reducing the vulnerability of CNI in the Devolved Sectors in Scotland by ensuring that appropriate protective security and resilience arrangements are in place. ▪ Support UK Government in their efforts to reduce the vulnerability of the CNI in Reserved Sectors and sub-sectors (e.g. Energy, Finance) through enhanced protective security & resilience. ▪ Minimize disruption to the Scottish public and business community by ensuring that relevant Consequence Management response plans are in place and Scotland is able to deal with a civil emergency (e.g. Preparing Scotland hub and spoke model). ▪ Develop a Scotland CNI partnership framework to ensure shared understanding and ownership of CNI issues in Scotland. ▪ Adopt a robust, proactive approach to all aspects of CNI planning and protection in Scotland, in line with the UK Government National Security Strategy mindful of the distinction between devolved and reserved areas.	*Pursue* ▪ Enhance local intelligence gathering opportunities and capability in the vicinity of CNI sites; ▪ Increase awareness and enhance quality of intelligence submissions. ▪ Prevent ▪ Develop Community Engagement strategies,16 where appropriate and agreed (subject to further consultation) which are relevant to the needs of the communities living in the vicinity of certain CNI sites; ▪ Develop Community Impact Assessments, where appropriate and agreed (subject to further consultation) which will assist in the implementation of new protective security and resilience projects. *Protect* ▪ Lead the way to reduce the vulnerability of the CNI in Devolved Sectors in Scotland by ensuring that appropriate protective security and resilience arrangements are in place; ▪ Support UK Government in reducing the vulnerability of CNI sites in the Reserved Sectors in Scotland; ▪ Work in partnership with CPNI, SSDs and others to develop protective security arrangements on the approach to CNI sites where appropriate, which are realistic and proportionate based on current threat and risk assessments; ▪ Monitor the development of site specific incident response plans; ▪ Monitor the development of Generic Counter Terrorist incident response Plans; ▪ Where appropriate, and in Reserved Sectors in consultation with the SSD, encourage infrastructure sectors to protect critical assets to avoid disruption to services from natural hazards. *Prepare* ▪ Develop a detailed understanding of the interdependencies and impact of loss issues for Scotland as a whole and for each of the SCG areas; ▪ Develop local planning arrangements, which seek to integrate emergency planning and counter terrorist planning teams, with the aim of providing realistic and effective contingency plans for all CNI sites; ▪ Policies to adapt to increasing threat from climate change; ▪ Support information sharing on infrastructure to improve emergency planning and response arrangements for natural hazards; ▪ Promote policies to ensure location, layout and design of new infrastructure considers risks from natural hazards; ▪ Work with infrastructure sectors to improve the resilience of networks and systems providing essential services.

Table 5: Summary of the main practices

Local CIP-R Programme	Main Practices

Copenhagen Capital Region	▪ Regulations for transport of hazardous goods. ▪ A holistic risk analysis (2010) to identify and prioritise the company's risks. Once a year, the Board of Directors presents a report that sets out the company's key risks and specific proposals for handling them. ▪ Joint contingency plans including an internal crisis response, to handle accidents on the link. The contingency plans are set as a part of the national safety plans of both Denmark and Sweden, and are tested regularly through exercises. Implementation of the Joint contingency plans. ▪ Continuous exercises and training s including full-scale exercises every 4 years, table-top exercises, small-scale exercises (scenarios) and weekly alerting exercises. ▪ An e-learning platform for involved parties to learn safety issues and get prepared for accidents. ▪ Two control rooms located on the Danish and Swedish sides. ▪ Partnership with 9 Danish and 6 Swedish agencies, including local police, fire, rescue, medical, alarm units and the traffic and rail control agencies. ▪ Tetra – RAKEL/SINE Gateway System: SINE is a digital radio network based on the Tetra standard and is used by all Danish emergency services dealing with public order, safety and health. ▪ Other communication tools: - Radio - Dark Fibre Link ▪ COMputer-Based Alarm System Oresundsbron (COMBAS O): A computer-based alarm system for the Oresund Fixed Link to ensure efficient and rapid alarms to relevant parties and immediately accessible action plans.
Kennemerland Safety Region	▪ Emergency response plans and their implementation: - Joint Local Emergency Response Action Plan (LERAP) implemented at Schiphol as local crisis management plan driven by Airline and local First Responder - 2014 updated Crisis Management Plan Schiphol issued by VRK including roles for Private Partners (Rail, Cargo Companies, etc.). The plan will be updated on a yearly basis. - The Emergency Plan of AAS - Emergency plan for the Schiphol tunnel of ProRail - Operational plan of the Royal Military Constabulary - Plans of the Fire Department and Health Department (GHOR) - Municipal plans Shelter & Care, CRIB and Communication - Procedures/plans LVNL, KLM, and other private organisations ▪ Regular exercises of the safety region and those held by the Amsterdam Airport Schiphol. ▪ Exchange of relevant documents, as well as discussion in meetings regarding safety and response topics. ▪ The cooperation between Amsterdam Airport Schiphol and the Safety Region Kennemerland is based on activities at specific levels: - Dispatch Centers: - Executive-operational level partnership - Crisis response - Steering and administrative groups Schiphol ▪ LCMS (National Emergency Management System): a net-centric, web-based shared data system that ensures the information used in the organisation is at all times the same, known and verified, and this applies to neighbouring safety regions and national agencies.
Lombardy Region	▪ Mapping of emergency management processes and vital node analysis: - More than 200 regional critical nodes have been identified and documented as a ranking list of most critical nodes and clusters of nodes - Analysis of the accidents influencing regional CIs and creating a series of historical cases - Mapping the organizational models and operational processes of emergency management of the main CI operators active in the region ▪ Thematic Task-Forces (TTF): 3 TTF have been established, one focused on mapping of the information flows and communication channels among actors, another focused on developing collaborative procedures for coping with major meteorological events and the third one to set up collaborative activities in case of large blackout events.
Louisiana (LABEOC)	▪ CI/KR interdependencies and risk analyses including CI Consequence Analysis and Infrastructure Surveillance and Risk Assessment. ▪ "Big business-small business" Emergency Management Mentorship program: engaging big businesses (willing and able to mentor), with the small ones helping them to strengthen their disaster preparedness and reduce recovery time. The program also improves response capabilities and results in business recovery plans. ▪ Web portal for the LA BEOC where businesses are asked to register with the state before a disaster and identify any products or services they might provide to assist communities in the state that have been affected by a disaster. ▪ Functioning of the NIMSAT web portal during emergencies in providing products and services listed by businesses.

