Policy Evaluation Framework on The Governance of Critical Infrastructure Resilience in Latin America

Mary Kate Fisher
Catherine Gamper

IDB
Improving lives

Cataloging-in-Publication data provided by the Inter-American Development Bank Felipe Herrera Library

Fisher, Mary Kate.Policy evaluation framework on the governance of critical infrastructure resilience in Latin America / Mary Kate Fisher, Catherine Gamper.p. cm.Includes bibliographic references.1. Infrastructure (Economics)-Security measures-Latin America. 2. Infrastructure (Economics)-Risk assessment-Latin America. I. Gamper, Catherine. II. Inter-American Development Bank. Environment, Rural Development and Disaster Risk Management Division. III. Organisation for Economic Co-operation and Development. IV. Title. IDB-CP-60

Authors:
Mary Kate Fisher
CNA Safety and Security Division
Catherine Gamper
OECD Public Governance and Territorial Development Directorate

Editor:
Sergio Lacambra
Lead Specialist in Disaster Risk Management, Inter-American Development Bank, IDB
Charles Baubion
Risk Governance Expert, Public Governance and Territorial Development Directorate Organization for Economic Co-operation and Development, OECD
Leigh Wolfrom
Policy Analyst, Directorate for Financial and Enterprise Affairs, Organization for Economic Co-operation and Development, OECD.

Keywords:
Governance,Resilience, Critical Infrastructure, Disasters, Risk.

JEL codes:
O18, O54 y Q54

Pictures:
Claudio Osorio

Design and Layout:
www.verogorri.com

www.iadb.org

Copyright © 2017 Inter-American Development Bank. This work is licensed under a Creative Commons IGO 3.0 Attribution-NonCommercial-NoDerivatives (CC-IGO BY-NC-ND 3.0 IGO) license (http://creativecommons.org/licenses/by-nc-nd/3.0/igo/legalcode)and may be reproduced with attribution to the IDB and for any non-commercial purpose. No derivative work is allowed.

Any dispute related to the use of the works of the IDB that cannot be settled amicably shall be submitted to arbitration pursuant to the UNCITRAL rules. The use of the IDB's name for any purpose other than for attribution, and the use of IDB's logo shall be subject to a separate written license agreement between the IDB and the user and is not authorized as part of this CC-IGO license.

Note that link provided above includes additional terms and conditions of the license.

The opinions expressed in this publication are those of the authors and do no t necessarily reflect the views of the Inter-American Development Bank, its Board of Directors, or the countries they represent.

For Further Information, Please Contact:
Sergio Lacambra: *slacambra@iadb.org*
Catherine Gamper: *catherine.gamper@oecd.org*

Policy Evaluation Framework on The Governance of Critical Infrastructure Resilience in Latin America

OECD
BETTER POLICIES FOR BETTER LIVES

REGIONAL POLICY DIALOGUE

IDB
Improving lives

Table Of Contents

Introduction[1]

The interconnectedness of supply chains, technological and financial systems that form the foundation of the global economy are vulnerable to unanticipated events such as natural disasters, failures in key technical systems or malicious attacks capable of disrupting these complex systems and yielding impacts across borders that sometimes resonate globally. In the past decade, OECD and BRIC countries have experienced an estimated USD 1.5 trillion in economic damages from large-scale disasters. Increased concentration of people, especially vulnerable populations, and economic assets in risk prone areas has been a key contributing factor (OECD, 2014a).

The Latin America and Caribbean region is particularly exposed to natural hazards including earthquakes, volcanoes, and extreme weather. Increasing climate variability is expected to exacerbate weather hazards in the region (Economic Commission for Latin America and the Caribbean, 2015; World Bank 2012). In a global study of the world's top 15 countries exposed to three or more hazards, 7 are located in the Latin American and the Caribbean region (Dilley et al., 2005; Kreft et al, 2015). In particular, metropolitan areas in the region are expected to face an increased risk level in the future. A recent report examining economic risks in 300 major cities across the globe noted that 20 % of the top 20 cities at greatest economic risk are in Latin America (Cambridge Centre for Risk Studies, 2015). Four-fifths of Latin America's population lives in metropolitan areas, making it the most urbanised region in the world. Latin America's cities are also among the most unequal in the world, increasing the concentration of poor and hence vulnerable people potentially exposed to natural disasters. In the recent past the region was affected by major floods, such as in Colombia in 2010 and 2011, in Northern Chile in 2015, in Uruguay, Argentina and Brazil in 2016, but also major earthquakes, such as in 2016 in Ecuador(Fermandois, 2011; The Economist, 2011; ERCC,

The Latin America and Caribbean region is particularly exposed to natural hazards including earthquakes, volcanoes, and extreme weather.

1 The authors are grateful for extensive and constructive comments and inputs provided on different versions of this paper by Leigh Wolfrom (OECD, Directorate for Financial Affairs), Jack Radisch and Charles Baubion (OECD, Directorate for Public Governance and Territorial Development) and Sergio Lacambra Ayuso (Intra-American Development Bank). Jack Radisch, Stéphane Jacobzone and John Roche (all OECD) and David Kaufmann (CNA) have provided key guidance on the initial project concept note. The paper also benefited from discussions at the regional policy dialogue organised by the OECD and the Intra-American Development Bank in Panama in October 2016. Teresa Deubelli provided valuable research assistance in the process of revising the document.