	▪ Improving business resilience and survivability through temporary finding alternative ways of providing essential services until the infrastructure functioning has been recovered.
Montreal Metropolitan Community	▪ Centre Risque & Performance (CRP) of the École Polytechnique de Montréal supports the programme by consolidating the theory of organisational resilience, establishing a common set of terms and developing a method to evaluate resilience. ▪ DOMINO: a modelling, mapping, decision and planning assistance tool which is a system for managing interdependencies and analysing domino effects. ▪ The *Civil Security Center* of The Organisation of Civil Protection of Montreal metropolitan area (OSCAM) has made special arrangements with external suppliers/stakeholders in the event of a disaster. OSCAM is activated when a disturbing situation represents a significant risk to the life and health security of the population. ▪ Table-top exercises with an emphasis on the importance to work together before, during and after a disruption event. ▪ 2008 Quebec government's initiative to increase the resilience of its essential systems coordinated by the Civil security of Quebec (OSCQ), focused on maintaining or restoring the functioning of essential systems to an acceptable level despite any failures that might occur.
Pacific NorthWest Economic Region (PNWER)	▪ Center for Regional Disaster Resilience (CRDR): coordinates public and private critical infrastructures and key businesses stakeholders to examine interdependencies and cascading impacts resulting from different disasters. It also coordinates several regional 'sector councils' including cyber security, energy, fusion center info sharing, etc. ▪ CIP Task Force – initiated coordination of regional Critical Infrastructure Protection (CIP) managers from the states and provinces as well as federal partners to build relationships with one another, share information and best practices on a regular basis, and thus increase infrastructure and community resilience, leading to many states and provinces sharing CIP plans and training and exercise opportunities. ▪ 'Northwest Warning, Alert and Response Network' NWWARN information sharing platform: a regional alert and warning system to encourage cross-sector information sharing, which is now the communication backbone of the Washington State Fusion Center (WSFC), routinely used for two-way communications with around 3000 CI/KR stakeholders. ▪ Blue Cascades Exercise Series: developed to explore infrastructure interdependencies, at the same time building relationships and trust – supporting NWWARN use, including 6 exercises addressing variety of topics (e.g. cyber security, earthquake recovery, pandemics, supply chain resilience). Exercises have resulted in lessons learned and a lot of jurisdiction emergency and recovery plans. ▪ Regional Supply Chain Resilience Project: developing a supply chain resilience public-private sector working group that is able to provide input and advice on issues related to regional supply chain resilience to strengthen the region's ability to withstand and rapidly recover from disasters. ▪ Pacific Northwest Emergency Management Arrangement: a bi-national plan for recovering from a disaster in a cross-border area (CRDR). ▪ Private-Sector-Led Exercises: The CRDR participates in private-sector-led exercises, with trusted relationships as a primary benefit. ▪ Region 6 Critical Infrastructure Protection Work Group (CIP WG): made up of the region's key agencies and voluntary private-sector representation from some of the county's largest employers and owners and operators. The Region 6 CIP WG and the DHS Protective Security Advisor (PSA) have worked with the CRDR to facilitate interdependency workshops, tabletop exercises, and other partnership-building activities. ▪ Supply Chain Resilience Task Force: During an emergency, the CRDR may activate this task force to communicate directly with an EOC about what the critical elements and decisions are that would affect the region three to six months from the time of the incident.
Scottish Government	▪ 'Secure and Resilient' supports the all-risks approach outlined in the UK National Security Strategy by addressing UK Government strategies in tackling the priority risks outlined in the UK Government National Security Risk Assessment (NSRA) and National Risk Assessment (NRA), as well as other identified risks specific to Scotland. ▪ Critical Infrastructure Resilience Unit (CIRU) as the main unit devoted to CIP-R related activities in Scotland aimed to ensure that effective and appropriate resilience arrangements are in place across the devolved sectors in Scotland. ▪ 'Preparing Scotland' - set out as a 'hub and spokes' model - established as the guidance to responders assisting them in planning, response and recovery and aimed to establish good practice based on professional expertise, legislation and lessons learned from planning for and dealing with major emergencies at regional and local levels. Available in full to relevant responders and organisations involved in the operation, protection and resilience of Cis. ▪ Operation Estrela - infrastructure resilience exercise programme to threat from insider attack.

5. Discussion

Despite all the cases refer to a local dimension, they differ a lot in terms of institutional context and size of the Public-Private Partnership. It may also be noted that goals and objectives are largely heterogeneous, ranging from enhancing Emergency Management coordination to the development of a fully integrated regional resilience strategy.

Additional relevant findings that emerged by the in-depth analysis of the case studies are:

- The continuous improvement strategy implemented in most of the cases is based on a sequence of small but touchable win-win achievements; there are no cases of large programmes fully financed over a long time horizon;
- Activities and implemented technological or organisational solutions are largely focused on EM cycle; resilience functions are not emphasised as core dimensions to develop the contents of the programmes;
- Collaborative and qualitative approaches to solution design are dominant;
- Understanding/modelling and documenting interdependencies are issues addressed by almost all the programmes as part of the key prevention activities;
- Enhancing information sharing among all the public and private stakeholders is regarded as one of the key success factors and is deserved of specific support platforms and reference agreements;
- Exercises are the most common practice used to enhance awareness, trust and to build inter-organisational collaboration culture between public and private stakeholders.

The framework for the Development of Regional CIP-R Programmes provides the list and the relationships between the key elements that are needed for a successful and sustainable programme design and implementation (Figure 13).

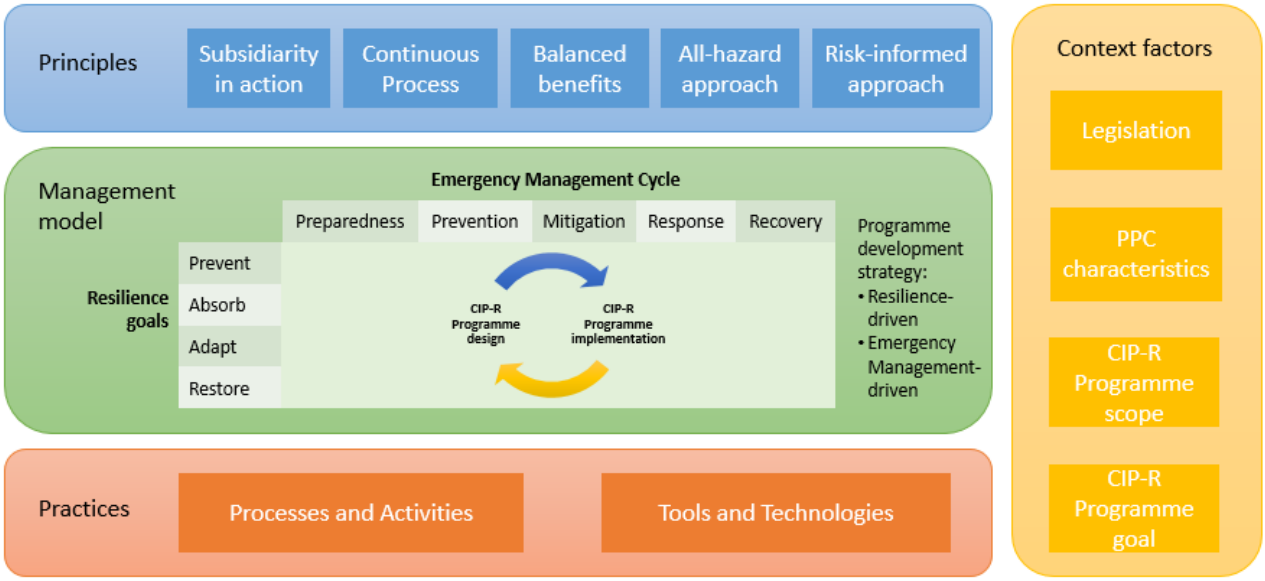

Figure 13: Framework for the development of Regional CIP-R programmes

The framework comprises four types of elements: the fundamental principles for a successful CIP-R programme development, the components of the management model, the set of practices that can be used to implement the programme, and the relevant context factors that influence the programme over its entire life cycle.

5.1 The fundamental principles

The development of regional CIP-R programmes and their CIP-R planning approach are grounded on the following five fundamental principles.

1) Subsidiarity “in action”

Subsidiarity and complementarity principles are at the roots of the EPCIP Programme. Regional strategies and programmes for CIP-R represent the best existing examples of a bottom-up approach to the subject and, as

such, the most promising opportunity for a deeper and more effective deployment of the subsidiarity principle in the CIP-R domain.

Involving stakeholders at regional level does not mean involving 'regional' CI operators only, but more precisely establish collaborative processes with relevant/national CI operators at a level that is closer to the field, thus closer to the implementation arena. A bottom up approach can leverage on existing local experiences to design and implement an effective CIP-R programme. This subsidiarity 'in action' is made of recognition, support, involvement, harmonisation and sometimes devolution to single stakeholders or group of stakeholders that brings distinctive capabilities for building the programme. Thus, subsidiarity "in action" can ensure that regional knowledge and expertise can fully address CIP-R through PPP where the bottom-up approach is regionally focused yet responsive to, and connected with, relevant national concerns.

2) Continuous improvement process

Existing successful experiences demonstrate that many local CIP-R Programmes rapidly evolved over the time, thanks to the virtuous cycle of:

- gaining commitment of some key stakeholders on relevant disruption scenarios;
- fixing achievable and win-win objectives in the short term;
- communicating tangible results and achievements to all stakeholders to involve them in the programme and expand the PPP;
- revising and enhancing scope, goals and objectives of the CIP-R programme thanks to the new entries.

3) Balanced benefits

A Regional CIP-Programme led by a local PPP is generally driven by a mix of different interests and needs: public authorities, responders' organisations, CI operators and owners, businesses ... Normally, it also covers a mid-long term planning horizon. Hence, the prioritisation of different types of achievable results is a key issue. It emerges that the strategy of pursuing balanced benefits – government vs business needs; short vs long term – is the most effective to assure long term sustainability of the programme and the achievement of tangible results.

4) All-hazard approach

The term 'All-hazard approach' denotes a way of CIP-R development able to comprise all conditions, environmental or manmade, either accidental or intentional, that have the potential to cause injury, illness, death, or loss of assets, service delivery, or other intangibles; or alternatively causing functional social, economic, or environmental harm.

Three closely related factors necessitate the development of a holistic, all-hazards approach to regional CIP-R:

- infrastructure vulnerabilities and interdependencies
- information sharing processes and solutions
- public-private collaboration

5) Risk-informed approach.

Risk-informed decision-making (RIDM) is a deliberative process that uses a set of performance measures, together with other considerations, to "inform" decision-making. The RIDM process acknowledges that human judgment has a relevant role in decisions, and that technical information cannot be the unique basis for decision-making. This is because of inevitable gaps in the technical information, and also because decision-making is an intrinsically subjective, value-based task. In tackling complex decision-making problems involving multiple, competing objectives, the cumulative knowledge provided by experienced personnel is essential for integrating technical and nontechnical elements to produce dependable decisions.