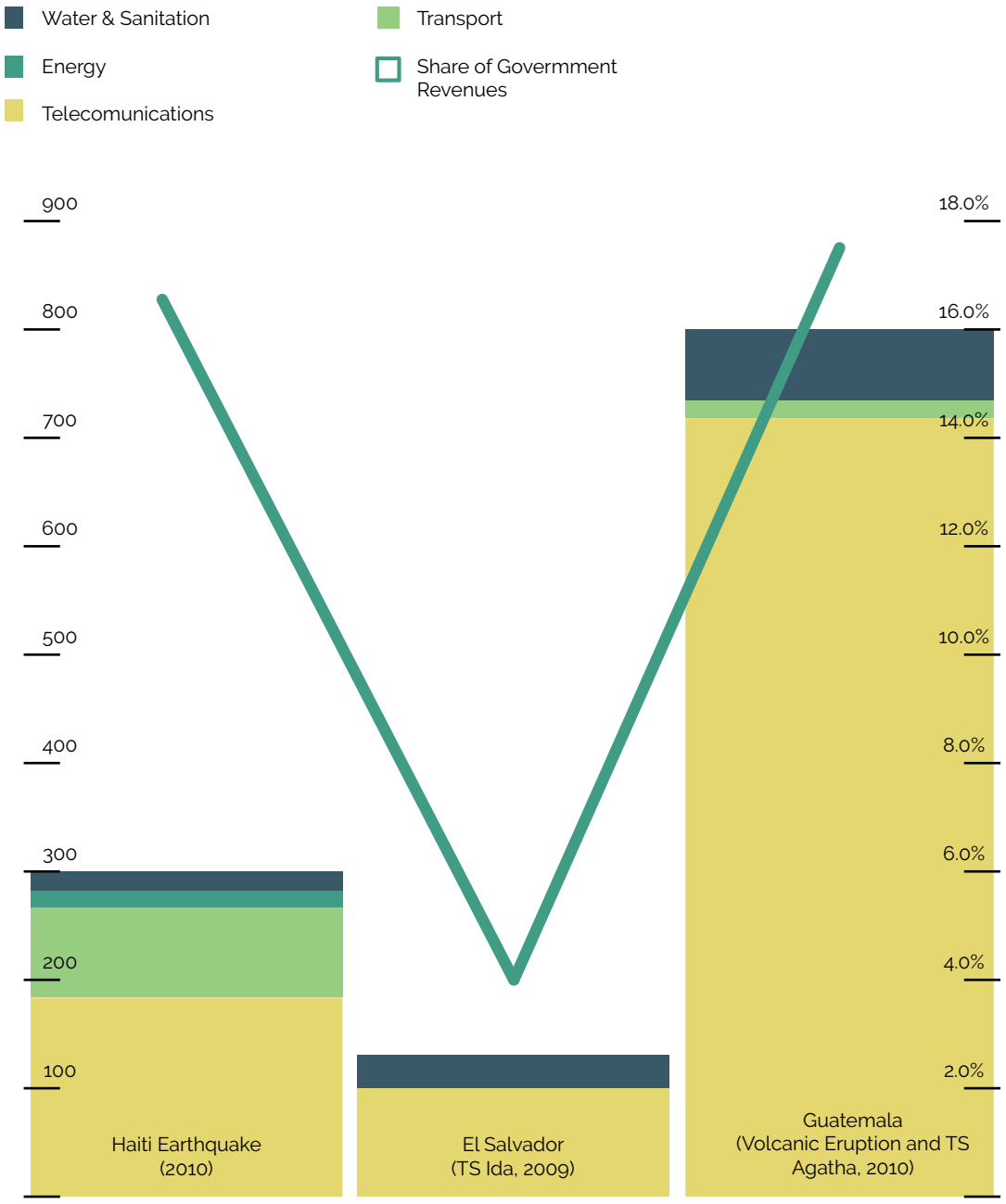
2015; USGS, 2016; Masoero, 2016; Davies, 2016). As infrastructure investments are a key priority to foster economic development in the Latin America and the Caribbean region, building resilience, that is to say the capacity of critical infrastructure to absorb and withstand the negative effects of natural disasters while retaining its pre-disaster functions, into existing and future investments is of key importance (OECD, 2014a; Chang et al., 2013).The region seeks to invest a significant amount of resources to build infrastructure, some of which constitutes critical infrastructure, over the next decades to achieve integration in international global supply chains and boost its productivity. Stable and cost-effective provision of energy and telecommunications has been deemed essential to expand the production possibilities for firms. There is an opportunity for many countries in Latin America to build in resilience in the current rehabilitation and upgrading of existing and the development of future critical infrastructure planning procedures.

Critical infrastructure underpins economies, governments, and societies. The resilience of critical infrastructure not only determines the degree to which countries can be affected by natural hazards, accidents, and intentional attacks, but also preconditions their ability to respond to and recover from these disruptive shocks. If not constructed and managed properly, disruptions to critical infrastructure systems, such as energy, transport, water supply and sanitation and telecommunications, can act as a vector in spreading the negative impacts of disasters. For example, the Great East Japan Earthquake in 2011 caused major interruptions to power supply to an estimated 4.4 million households, and Japan's main rail and boat transport routes were closed for 18 days. Overall the earthquake and its cascading impacts caused some 16,000 casualties and an estimated USD 300 billion in economic damages (OECD, 2014).

Damage to critical systems can cause significant social hardship by disrupting access to basic life lines such as electricity or drinking water, and can produce large economic knock-on impacts by disrupting business for longer periods han the actual disaster event. These functions are fundamental to the overall wellbeing of the populations affected by a significant disaster, and can either bolster, or hinder, their ability to recover.

In the Latin America and Caribbean region, large-scale disasters have revealed significant critical infrastructure vulnerabilities. For example, nearly a quarter of Colombia's highways were damaged, or destroyed, during the 2010 floods and associated landslides (Garcia, 2010). In Chile, the 2010 earthquake and ensuing tsunami led to the collapse of the telecommunication system and hampered the government's means to manage the disaster response. The healthcare and education systems were both significantly impacted with a high number of hospitals damaged and some public schools closed for as many as 45 days. The earthquake and its cascading impacts caused an equivalent of 18% of GDP in economic damages (OECD, 2014a).

Figure 1 Three examples of Estimated public sector damages and losses by infrastructure type



Source: Public share of damages and losses taken from Post-Disaster Needs Assessments completed for each country (Haiti: https://www.gfdrr.org/sites/default/files/GFDRR_Haiti_PDNA_2010_EN.pdf; El Salvador: https://www.gfdrr.org/sites/gfdrr/files/publication/GFDRR_PDNA_ElSalvador.pdf; Guatemala: https://www.gfdrr.org/sites/default/files/Evaluacion_de_danos_y_perdidas_AGATHA_Y_PACAYA_oct_8_2010_reduced.pdf). Government revenues for the year of the disaster, as reported in the IMF's World Economic Outlook 2014, were used to calculate public sector damages and losses as a share of government revenues.

Damage to critical systems can cause significant social hardship by disrupting access to basic life lines such as electricity or drinking water, and can produce large economic knock-on impacts by disrupting business for some time beyond the actual disaster event.

The rebuilding of critical infrastructure after a disaster can also account for a significant share of public reconstruction costs. Infrastructure recovery costs can be large and governments have to shoulder them often times. Figure 1 demonstrates the estimated public sector costs of three major recent disasters in Haiti, El Salvador and Guatemala, as well as the significance of these costs relative to public sector revenues. It also illustrates that the impact of critical infrastructure disruptions depends on the affected sector, with disruptions in transport infrastructure causing the highest costs. A recent study found that a number of countries in the region, including Guatemala, Honduras, Colombia, Mexico and Brazil, could face a sovereign ratings downgrade as a result of 1-in-250 year tropical cyclone or flood event due to the implications for economic growth, government finances, and external trade, with climate change exacerbating the potential impact (Standard & Poor's Ratings Services, 2015).

In the best circumstances, resilient critical infrastructure can resist or absorb the effects of a shock, and rebound in a fashion that enhances the timeliness and efficacy of response activities. However, where critical infrastructure is not able to withstand the impacts of a shock, it can serve as a hazard multiplier, heightening the severity of a shock as cascading impacts within and across sectors contribute additional layers of complexity, and often hamper, or even prevent, the execution of response activities. The public sector plays a crucial role in promoting the resilience of critical infrastructure, e.g. by evaluating risk reduction actions taken by owners/operators of critical infrastructure or by funding activities that enhance critical infrastructure owners' and operators' awareness of risks and resilience measures. Despite progress some countries have made in reducing risks and increasing preparedness, ensuring resilience of critical infrastructure has proven to be a key challenge.

The objective of this report is to develop a policy evaluation framework on the governance of resilient critical infrastructure. Based on a forward-looking analysis of good practices in critical infrastructure resilience, it builds on relevant OECD guidance in this area, including the OECD *Recommendation on the Governance of Critical Risks* (2014b) and the proposed OECD *Recommendation on Disaster Risk Financing Strategies* (*forthcoming*), by providing additional guidance on the application of the principles of effective governance and financial management found therein to managing risks related to critical infrastructure. The identified inform the development of a draft country questionnaire that provides

the basis for a subsequent cross-country comparative analysis of policies and practices in the governance of critical infrastructure resilience across a set of countries in the Latin America and the Caribbean region. Case study findings will be used to inform countries' policies and comprehensive strategies to strengthen resilience of critical infrastructure assets and services.