5.2 Management model

The key components of the management model of a Regional CIP-R Programme are:

1) Contents development matrix (Emergency Management cycle vs Resilience core functions);
2) CIP-R Programme design and implementation process;
3) CIP-R Programme long term development strategy.

A long lasting CIP-R Programme is expected to pass through different phases in its life cycle. Its evolution is strongly influenced by the origin and goal set at the beginning of the Regional CIP-R Programme life. Sometimes the goal may change due to changes in political priorities (e.g. security and protection issues vs safety and resilience issues) or dramatic evolutions in the most relevant threats a certain region is exposed to (e.g. due to Climate Change). Another evolutionary dimension is the increase in size of the PPP, thanks to new members, or of the geographical extension of the programme.

The temporal evolution of the CIP-R programme, managed through its design-implementation cycles, can be driven, time by time, by different priorities or by a different mix of perspectives. Here we highlight two main development strategies, two perspectives (or logic) are equally important and complementary:

- ***Emergency Management-driven development strategy*** emphasises the operational integration of the CIP-R Programme with the management of real events. It is preferable when the PPP is led by public authorities, with security roles, or by responders; in these cases, the goal of the CIP-Programme is generally more focused on EM improvement (e.g. Kennemerland Safety Region, LABEOC, PNWER).
- ***Resilience-driven development strategy*** emphasises the supportive role of the PPP and its Regional CIP-R Programme. The programme is developed to build protection and resilience capabilities into the regional system, that are exploited by different organisations (e.g. EM, Civil Protection agencies, or Police forces) through decision making and operational processes that are largely out of the scope of the programme (e.g. Lombardy Region, Scotland). This is typical when the PPP is led by private stakeholders (Montreal Metropolitan Community).

One of the key issues in developing successful CIP-R programmes is that these two perspectives are not completely overlapped, even though they share some common traits. Hence, a way must be found to assume both and harmonise them into a unique and consistent programme. Having a Regional CIP-R Programme aligned with the Emergency (or Disaster) Management cycle is also vital to check and assure the compatibility and full integration of the programme with the EM or Civil Protection system already in place in the region. An approach which facilitates emergency services and CI operators to collaborate in addressing resilience improvement measures, while planning to cope with CI disruptions (Figure 14), was proposed by Kozine & Andersen (2015).

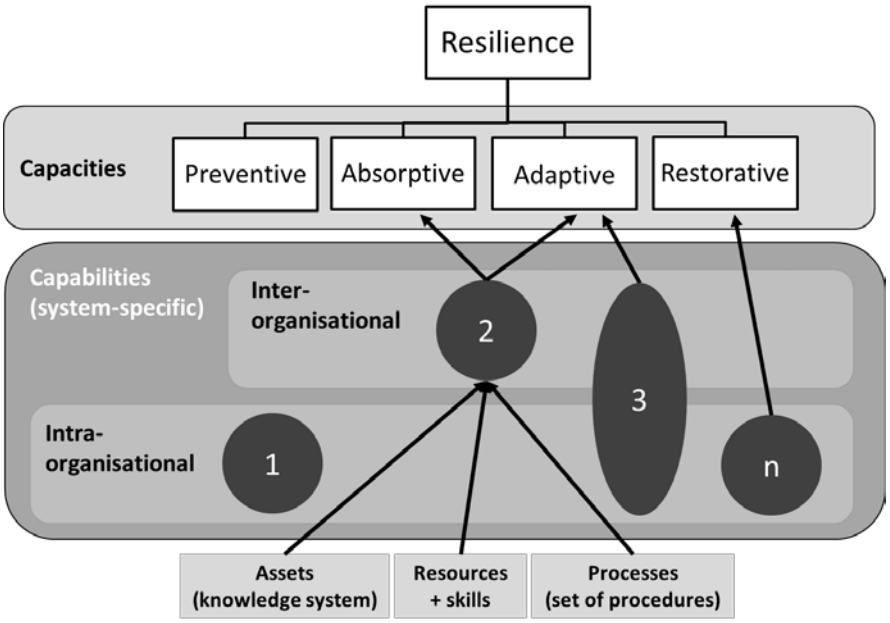

Figure 14: Building system resilience (adapted from Kozine & Andersen (2015))

This framework for integrating the resilience capacities of CI into the EM cycle reflects the main characteristics of such emergencies (e.g. interdependent, multi-sectoral, multi-stakeholder) and supports the identification, assessment and development of specific resilience (technical and organizational) capabilities. The Capability Building Cycle (Figure 15) presents an operational approach for continuous process of programme design and implementation (as in the framework – Figure 13) of a Regional CIP-R Programme. A pilot case in Lombardy

Region (Italy) fostered collaborative EM in the context of public-private collaboration for CI resilience (by supporting the preparedness and collaborative planning activities) and demonstrated the applicability of the approach (Trucco et al., 2016).

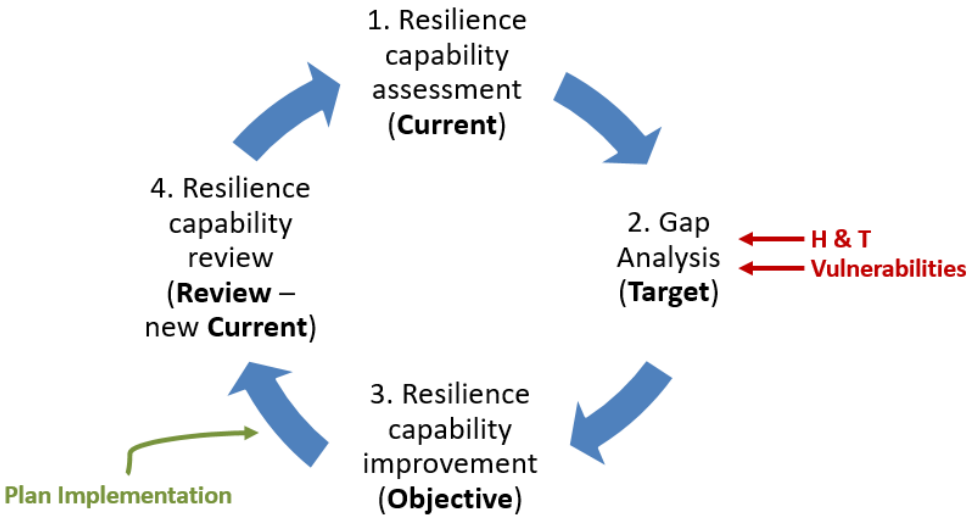

Figure 15: Capability building cycle (adapted from Trucco et al., 2016)

5.3 Good Practices

Good practices (GPs) are generally defined as 'Commercial or professional procedures that are accepted or prescribed as being correct or most effective'. It is any collection of specific methods that when applied solve an existing problem, produce expected results and bring benefits. Within the context of these guidelines, the concept applies to available knowledge to addressing:

- Establishment and management of regional PPPs for Critical Infrastructure Protection and Resilience;
- The implementation of a CIP-R programme in an efficient and effective way, thus assuring the achievement of its main objectives and goal.

The rationale is to disseminate and promote a set of practices that have been effective in addressing key issues in regional CIP-R initiatives and, as such, can be deemed as a reference or source of expertise to set-up and develop regional CIP-R programmes.

The practices can be classified into two main categories:

- Activities and processes;
- Tools and technologies.

The collection of the identified GPs (Trucco et al., 2015) had also been evaluated along three main parameters (implementation effort, transferability potential, type and relevance of expected benefits) through engagement of international experts, professionals and researchers the GPs.

5.4 Context factors

Finally, different context factors influence the contents and the management model of a Regional CIP-R Programme in its start-up and evolutionary process phases.

1) **Legislation** (national and local) - In addition to EC legislation on CIP (EC Directive 2008/114/EC) and the related European Programme for Critical Infrastructure Protection (EPCIP), national legislation in single Member States plays a crucial role in shaping regional initiatives on CIP-R.
   In several EU countries, opportunities for engaging stakeholders in the development of a local CIP-R programme might be found directly in extant legislation:
   - thanks to awareness and concern of CI operators induced by responsibilities and enforced requirements for action (e.g. in Scotland and Italy);
   - well established culture and standards at national level thanks to a coherent regulatory framework (e.g. The Netherlands);
   - resources – financial, technological, skills and knowledge – made available at nation-al level (e.g. in the Netherlands and Denmark);

- full or partial devolution of CIP-R responsibilities with clear interfaces with national and EC levels (e.g. Scotland).

2) **PPP Characteristics** - characteristics of the PPP that leads a specific Regional CIP-R Programme have strong influence on the scope, objectives, activities, and also on the quality of achievements of the programme itself.
   Governance by a Lead Organisation is the most common form of governance for PPPs addressing CIP-R issues, where the leading organisation is a public body with specific responsibilities for CIP-R at national or regional level. There are some examples of shared governance where private CI operators are more directly engaged in defining scope and goals of the collaborative network, such as the case of Montreal Metropolitan Community (Canada). In this case, the PPP is collectively led by CI operators and technically sup-ported by the Ecole Polytechnique de Montreal, scope and goal of the partnerships is however limited to the understanding and assessment of interdependencies among CI in the area. Public authorities receive the results of the assessment and are only involved in the evaluation of potential win-win solutions for the removal of most critical dependencies or their better management. These types of PPPs are characterised by a few number of member organisation, a narrow and well-focused goal but with a high level of consensus.
   When the PPP is a direct result of a public policy for involving the private sector in the development and/or implementation of CIP-R programmes, such as in The Netherlands where "Security Regions" are mandated to do so, the size is generally larger, and the scope and objectives are predominantly set by public authorities. This highest potential for impact on the region is balanced by the challenges brought by a relatively lower level of trust and goal consensus. As an example, it may happen that in practice not all the involved CI operators are willing to commit themselves to implementing collaborative plans, containing additional responsibilities or the mobilisation of additional resources, put in place under the strong leadership of public authorities.

3) **CIP-R Programme Scope and Goal** - Characteristics of a Regional CIP-R programme strongly depend on the scope of the programme and on the goals that the leading Organisation or PPP want to achieve through the programme. The most important scoping factor is the policy/strategy background set for the programme, that is: protection-centred vs resilience-centred programmes. Other elements that influence the overall scope: The set of CI sectors covered, the type of regional dimension of the programme, the Phases of the EM cycle covered by the programme...
   Different goals or priorities are also possible for Regional CIP-Programmes, such as:
   - Improvement of Emergency and Disaster Management (also cross-border);
   - Identification and assessment of CI interdependencies;
   - Contribute to a better protection and resilience of National Critical Infrastructure;
   - Business continuity of different private sectors, CI operators, SMEs;
   - Community resilience.

6. Conclusions

PPP's effectiveness and contribution to CIP-R largely depends on the way it has been implemented, its main focus, and the achieved maturity level its inherent relationships. We argue that PPPs present a good way to tackle CIP-R issues on low (regional) level, but there is still a long way to go before reaching their full potential. Things are constantly changing so it makes it a never-ending process to make sure that you have a partnership and system that can respond effectively and efficiently when you need it. The emergence of CIP-R focused PPPs opens to the need of (re)defining missions, mutual relationships and governance models of multilevel CIP-R programmes (continental, national, local, ...) as key factors for effective and efficient policies. Another challenge is the important role of universities and research centres in developing and incorporating appropriate and relevant scientific knowledge into the activities and efforts in protection and resilience of CI.