2. The Critical Infrastructure Resilience Imperative: Lessons From The Past

Much of what constitutes countries' present-day objectives in rendering their critical infrastructure more resilient relies on information obtained during past experiences with infrastructure failures. While a more forward-looking perspective is indispensable in designing risk management strategies, in particular also for critical infrastructure management, the lessons learned provide an informative starting point and can provide the necessary impetus to invest in strengthening their resilience.

The following section will describe examples of past infrastructure failures and lessons learned. It will show that the cascading impacts associated with critical infrastructure failures have often been extensive and unanticipated. The examples shown in this section were chosen to demonstrate different types of infrastructure failures. The first example of Super Storm Sandy in New York describes the case where an extreme weather event led to critical infrastructure failures and cascading impacts in an area that had received considerable support for emergency preparedness and response planning following the terrorist attacks of September 11, 2001. The second example looks at the 2011 Great East Japan Earthquake and its cascading effects of the tsunami and the Fukushima Daiichi Nuclear Power Plant accident, which brought to light the need for an all-hazards approach to critical infrastructure resilience planning. The third example illustrates a major cascading power outage in the Northeast United States and Canada in 2003 illustrating the consequences of deferring critical infrastructure maintenance and the inadequacies of standard redundancy mechanisms. The remaining examples of an earthquake in Peru in 2007 and one in Chile in 2010 demonstrate the knock-on impacts and interconnectedness of lifeline sectors.

2.1 Hurricane Sandy, United States 2011

In late October 2012, Superstorm Sandy struck New Jersey and New York, leaving in its wake roughly $68 billion in damages and major impacts on the energy, transportation, communications, water, and health sectors in the greater New York-New Jersey metropolitan area (Flynn, 2015). An estimated 8.5 million households suffered from electricity shortages and 5.4 million people were affected by the loss of subway services. The damages to transport services alone were estimated at more than USD 10 billion (OECD, 2014a). Following landfall, the interdependencies of the highly networked fuel supply and distribution system and the electric power sector along the East Coast of the United States became evident. Unlike previous fuel supply shocks following hurricanes in the United States, this event primarily affected consumers not producers. Some of the hardest hit areas were already at a disadvantage prior to landfall, as their fuel retail outlets were low on fuel, or had completely exhausted their supplies due to a surge in fuel demand as a result of resident preparations for the storm. After Sandy hit, many of the fuel outlets that had supplies were non-functional, because their pumps lacked power due to electrical outages (NACS, 2013) Meanwhile, retail outlets without fuel supply could not be resupplied, because compressor stations lacked the auxiliary power capabilities necessary to maintain

interstate pipeline operations (NACS, 2013). These interdependencies between the fuel sector and, electric power sector, and the potential for related cascading impacts, were unanticipated..

Lessons Learned

Four key areas have been identified as being responsible for the observed critical infrastructure failures. (Flynn, 2015) First, stakeholders had little understanding of critical infrastructure interdependencies and the potential for cascading impacts associated with system disruptions (e.g., the linkage between the fuel distribution and retail network and the power sector). Second, building standards have not evolved with the development of more modern engineering designs, tools, and practices that are capable of enhancing the resilience of interdependent systems. Critical elements of the transportation system such as tunnels, bridges, rail lines and stations of the New Jersey/New York metropolitan transit services, which serve as the primary means for moving people and goods within the region, are located in low-lying areas and have in many cases not been built to withstand flooding. Third, current organizational management frameworks and regional governance have not been sufficiently designed to address lifeline sector–fuel, electricity, water, transportation, communications and health–interdependencies. For example, healthcare facility evacuation plans prompted the release of all but those patients with the most serious conditions into a community that ultimately did not have power necessary to run medical devices at home or transportation access for caregivers to reach home-bound patients. Fourth there are not enough economic and/or policy incentives for developing resilience and in many cases, institutional and financial disincentives detract from investments in resilience. For example, many public and private operators opt to accept federal financial disaster assistance rather than rely on their own funds to invest in resilience measures. Insufficient regional coordination and collaboration across the New York and New Jersey Metropolitan Areas in managing risks that disasters pose to regional lifeline infrastructures has been another contributing factor that exacerbated disaster impacts (Flynn, 2015).

In recognition of the magnitude of recovery, the President of the United States created the Hurricane Sandy Rebuilding Task Force charged with "identifying and working to remove obstacles to resilient rebuilding while taking into account existing and future risks and promoting the long-term sustainability of communities and ecosystems in the Sandy-affected region" (Hurricane Sandy Rebuilding Task Force, 2013). In its report, the Task Force noted the storm's particularly devastating impact on the region's energy (e.g., extensive power outages and liquid fuel shortages), communications, transportation, water and wastewater management, and healthcare infrastructure and the significant associated delays in response and recovery efforts and losses in economic activity. Based on lessons learned during the recovery process, the Task Force developed a set of 69 recommendations, nearly half of which included a call to develop resilience in the course of the recovery process (Hurricane Sandy Rebuilding Task Force, 2013).

In response to the massive power cut that followed hurricane Sandy in New York and New Jersey the Federal Emergency Management Agency (FEMA) established, at the request of the President, the Energy Resto-

ration Task Force. The Task Force supported a massive private power restoration effort, in which electric utilities executed mutual aid agreements to deploy over 70,000 workers to the affected areas. It enabled air transportation of 229 power-restoration vehicles and 487 personnel to help New York and New Jersey restore power (FEMA, 2013).

2.2 The Great East Japanese Earthquake, 2011

In 2011 an earthquake off the coast of Japan caused significant damage on land and triggered a series of large tsunami waves that severely impacted the north-eastern coast. Inland flooding due to the tsunamis, in turn, set in motion a major nuclear accident at the Fukushima Daiichi nuclear power plant (McGee et al., 2014). Although the Fukushima Daiichi nuclear power station survived the earthquake relatively unscathed and even initiated emergency shutdown procedures appropriately, the design of the site was not adequate to prevent flooding from a tsunami that significantly exceeded site barrier heights. Grid-based electrical power to the area had been knocked offline as result of the earthquake and when the tsunami breeched the site's walls, the subsequent flooding drowned the facility's back-up diesel power generating units and secondary back-up DC batteries (Acton & Hibbs, 2012). Without power, the plant was unable to provide sufficient cooling to three of its reactors which ultimately suffered a level 7 event full meltdown (on an International Nuclear Event scale of 1-7), in excess of even the 1986 Chernobyl disaster (McGee et al., 2014). An estimated 4.4 million households were affected by reduced power supply provided by TEPCO, the Tokyo Electric Power Company. The Shinkansen high-speed rail was closed during two weeks (OECD, 2014a).

Lessons Learned

Post-event analyses revealed that the meltdown was, to some extent, preventable. The incident may have caused fewer impacts had the power plant incorporated the resilience concept into the design . For example, the plant's cooling system was functionally dependent on assured electrical power, and the fire brigade response might have been more timely and reduced the impact if traffic routes were not blocked (Bach et al., 2013). Although the Japanese nuclear industry had the highest nuclear safety standards in the world in terms of seismic risk management, it may have come at the detriment of accounting for a wider range of potential (knock-on) risks. These contributing factors demonstrate the critical role of effective regulators and the need for regular safety reviews that account for and lead to the incorporation of both the dynamic and evolving threat landscape and contemporary best practices (Acton & Hibbs, 2012)..

2.3 Northeast United States And Canadian Power Outage, 2003

On August 14, 2003, a fault due to a high-voltage power line in northern Ohio brushing against overgrown trees led to a system shut down (Minkel, 2008). This occurrence would have normally set off an alarm, but the alarm system failed. As operators attempted to identify the problem, additional lines touched trees and shut down leading

to an overburdening of lines that remained operational. Within two hours of the initial problem, the overloaded lines shut down triggering cascading failures in south-eastern Canada and eight states in the Northeast United States (Minkel, 2008). The outage impacted a range of other critical infrastructure sectors including energy, communications, finance, health care, food, water, transportation, safety, government and manufacturing (Public Safety and Emergency Preparedness Canada, 2006). Ultimately, the blackout impacted 50 million people in both the United States and in Canada at an estimated cost of USD 6 billion (Minkel, 2008)..

Lessons Learned

The 2003 blackout serves as a case study of the challenges associated with varying levels of fragmented control, accountability, and authority for critical infrastructure (U.S.-Canada Power System Outage Task Force, 2004). The official bilateral government report examining the 2003 Northeast Power outage described direct causes and contributing factors of the incident, including: "failure to maintain adequate reactive power support; failure to ensure operation within secure limits; inadequate vegetation management; inadequate operator training; failure to identify emergency conditions and communicate that status to neighbouring systems; and inadequate regional-scale visibility over the bulk power system" (U.S.-Canada Power System Outage Task Force, 2004). The latter resulted in situations where for example in the city of Ottawa the bridges that crossed over to Quebec were half lit because the power was still on in Gatineau, Quebec but there seemed to be no ability to send that power to the side of the province of Ontario.

These findings translated to several notable lessons learned in the form of recommendations. For example, the Task Force asserted that regulators, the electric power industry, and related stakeholders should adhere to high reliability standards, using market mechanisms when and where possible, but always choosing high reliability over commercial objectives should conflicts between the two arise (U.S.-Canada Power System Outage Task Force, 2004). The report went on to emphasize that both regulators and consumers should recognize that reliability requires investment and operational expenditures that businesses will be unwilling to commit to if the costs are not accompanied by assurances from regulators regarding recoverability (U.S.-Canada Power System Outage Task Force, 2004). Prompted by the analysis of the blackout incident, the United States Congress passed the Energy Policy Act of 2005, which enabled the Federal Energy Regulatory Commission (FERC) to enforce new North American Electricity Reliability Corporation standards; five years following the incident, FERC had far approved 96 new reliability standards (Minkel, 2008).

2.4 Pisco Earthquake 2007, Peru

Coastal Peru has been subject to a number of large earthquakes and in August 2007, a Magnitude 8.0 earthquake struck near the town of Pisco (USGS, 2007). As a result of the "Earthquake of the South," the city of Ica and coastal towns south of Lima lost power and telephone service. Damaged highways and bridges, and fallen power lines hindered rescue workers efforts to reach the affected areas. The

healthcare system was heavily impacted with14 facilities destroyed and 112 others affected. Overwhelmed with patients, the Pisco hospital was unable to provide care due to power and water outages. Water service was affected for an average of 16 days in 81 % of households which required the use of water trucks as a main alternative source of supply (World Bank, Water and Sanitation Program, 2011). Some areas in Pisco were still only receiving water one hour per day six weeks post-earthquake which complicated the provision of healthcare services (United Nations Office of the Resident Coordinator, 2007; Chapin et al., 2009). The cost of the repairs to the impacted water and sanitation systems was the cost-equivalent of installing at least 8,183 drinking water and 7,925 wastewater connections benefiting over 160,000 residents. Restoring drinking water and sanitation systems to pre-disaster status required the equivalent of 6.5 times the budget spent for drinking water and sanitation by the provincial municipalities in 2007. If the water and sanitation providers had performed ongoing maintenance, the estimated value of the damage would have been nearly 6 times less (World Bank, Water and Sanitation Program, 2011).

Lessons Learned

The 2007 Earthquake of the South in Peru revealed vulnerabilities related to the interconnectedness of lifeline sectors (water and health, electric power and health). Following the observed complications associated with significant infrastructure damage in the wake of the earthquake, the government enacted a new law (Law N° 29078) to create an autonomous Fund for the Reconstruction of the South (FORSUR) and authorized a supplementary credit of USD 31.6 millions to enable the reconstruction of public infrastructure in the areas affected by the earthquake (Chapin et al., 2009; Taucer et al., 2009). Upscaling this to the national level, the government passed a law (Law N° 29951) providing for the specific allocation of resources to finance risk identification activities for the environment, health, housing, and water and sanitation sectors. The law also validates resources earmarked for financing risk reduction in the agriculture, health, housing, education and transportation sectors. Building on the experience of the 2007 earthquake, the government also restructured the country's emergency management and disaster risk reduction responsibilities to ensure adequate focus and funding for both risk identification and reduction and preparation and response processes (Law N° 29664; IDB, 2015)..

2.5 Chile Earthquake 2010

The 2010 earthquake that occurred on February 27 off the coast of central Chile resulted in USD 30 billion (18 % of GDP) worth of total damages and of that total, USD 20.9 billion (12.7 % of GDP) was due to infrastructure damage. The earthquake affected a region comprising 30-40 % of national manufacturing capacity. Almost all commercial activity was suspended in this area for a few days and while most industries were able to restart production, some major industries, in particular relating to pulp paper production, wine making and oil refining had no, or significantly reduced, commercial activity for months. The total decline in national economic activity in

March 2010 was assessed at 5 %. Economic disruption continued over the next three months, finally returning to pre-disaster levels by July 2010 (Muir-Wood, 2011). The earthquake's impacts could have been far worse if not for deliberate planning in the energy sector and strong building codes designed around seismic risk (Fermandois, 2011).

Lessons Learned

Reflecting on the impacts of 2010 earthquake, the Chilean Government took actions to address observed vulnerabilities. At the operational level, the Chilean government committed to resolve the communications outages and monitoring outages that occurred in 2010 with investments in real-time monitoring processes and robust telecommunications systems complete with redundancies (Fermandois, 2011). The Chilean Insurance Industry Association (AACH) has been developing a map to identify all risk areas susceptible to earthquakes and tsunamis within the economy. This map is expected to be a publicly-available tool that will contribute to future methodologies for disaster risk management. The AACH is also developing an earthquake and tsunami risk model, in co-operation with the Insurance Regulatory and Supervisory Authority that will be shared with government authorities for their use in risk assessment and when developing policies for public and private infrastructure investment (OECD, 2015a). Despite good building codes, the loss in housing and infrastructure was extensive, with much of it not covered by hazard insurance. To enable swift recovery of housing and infrastructure, the government took a proactive stance, raising taxes to fund recovery costs and speedily implementing a housing recovery program (Comerio, 2013).

2.6 Conclusions

Disaster incidents lay bare the complexities and vulnerabilities of interdependent critical infrastructure systems. Past major incidents offer insight into the range of potential consequences and policy lessons. In many cases incentive structures, such as very likely or guaranteed government assistance in the aftermath of a disaster, may have hindered higher *ex ante* investments in resilience measures. At the same time, operators of critical infrastructure may not comply with resilience regulations if they do not have the assurance that they will be able to recuperate the costs of such investments. Governments should thus consider removing disincentives that undermine and instead creating an incentive structure that encourages *ex ante* investments. Governance arrangements can play a critical role in boosting resilience, too. A failure in aligning control, accountability and authority can lead to an underinvestment in resilience by operators of critical infrastructure. The Great East Japan Earthquake, for example, has demonstrated the need for giving regulatory oversight bodies the necessary independence to enforce and monitor the uptake of resilience regulations. Making effective governance arrangements work is even more challenging when the impacts of a disaster crosses country borders, as was the case during the 2003 blackout in Canada and the United States. To manage risks to transboundary lifeline infrastructures, governments should consider establishing in-

ter-regional and transboundary coordination and collaboration mechanisms.