Regional level is the operational level where the CIP-R concerns are first tackled, the first one to carry the burden of incident response, and the level where the major portion of resilience capabilities are built. The implementation process has to be mainly developed according to a bottom-up approach, since the top-down approach (which policy-making follows) does not ensure the success of CIP-R measures (FEMA, 2011). In order to properly address all the challenges, it is important and necessary to align programmes on different levels – i.e. in which way are regional CIP-R strategies able to address CIP-R issues at higher levels, and vice versa, how can CIP-R policies and strategies support a bottom-up approach in the form of regional programmes. Such an alignment needs to consider many aspects and dimensions in the context of CIP-R, such as principles, goals and objectives of these programmes and the multi-level partners, responsibilities, and activities.

What is even more important, is to avoid fragmentation within a regional CIP-R programme, from strategic to operational level. Regional programmes are based on the willingness of each partner to assume responsibility

for a share of the effort. The focus is on the process of building (collaborative) capabilities to anticipate, absorb, adapt to, and/or rapidly recover from a potentially disruptive event. The development of those capabilities (whether technical, organisational, social or economic), needs to be aligned with the programme strategy. Well-developed programmes following this approach are able to form cross-regional (and cross-border) relationships and possess ability to easily scale up, if needed.

This study can be used by both public and private entities to better understand the distinctive features of CIP-R related PPPs, their establishment, functioning and managements, possible strengths and weaknesses and different ways of achieving practical objectives.

Acknowledgment

The authors would like to express their gratitude to all the people involved in the four PPPs and collaborating organizations – namely, Centre Risque & Performance (CRP), Department of Mathematics and Industrial Engineering at École Polytechnique de Montréal (Québec, Canada), Organization of Civil Protection of Montreal (L'Organisation de sécurité civile de l'agglomération de Montréal – OSCAM), National Incident Management Systems and Advanced Technologies (NIMSAT) Institute at University of Louisiana, Lafayette (LA, USA), Pacific NorthWest Economic region, Seattle (WA, USA), GAP-Santé research unit at University of Ottawa (Ontario, Canada), Directorate General on Security and Civil Protection, Lombardy Region (Milan, Italy), Scottish Government (UK), Kennemerland Safety Region (The Netherlands), Oresundsbron (Denmark-Sweden), Technical University of Denmark (DTU), Danish Emergency Management Agency (DEMA) and Copenhagen Capital Region Pre-Hospital Services (Pre-Hosp) - for their help, time, collaborative efforts, availability for interviews, documentation and kind hospitality.

The present study has been funded with support from European Commission, under CIPS/ISEC Work Programme. The financial support is gratefully acknowledged. This publication reflects the views only of the author, and the European Commission cannot be held responsible for any use which may be made of the information contained therein.

References

American Heritage Dictionary of the English Language, 3rd edition (1996).

Andersson, J. J., & Malm, A. (2006). Public-private partnerships and the challenge of critical infrastructure protection. *International CIIP handbook*, *2*, 139-166.

Auerswald, P., Branscomb, L. M., La Porte, T. M., Michel-Kerjan, E., & Michel-Kerjan, E. (2005). The challenge of protecting critical infrastructure. *Issues in Science and Technology*, *22*(1), 77-83.

Barnes, J., & Newbold, K. (2005). Humans as a critical infrastructure: Public-private partnerships essential to resiliency and response. In *Critical Infrastructure Protection, First IEEE International Workshop on* (pp. 9-pp). IEEE.

Beaton, E. K., Boiney, L. G., Drury, J. L., GreenPope, R. A., Henriques, R. D., Howland, M., & Klein, G. L. (2010, May). Elements needed to support a crisis management collaboration framework. In *Integrated Communications Navigation and Surveillance Conference (ICNS), 2010* (pp. N1-1). IEEE.

Benbasat, I., Goldstein, D. K., & Mead, M. (1987). The case research strategy in studies of information systems. MIS quarterly, 369-386.

Boin, A. (2005) Designing effective response structures: A discussion of established pitfalls, best practices and critical design parameters. *A background paper prepared for the Swedish Tsunami Commission*, 2005.

Boin, A., & McConnell, A. (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.

Boone, W. (2012). *Full Spectrum Resilience: An Executive Summary*, CIP report June 2012, Center for Infrastructure Protection and Homeland Security, George Mason University, VA (USA)

Bouchon, S. (2006). The Vulnerability of interdependent Critical Infrastructures Systems: Epistemological and Conceptual State of the Art. *Institute for the Protection and Security of the Citizen, Joint Research Centre, European Commission*, *99*.

Cagno, E., De Ambroggi., M & Trucco, P (2011), Interdependency analysis of CIs in real scenarios, Proceedings of ESREL 2011 - Advances in Safety, Reliability and Risk Management, Bérenguer, Grall & Guedes Soares (eds), pp. 2508-2514, Taylor & Francis Group, London, ISBN 978-0-415-68379-1.

Comfort, L. K. (2007). Crisis management in hindsight: Cognition, communication, coordination, and control. *Public Administration Review*, *67*(s1), 189-197.

CRN Report (2009) 'Focal Report 2: Critical Infrastructure Protection', Zurich.

De Bruijne, M., & Van Eeten, M. (2007). Systems that should have failed: critical infrastructure protection in an institutionally fragmented environment. *Journal of contingencies and crisis management*, *15*(1), 18-29.