The lessons from previous disasters show that governments and stakeholders need to move from identifying singular risks to considering the interdependencies in critical infrastructure systems to better understand the potential cascading impacts. To mitigate cascading effects, existing building codes, standards, and guidance for the interdependent sectors should be updated to reflect that the vulnerability to one could disrupt several or all dependent sectors. The 2010 earthquake in Chile, for example, showed that although building codes and standards alone cannot prevent damages, they can significantly limit the potential impacts of a disaster.

3. The Implementation Of Meaningful Investments In The Operational And Financial Resilience Of Critical Infrastructure Can However Only Occur If There Is A Comprehensive And Coordinated Risk-Based Framework Guiding The Incorporation Of Lessons Learned In Public And Private-Sector Actions And Investments Intended To Enhance Critical Infrastructure Systems' Ability To Prepare For, Absorb, Adapt To, And Recover From Disruptions. The Evolving Role Of Resilience

3.1 From Critical Infrastructure Protection To Resilience

Governments have dedicated specific attention to the importance of, and vulnerabilities associated with, critical infrastructure for decades. Until the mid-2000s, most critical infrastructure policies and activities centred on the protection of assets. Given the rising costs of natural disasters as

well as following the September 11 attacks in 2001 in the United States, the 2002 Bali and the 2005 London bombings and the increasingly frequent cyber-attacks targeting critical infrastructures governments began to shift the focus from critical infrastructure protection to critical infrastructure resilience (Critical Five, 2014). Resilience in this context can be defined as the capacity of critical infrastructure to absorb disturbance while still retaining essentially the same function as prior to the disruptive shock (OECD, 2014a; Chang et al., 2013). An extension of this definition is described by Barami (2013), who emphasizes the complex and multi-faceted nature of critical infrastructure resilience. Barami applies a risk-based and layered approach accounting for complex infrastructures interdependencies; while considering potential solutions applicable through the infrastructure system lifecycle (i.e., design, construction, and operation). Resilience is therefore defined not as a single outcome or an exclusively post-disaster recovery capability but rather as a dynamic process that applies a risk- and lifecycle-based method for addressing the vulnerabilities of critical infrastructure systems, making systems more fault-tolerant, more efficient, smarter, and better able to adapt to unexpected challenges (Barami, 2013).

Under the critical infrastructure protection paradigm, stakeholders viewed critical infrastructure risk management from a predominately asset-based perspective with a focus on security and physical measures as the means for preventing critical infrastructure disruptions altogether. The shift toward a resilience-based perspective was prompted, at least in part, by the recognition of the considerable degree of uncertainty about the intensity and the complexity of future disasters, with climate change being one of the influencing factors. The nature of such unpredictable scales of disasters requires incremental approaches that cannot eliminate or even sufficiently predict the impacts of disasters, but that can prepare assets and systems with capacities to be restored and rehabilitated swiftly. For example, the critical infrastructure impacts of an incident such as Hurricane Sandy in an area that had received considerable funding and had engaged in substantial protection activities following the attacks of 11 September 2001 demonstrated that protective activities alone would not be sufficient to address the range of potential critical infrastructure impacts and associated interdependent risks. Furthermore, the extent of activities and measures required to fully protect critical infrastructure from all hazards is cost prohibitive and it therefore became desirable to promote the ability of critical infrastructure to adapt, absorb, and even fail safely.

The resilience focus does not preclude protection, or security considerations. It rather broadens the lens of critical infrastructure frameworks to include preventive actions that address all hazards, run throughout the risk management cycle (Moteff, 2012), and provides for integrating concepts such as adaptability, flexibility and robustness (Flynn, 2008; Barami, 2013). The resilience focus also includes measures that enable financial resilience, i.e. having the capacity and resources to absorb and recover from disaster losses without significant financial distress (G20/OECD, 2012). This can be accomplished by ensuring that the owners and operators of critical infrastructure, whether national, sub-national or private, have appropriate financial arrangements in place to mitigate their exposure to

disaster risks. Available approaches include transferring disaster risks through disaster insurance mechanisms or dedicated funds to cover recovery costs (G20/OECD, 2012). Public-private partnerships and public subsidies can be useful to unlock additional funding for investments in structural measures and their maintenance, which in the long run enables a more cost-effective approach to resilience than *ex post* financing (Barami, 2013; OECD, 2016).

3.2 Governance Challenges To Critical Infrastructure Resilience

There are many challenges that arise in making critical infrastructure resilient, which stem from the variety of actors involved who are driven by different objectives and incentives:

- Critical infrastructure owners and operators may underinvest in resilience compared to what would be socially optimal. Primarily concerned with their organisation's interests, operators of critical infrastructure might not be considering the risk and associated cascading costs for society that a disruption of their services may cause. Limited direct experience with disasters causing disruption in critical infrastructure and major spill-over effects may also contribute to this. Without legal requirements and targeted risk communication, providers may have little incentive to go beyond avoiding or mitigating physical damage to their own systems. In many cases the legal liability for disruption in critical infrastructure is with the dependent service providers rather than with the critical infrastructure operators themselves (e.g. when a power outage in a building results in accidents, which would be the liability of the building owner) (Chang et al., 2013).
- Underinvestment in resilience might also be due to an overreliance on governments as a financier of last resort. If there is a track record of post disaster financial assistance for rehabilitating and reconstructing public infrastructure, there may not be sufficient incentives for investing in resilience measures *ex ante* of disasters, independently of infrastructure being publicly or privately owned. Critical infrastructure operators, particularly those from the private sector, may have a strong interest to maximize efficiency and profit. do so
- Owners and operators of critical infrastructure might follow organisational, rather than regional or national interests, which may result in sub-optimal provision of resilience measures. Examples are dams along a river, which might be built by the operators of a hydropower plant, but that could also protect other critical infrastructure downstream, if constructed accordingly. Dam operators may only be willing to put resilience measures in place that protect downstream operators of other critical infrastructure, if costs for them are shared by everyone. If the collective action problem is left unaddressed, upstream operators might ignore the needs

of downstream infrastructure and forgo the option of putting in place resilience at optimal cost levels. Governments are not always in a position to make public and private sector critical infrastructure operators put resilience measures in place. , for example,appropriate ,as the definition of resilience targets may be too the design of standards sEnergy operators might for example require different resilience measures than transportation or telecommunication operators, even when facing the same hazards. Owing to the complexity and diversity in appropriate resilience measures governments oftencontinuously monitor the implementation of legally required resilience measures In addition, legal requirements for the implementation of resilience measures may create problems of competition and unwillingness for those operators required to implement them. Aside from the circumstance that some operators might lack the necessary funding to cover the costs of such measures, this requirement creates a competitive advantage for those operators that do not have to make these investments.

To design and set up adequate policies it is key to identify the respective bottlenecks and challenges. At the same time, it is important to consider all possible consequences of the policies and regulations choices made to boost critical infrastructure resilience. For example, if policy-makers create an environment that provides incentives to merely restore infrastructure to its previous condition following a disaster thereby forgoing a natural opportunity to "build back better," then infrastructure operators will likely respond in an equivalent manner, unless there is a separate recognized business case for improvement. As with any business, critical infrastructure owners and operators make trade-offs based on known risks and choose economically rational investments relative to competitive market dynamics and resource constraints Businesses may also shy away from collaborative efforts to build resilience due to the risk of divulging information on their vulnerability, which might have an impact on their market value, or on their resilience investments (OECD, 2015a). Finally, resilience may also be undermined by a fragmented and incomplete understanding of the potential problems and the potential solutions. Ensuring precision in the identification and framing of problems requires stakeholders to possess an in-depth understanding of the environment.

Based on the above the discussion of the concept of resilience in critical infrastructure a policy evaluation framework will be presented. The framework will spell out key criteria, including on governance and financial arrangements that can inform the evaluation of the level of resilience of countries' critical infrastructure. In subsequent work this framework, and the questionnaire in the Annex, should inform country case studies as well as cross-country analysis whose results will be translated to broad policy recommendations to inform countries' work going forward.

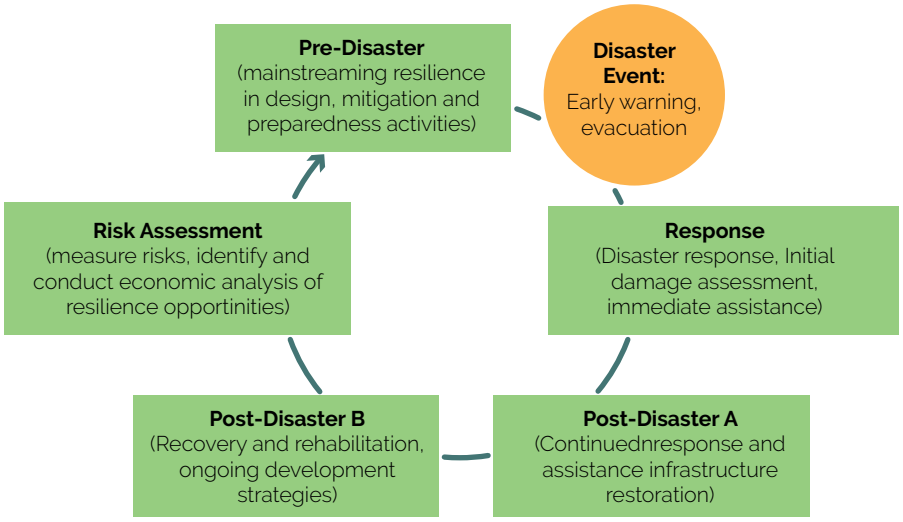
4. Overcoming Challenges And Increasing Critical Infrastructure Resilience: A Draft Policy Framework

Achieving critical infrastructure resilience requires adherence to a critical infrastructure risk management process that complements activities within the broader disaster risk management cycle. The majority of critical infrastructure resilience planning activities occur during the risk assessment and pre-disaster phases of the disaster risk management cycle (see figure 2, below), while the management of resilience in critical infrastructure focuses on activities in all phases of the risk management cycle, such as in the aftermath of a disaster, when damaged infrastructure is built back better.

Countries intent on engaging in critical infrastructure resilience planning and management activities should develop commonly agreed assessment and evaluation guidelines as well as governance arrangements. It is equally important for countries to identify funding mechanisms that can be used to support initial and ongoing critical infrastructure resilience efforts. In the following a policy evaluation framework will be provided that will subsequently inform country case study questionnaires:

- Definition of critical infrastructure
- Criticality assessment
- Risk, vulnerability and interdependency assessments
- Governance arrangements
- Policy instruments (eg regulations, incentives or voluntary mechanisms)
- Development of national critical infrastructure resilience strategies
- Critical infrastructure financing

Figure 2. disaster risk management cycle



Source: adapted from OECD (2014a)

- Monitoring and evaluation
- The use of exercise and post-event lessons learned

4.1 Definition Of Critical Infrastructure

The definition of critical infrastructures should not be a one-off exercise, potentially revised every so often. Rather, the definition of critical infrastructure is subject to dynamic national and international trends, such as an increasing reliance on information technology, as well as influenced by the political situation and by contemporary threats and disaster events. The ongoing process of defining critical infrastructure is dependent on continued stakeholder discussions (stangl et al., 2012). In this context it is important that the resulting definition of critical infrastructure allows resilience investments to be targeted to the sectors that are most crucial to societal and economic security and stability (clancy, 2012).

The approaches for defining critical infrastructure differ across countries (table 2), although they share common themes. "Critical" functions are those that are essential for social and economic well-being in general and to public safety and security more specifically. Most of the country definitions also recognize the interdependence of systems and make specific reference to physical infrastructure, production systems or communications networks (gordon and dion, 2008). Table 2 provides the definition of critical infrastructure across six oecd countries, namely australia, canada, germany, new zealand, the united kingdom, and the united states.

In a shared narrative report seeking to develop a common understanding of critical infrastructure, australia, canada, new zealand, the united kingdom, and the united states proposed the following shared definition of critical infrastructure: critical infrastructure, also referred to as nationally significant infrastructure, can be broadly defined as the systems, assets, facilities and networks that provide essential services and are necessary for the national security, economic security, prosperity, and health and safety of their respective nations (critical five, 2014).

Table 2. National Critical Infrastructure Definition

AUSTRALIA	"Those physical facilities, supply chains, information technologies and communication networks which, if destroyed, degraded or rendered unavailable for an extended period, would significantly impact the social or economic wellbeing of the nation or affect Australia's ability to conduct national defence and ensure national security."
CANADA	"Critical infrastructure refers to processes, systems, facilities, technologies, networks, assets and services essential to the health, safety, security or economic well-being of Canadians and the effective functioning of government. Critical infrastructure can be stand-alone or interconnected and interdependent within and across provinces, territories and national borders. Disruptions of critical infrastructure could result in catastrophic loss of life, adverse economic effects, and significant harm to public confidence."
GERMANY	"Critical infrastructures (CI) are organizational and physical structures and facilities of such vital importance to a nation's society and economy that their failure or degradation would result in sustained supply shortages, significant disruption of public safety and security, or other dramatic consequences."
NEW ZEALAND	"Critical infrastructure is that infrastructure necessary to provide critical services, whose interruption would have a serious adverse effect on New Zealand as a whole or on a large proportion of the population, and which would require immediate reinstatement. New Zealand's critical infrastructure has been identified as those assets and systems required for the maintenance of: governance including law and order and national and economic security; telecommunications and the Internet; energy including electricity generation and distribution, and the distribution of oil and gas; finance and banking; transport; emergency services."
SWEDEN	"Those assets, systems or parts thereof located in the EU Member States which are essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions."
UNITED KINGDOM	"Those infrastructure assets (physical or electronic) that are vital to the continued delivery and integrity of the essential services upon which the UK relies, the loss or compromise of which would lead to severe economic or social consequences or to loss of life."
UNITED STATES	"Critical infrastructure represents systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."

Sources: (Australia) Critical Infrastructure Resilience Strategy (2010) and Critical Infrastructure Resilience Strategy: Plan (2015); (Canada) National Strategy for Critical Infrastructure (2009) and Action Plan for Critical Infrastructure 2014-2017; (Germany) National Strategy for Critical Infrastructure Protection (2009); (New Zealand) Presentation at the International Disaster and Risk Conference, Davos, 28 August 2008. Critical Infrastructure Resilience: Perspective from New Zealand. Patrick Helm, Department of the Prime Minister & Cabinet, New Zealand; (Sweden) Action Plan for the Protection of Vital Societal Functions & Critical Infrastructure (2014); (United Kingdom) Strategic Framework and Policy Statement on Improving the Resilience of Critical Infrastructure to Disruption from Natural Hazards (2010) and Keeping the Country Running: Natural Hazards and Infrastructure (2011); (United States) The National Infrastructure Protection Plan 2013 Partnering for Critical Infrastructure Security and Resilience; OECD (2015b). Establishing effective Public –Private Partnerships for risk management. What are the possible options for government? OECD High Level Risk Forum, December 2015.