Denzin, N. K. (1989). The Research Act.–3. *Auflage. Englewood Cliffs*.
Department of Homeland Security (DHS, 2006). National infrastructure protection plan (NIPP), Washington, DC.
Department of Homeland Security (DHS, 2009). National infrastructure protection plan (NIPP): Partnering to enhance protection and resiliency, Washington, DC.
Department of Homeland Security (DHS, 2013). National infrastructure protection plan (NIPP): Partnering for Critical Infrastructure Security and Resilience, Washington, DC.
Department of Homeland Security US (DHS, 2013) website, Critical Infrastructure Protection Partnerships and Information Sharing (http://www.dhs.gov/critical-infrastructure-protection-partnerships-and-information-sharing), visited on 10/04/2013.
DHS (US), Homeland Security Grant Program - Supplemental Resource: Support For Public-Private Collaboration, 2012
Dunn Cavelty, M., & Suter, M. (2008). Early warning for critical infrastructure protection and the road to public-private information sharing. *Intelligencia y Seguridad*, *4*, 85-113.
Dunn-Cavelty, M., & Suter, M. (2009). Public–Private Partnerships are no silver bullet: An expanded governance model for Critical Infrastructure Protection. *International Journal of Critical Infrastructure Protection*, *2*(4), 179-187.
Eckert, S. (2005). Protecting Critical Infrastructure: The Role of the Private Sector. *Guns and Butter: The Political Economy of International Security, in: P. Dombrowski (Ed.), Lynne Rienner Publishers, Boulder, Colorado*.
Eisenhardt, K. M. (1989). Building theories from case study research. *Academy of management review*, *14*(4), 532-550.
European Commission (2005). Communication to the European Parliament, the Council, the European Economic and Social Committee and The Committee of the Regions on Public-Private Partnerships and Community Law on Public Procurement and Concessions, COM(2005) 569 final
European Commission (2005). *Green Paper on a European Programme for Critical Infrastructure Protection*, COM(2005) 576 final
European Commission (2006). Communication from the Commission of 12 December 2006 on a European Programme for Critical Infrastructure Protection, COM(2006) 786 final
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*
European Commission (2009) Conclusions of the European Council of 10/11 December 2009 on 'The Stockholm Programme — An open and secure Europe serving and protecting citizens (2010-2014)'; 17024/09.
European Commission (2012), Staff Working Document on the Review of the European Programme for Critical Infrastructure Protection (EPCIP), SWD(2012) 190 final
European Commission (2013), DG Home Affairs – Critical Infrastructures page. Available at: http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/crisis-and-terrorism/critical-infrastructure/index_en.htm
FEMA (2011). Five Years Later: An Assessment of the Post Katrina Emergency Management Reform Act, Written Statement of Craig Fugate, FEMA Administrator.
FEMA (2012). After Action Report of the first national conference on "Building Resilience through Public-Private Partnerships" August 3 – 4, 2011 Washington, D.C., progress published January 2012.
Givens, A. D., & Busch, N. E. (2013). Realizing the promise of public-private partnerships in US critical infrastructure protection. *International Journal of Critical Infrastructure Protection*, *6*(1), 39-50.
Heineman, B. W. Jr. (2011) Crisis Management Failures in Japan's Reactors and the BP Spill, *Harvard Business Review*
Helbing, D., Ammoser, H., & Kühnert, C. (2006). Information flows in hierarchical networks and the capability of organizations to successfully respond to failures, crises, and disasters. *Physica A: Statistical Mechanics and its Applications*, *363*(1), 141-150.
Henriques, F., & Rego, D. (2008). OASIS Tactical Situation Object: a route to interoperability. In *Proceedings of the 26th annual ACM International Conference on Design of Communication* (pp. 269-270). ACM.National Incident Management Systems and Advanced Technologies (NIMSAT, 2012) Institute, Compendium of Public-Private Partnerships for Emergency Management.
Hilton, B. (Ed.). (2006). *Emerging spatial information systems and applications*. IGI Global.
Kozine, I., & Andersen, H. B. (2015). Integration of resilience capabilities for Critical Infrastructures into the Emergency Management set-up. *L. Podofillini L, B. Sudret, B. Stojadinovic, E. Zio, W. Kröger (Eds.), Safety and Reliability of Complex Engineered Systems: ESREL, 2015*, 171-176.
Kröger, W. (2008). Critical infrastructures at risk: A need for a new conceptual approach and extended analytical tools. *Reliability Engineering & System Safety*, *93*(12), 1781-1787.
Lecomte, E. L., Pang, A. W., & Russell, J. W. (1998). *Ice storm'98* (p. 39). Ottawa,, Canada: Institute for Catastrophic Loss Reduction.
Lemyre, L., Pinsent, C., Boutette, P., Corneil, W., Riding, J., Riding, D., Johnson, M. Lalande-Markon, S. Gibson & Lemus, C. (2011). Research Using In Vivo Simulation of Meta-Organizational Shared Decision Making (SDM). Task 3:

Testing the Shared Decision Making Framework in Vivo (No. DRDC-CSS-CR-2011-32). Defence Research and Development Canada Ottawa (Ontario) Centre for Security Science.
Lombardy Region (2007), Regione Lombardia: PRIM 2007–2010, Programma Regionale Integrato di Mitigazione dei Rischi, Studi Preparatori – Incidenti ad elevata rilevanza sociale in Lombardia, Regione Lombardia – Protezione civile, Prevenzione e Polizia Locale (in Italian)
McEvily, B., Perrone, V., & Zaheer, A. (2003). Trust as an organizing principle. *Organization science*, *14*(1), 91-103.
McNally, R. K., Lee, S. W., Yavagal, D., & Xiang, W. N. (2007). Learning the critical infrastructure interdependencies through an ontology-based information system. *Environment and Planning B: Planning and Design*, *34*(6), 1103-1124.
Meredith, J. (1998). Building operations management theory through case and field research. *Journal of operations management*, *16*(4), 441-454.
Moteff, J. D. & Stevens, G. M. (2003), *Congressional Research Service, Critical Infrastructure Information Disclosure and Homeland Security*, RL31547 (Jan. 29, 2003).
Moynihan, D. P. (2009). The network governance of crisis response: Case studies of incident command systems. *Journal of Public Administration Research and Theory*, *19* (4), 895-915.
Natarajan, N. (2013). Partnerships and Information Sharing: The Administration's Efforts to Enhance Critical Infrastructure Security and Resilience. *CIP report April 2013, Center for Infrastructure Protection and Homeland Security, George Mason University, VA (USA)*
National Commission on the BP Deepwater Horizon Oil Spill and Offshore Drilling (2011), *Final Report: BP Deepwater Horizon Oil Spill and Offshore Drilling*, released January 11th, 2011.
National Incident Management Systems and Advanced Technologies (NIMSAT, 2012) Institute, Big Business - Small Business Mentorship Program launches for enhanced disaster resiliency, press release on June 1st, 2012.
National Infrastructure Advisory Council (NIAC, 2006), Public-Private Sector Intelligence Coordination – Final Report and Recommendations by the Council.
National Infrastructure Advisory Council (NIAC, 2012), Intelligence information sharing, Final Report and Recommendations, 2012
National Infrastructure Advisory Council (US). (2009). *Critical Infrastructure Resilience: Final Report and Recommendations*.
NATO (2007) Architecture Framework v3.
Ouyang, M. (2014). Review on modeling and simulation of interdependent critical infrastructure systems. *Reliability engineering & System safety*, *121*, 43-60.
PCCIP (1997). Protecting America's Infrastructures: The Report of the President's Commission on Critical Infrastructure Protection.
Percy, S. V. (2007). Mercenaries: Strong norm, weak law. *International Organization*, *61*(02), 367-397.
Petrenj, B. & Trucco, P. (2014). Simulation-based characterisation of critical infrastructure system resilience. International Journal of Critical Infrastructures, 10(3-4), 347-374.
Petrenj, B., Lettieri, E., & Trucco, P. (2013). Information sharing and collaboration for critical infrastructure resilience–a comprehensive review on barriers and emerging capabilities. *International Journal of Critical Infrastructures*, *9*(4), 304-329.
Presidential Policy Directive. (2013). Critical infrastructure security and resilience. PPD-21, Released February 12, 2013.
Prieto, D. (2006). Information sharing with the private sector. *Seeds of Disaster, Roots of Response. How Private Action Can Reduce Public Vulnerability*, 404-428.
Provan, K. G., & Kenis, P. (2008). Modes of network governance: Structure, management, and effectiveness. *Journal of public administration research and theory*, *18*(2), 229-252.
Pursiainen, C. (2009). The challenges for European critical infrastructure protection. *European Integration*, *31*(6), 721-739.
Robert, B., & Morabito, L. (2009). An approach to identifying geographic interdependencies among critical infrastructures. *International Journal of Critical Infrastructures*, *6*(1), 17-30.
Robert, B., De Calan, R., & Morabito, L. (2008). Modelling interdependencies among critical infrastructures. *International Journal of Critical Infrastructures*, *4*(4), 392-408.
Robert, B., Morabito, L., & Quenneville, O. (2007). The preventive approach to risks related to interdependent infrastructures. *International journal of emergency management*, *4*(2), 166-182.
Roby, C. J. & Alberts, D. S. (2012) NATO NEC C2 maturity model, *DoD Command and Control Research Program,* Washington, DC. Available at: www.dodccrp.org.
Schraagen, J. M., Veld, M. H., & De Koning, L. (2010). Information sharing during crisis management in hierarchical vs. network teams. *Journal of contingencies and crisis management*, *18*(2), 117-127.
Seuring, S. A. (2008). Assessing the rigor of case study research in supply chain management. *Supply Chain Management: An International Journal*, *13*(2), 128-137.
Shani, A. B., & Pasmore, W. A. (1985). Organization inquiry: Towards a new model of the action research process. *Contemporary Organization development: Current Thinking and Aplications, Scott, Foresman, Glenview, IL*, 438-448.

Shani, A. B., David, A., & Willson, C. (2004). Collaborative research: Alternative roadmaps. *N. Adler, AB (Rami) Shani & A. Styhre (Eds.), Collaborative research in organizations: Foundations for learning, change, and theoretical development*, 83-100.

Susman, G. I., & Evered, R. D. (1978). An assessment of the scientific merits of action research. *Administrative science quarterly*, 582-603.

Trucco, P., Cagno, E., & De Ambroggi, M. (2012). Dynamic functional modelling of vulnerability and interoperability of Critical Infrastructures. *Reliability Engineering & System Safety*, *105*, 51-63.

Trucco, P., Petrenj, B., Bouchon, S., & Di Mauro, C. (2015). The rise of regional programmes on critical infrastructure resilience: identification and assessment of current good practices. *WIT Transactions on The Built Environment*, *150*, 233-245.

Trucco, P., Petrenj, B., Kozine, I., & Andersen, H. B. (2016). Emergency management involving critical infrastructure disruptions: Operationalizing the deployment of resilience capabilities. In *Risk, Reliability and Safety: Innovating Theory and Practice* (pp. 548-555) ESREL 2016. CRC Press.

United Nations (2005), Report of the World Conference on disaster prevention, Kobe (Hyogo, Japan)

United Nations, International Strategy for Disaster Reduction (UN/ISDR, 2006) - Platform for the Promotion of Early Warning, available at: http://www.unisdr.org/2006/ppew/whats-ew/basics-ew.htm

Voss, C., Tsikriktsis, N., & Frohlich, M. (2002). Case research in operations management. *International journal of operations & production management*, *22*(2), 195-219.

Walsham, G. (1995). The emergence of interpretivism in IS research. *Information systems research*, *6*(4), 376-394.

Whyte, W. F., Greenwood, D. J., & Lazes, P. (1989). Participatory action research: Through practice to science in social research. *American Behavioral Scientist*, *32*(5), 513-551.

Willis, H. H., Lester, G., & Treverton, G. F. (2009). Information sharing for infrastructure risk management: Barriers and solutions. *Intelligence and National Security*, *24*(3), 339-365.

Yin, R. K. (2003). *Case study research: Design and methods*. Sage publications.