Table 3. Critical Infrastructure Sector and Sub-Sector examples

Expamples	Australia	Canada	France	Germany	The Netherland	New Zealand	Switzer-land	United Kingdom	United States
ENERGY	●	●	●	●	●	●	●	●	●
FOOD (& AGRICULTURE)	●	●	●	●	●		●	●	●
Water (& Wastewater)	●	●	●	●	●	●	●	●	●
Transportation	●	●	●	●	●	●	●	●	●
Health	●	●	●	●	●		●	●	●
Banking & Finance	●	●	●	●	●		●	●	●
Communication	●	●				●		●	●
Government		●	●	●	●		●	●	●
Manufacturing & Industry		●	●	●	● [1]		●		● [2]
Safety		●							
Social Infrastructure						●			
Laboratories	●								
Chemical	●								●
Defense	●		●						●
Commercial Facilities									●
Dams					●				●
ICT	●	●	●	●	●		●	●	●
Nuclear									●
Emergency Services	●	●	●	●	●		●	●	●
Law Enforcement			●	●	●				

Notes: 1) Chemical and nuclear industries 2) Critical manufacturing, nuclear reactors, materials, waste, chemical industry
Source: Critical Five (2014). Forging a Common Understanding for Critical Infrastructure; OECD (2015b).

In the latin america and caribbean region, a recent report on the results of the inter-american development bank's index of governance and public policy in disaster management (igopp) revealed that 14 out of 17 countries surveyed have defined critical infrastructure in their respective legal frameworks. In mexico, for example, strategic infrastructure is defined as infrastructure that is indispensable for the provision of public goods and services and whose destruction or disruption is a threat to national security. While chile has developed a classification of structures including a category for buildings and other structures (e.G. Hospitals, fire stations) that are essential in the context of a disaster (idb, 2015).

In terms of sectors that provide critical infrastructure, at the most basic level, these include lifeline systems such as water, wastewater, power, transportation, and telecommunications systems that enable the intended functions of the built environment, emergency response systems, and other infrastructure (nrc, 2009). In many oecd countries the lifeline sectors also include finance, health and food. As the definition of critical infrastructure, the exact sectors and sub-sectors that it comprises varied across countries (table 3).

4.2 Criticality Assessment

Based on the definition of critical infrastructure, criticality assessments should be conducted to identify assets, systems, and networks that are truly critical (dhs, 2013; zaballos and juen, 2016). Criticality may be viewed differently across levels of government and private sector owners and operators, thus it is important to communicate criticality perspectives via structured information-sharing activities throughout the critical infrastructure risk management process and to develop lists of infrastructure that is critical at various jurisdictional levels (dhs, 2013). Figure 4 illustrates a criticality hierarchy used by the state of victoria in australia.

Criticality assessments are predicated on the linkages between risks and impacts. Commonly used approaches to assess criticality in the context of impacts focus on incident consequences such as the incidence of injuries or losses (theoharidou et al., 2009). Impact is usually evaluated with respect to three primary characteristics:

I. Scope or spatial distribution – the geographic area that could be affected by the loss or unavailability of a critical infrastructure;

II. Severity or intensity or magnitude – the consequences of the disruption or destruction of a particular critical infrastructure; and

III. Effects of time or temporal distribution – the point that the loss of an element could have a serious impact (immediate, one to two days, one week, etc.).

For example, the european commission defines a minimum set of criteria for critical infrastructure assessments, including:

I. Public impacts, including the population affected and incidences of loss of life, medical illness, serious injury, and evacuation;

II. Economic impacts, including gdp effect, economic loss, and degradation of products or services;

III. Environmental impacts, including the effect on the public and the surrounding environment;

IV. Interdependence, namely the interdependencies between critical infrastructure elements;

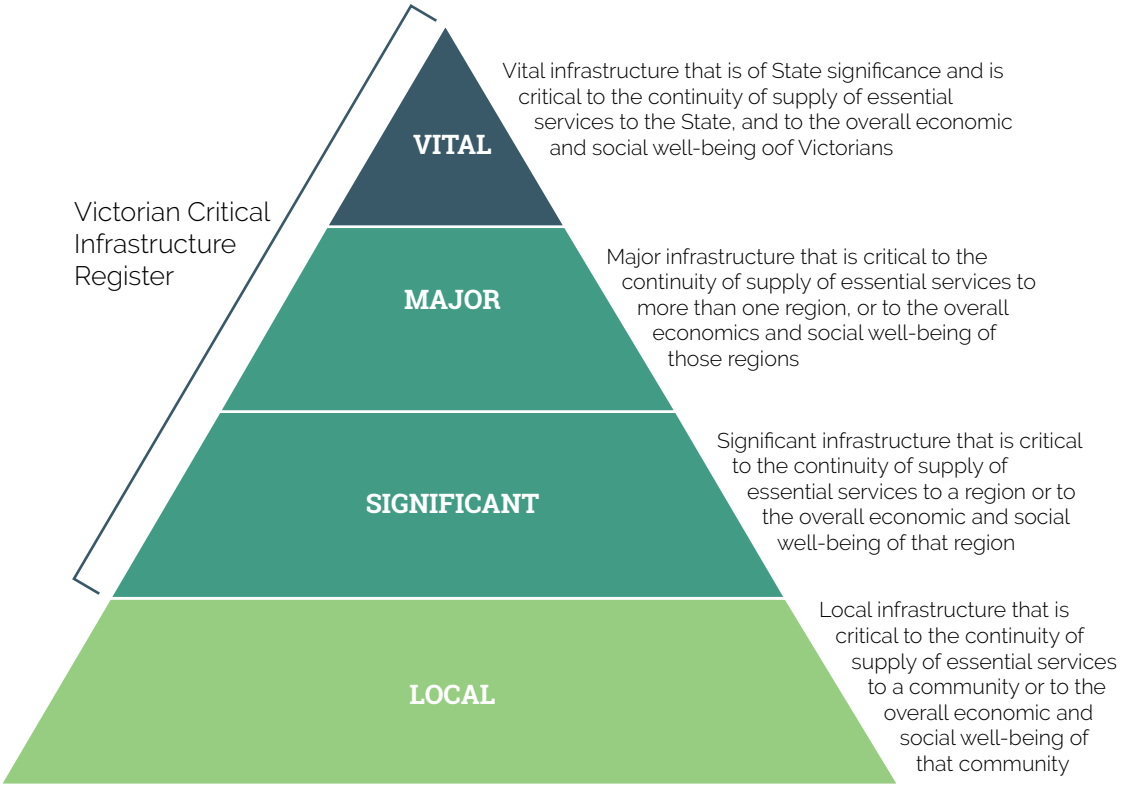
V. Political impacts, including confidence in the government; and

VI. Psychological impacts, including observed psychological effects on the population (theoharidou et al., 2009).

Similar to criteria outlined above, the european commission assess these criteria on the basis of scope (local, regional, national and international) and timing (during and following the event) (theoharidou et al,. 2009).

Source: Victoria, Australia State Government (December, 2012). A Roadmap for Victorian Critical Infrastructure Resilience.

Figure 4. Example of Infrastructure Criticality Hierarchy: The Case of Victoria, Australia



4.3 Risk, Vulnerability, And Interdependency Assessments

4.3.1 Understanding Risks And Vulnerabilities

Risk and vulnerability assessments identify relative risks and vulnerabilities faced by critical infrastructure and assess the impact and consequences, as well as the likelihood of a hazardous event. They inform public and private decision-makers about the level of security and the need for resilience investments and can increase support for investments in resilience measures, as well as for extraordinary measures during times of crisis (critical five, 2014; dhs, 2013; oecd, 2014a; zaballos & juen, 2016; oecd (*forthcoming*)). These assessments serve to identify applicable resilience measures for more robust and resilient critical infrastructure systems. Examples of available measures include hardening and reconfiguration, e.G. Through the elevation of assets at risk from flooding, dry and wet proofing, or removing physical impediments that restrict water flow in rivers and floodplains, and elevating equipment and generators and redundancy (e.G. Through power generation back up capabilities), enhanced monitoring, and risk-appropriate emergency response plans. Beyond enabling the selection of appropriate resilience measures, risk and vulnerability assessments help to integrate resilience efforts into the broader infrastructure life-cycle.

Given the diverse risk profile of critical infrastructure risk and vulnerability assessments need to consider the full range of natural and man-made hazards, including terrorist and cyber-attacks, as well as human and technical errors, and their underlying driving forces. Comprehensive risk and vulnerability assessments not only consider the most likely scenarios, but also take risk scenarios into account that are less probable, but might nonetheless materialize. Taking a holistic, all-hazards approach can help in uncovering complex vulnerabilities and identify interdependencies across sectors and risks (g20/oecd, 2012; oecd (*forthcoming*)). An increasing number of countries recognises the need to take the full range of potential disaster events into account (oecd (*forthcoming*). Germany's national strategy for critical infrastructure protection, for example, considers a wide range of possible threats including natural hazards, technical failures or human errors (such as system failure, negligence accidents or organizational failures) and terrorism, crime and conflict, which includes sabotage; other forms of criminal behaviour (e.G., Cyber hacking and cyber-attacks); and civil war, or war (federal republic of germany, 2009). Canada's national strategy for critical infrastructure equally stresses the need for an all hazards risk analyses that takes accidental, intentional and natural hazards into account (canadian government, 2009).

Risk assessments can be performed using a variety of methodologies, ranging from deterministic approaches to probabilistic methods. Deterministic approaches analyses and interprets historical disaster events and available retrospective data in light of new developments, such as climate change and technological advances, which may influence and change their shape and impact. Disaster scenarios and simulations may expand the retrospective analyses. To refine the estimates made through deterministic analyses, risk assessments for critical infrastructure should be expanded by probabilistic calculations (g20/oecd, 2012; oecd (*forthcoming*)). In light of risk patterns that are evolving

in the face of socio-economic changes, environmental dynamics and technological advances, risk and vulnerability assessments need to be carried out regularly and methods need to be adapted over time (oecd, 2014a; g20/oecd, 2012; oecd(*forthcoming*)). Risk assessments for critical infrastructure should for example consider that deliberate human acts, such as terrorist attacks, may be committed by attackers that adapt in accordance to preventive measures, reducing the reliability of probabilistic calculations for deliberate scenarios (brown and cox, 2011). In addition, data availability and quality shape risk, vulnerability, and interdependency assessment capabilities. Box 1 provides examples of critical infrastructure risk assessment employed in europe and the united states.

Across countries, critical infrastructure risk assessments differ in scope and focus (asset level, system or sector level) and according to the intended audience (policy makers, operators) (european commission, 2012; oecd, (*forthcoming*)). The majority of risk assessments focus on the sector or asset level, while cross-sectoral, or systems of systems risk assessments are less used (european commission, 2012). In light of complex risks arising from vulnerabilities and interdependencies across critical infrastructure sectors, this could prove a critical shortcoming (giannopoulos et al., 2012).

The focus of risk assessment correlates closely with the intended audience. While risk assessments at national level are mainly addressed to policy makers and useful for identifying key risks and vulnerabilities and corresponding counter measures, critical infrastructure operators may see more relevance in sector-specific risk assessments. Although national risk assessments are less granulated and predominantly rely

Box 1. Critical Infrastructure Risk Assessment Methodologies in Europe and North America

- **Cluster of User Networks in Transport and Energy relating to Anti-terrorist Activities (COUNTERACT).** COUNTERACT is similar to an organizational risk assessment methodology with a relatively narrowed focus on the transportation and energy sectors and terrorist threats. Applying a security risk assessment framework that is disaggregated into risk analysis and vulnerability assessment, the tool can identify gaps in threat prevention and mitigation and detect the possibility of optimizing the safeguards that are present.

- **Integrated approach for Critical Infrastructure Protection.** The Dutch National Safety and Security Strategy introduces a three step methodology for risk assessment in the context of critical infrastructure. Building on the National Risk Assessment process, economic, physical and social impact criteria determine the degree of criticality of infrastructure and the impact disruptions may have. A vulnerability assessment provides insight into the most important risks, threats, vulnerabilities and degree of resilience of this infrastructure. Finally, the approach foresees agreements on maintaining or, where needed, increasing the resilience of the vital infrastructure.

- **Critical Infrastructures and Systems Risk and Resilience Assessment Methodology (CRISRRAM).** CRISRRAM is a methodology developed by the European Commission. It takes an all-hazards and systems of systems approach, addressing risks and vulnerabilities of critical infrastructure at asset level, system level and society level. To tackle the complexity of risk assessments, CRISRRAM takes a scenario-based approach and recommends the assessment of all relevant single- and multi-hazard scenarios. To select the appropriate scenarios, Threat Likelihood Assessments should be done.

- **RAMCAP-Plus.** The RAMCAP-Plus methodology was developed by the American Society of Civil Engineers as an all-hazards risk and resilience assessment approach. It encompasses all infrastructures factoring in the dual objectives of protection and resilience. The seven steps in the methodology are: asset characterization; threat characterization; consequence analysis; vulnerability analysis; threat assessment; risk and resilience assessment; and risks and resilience management. The tool has been designed for use by critical infrastructure operators and decision-makers alike.

Source: Giannopoulos, Filippini & Schimmer., 2012; Theocharidous and Giannopoulos, 2015; OECD, 2017

Box 2. HAZUR: Understanding Critical Infrastructure Interdependencies in Cities

Following a drought, challenges with high-speed rail construction, and a significant power outage in 2007, the Barcelona City Council collaborated with IQS, a university research centre, to start the '3S - Security of Services Supply' Project. The '3S' Project aimed at identifying the weak points and risks faced by critical infrastructure in the Barcelona metropolitan area and improved operational plans to facilitate the continuity of services in the city under all hazards.

Building on the '3S' Project, the private spin-off 'OPTICITS' upscaled the project's approach into a tool that can contribute to enabling the resilience of critical infrastructure in other cities. OPTICITS developed the HAZUR methodology and online software-based platform to carry out assessments of city resilience and the redundancy of infrastructure networks and provide a mechanism for actively monitoring city resilience. HAZUR factors interdependencies and incorporates information reported by citizens, transmitted by private sector operators, and recorded through a network of sensors. The software also maps the operative status of infrastructure and their interdependences and provides swift oversight of interruptions. The software can also be used to model the impact a hazard may have on a city's network of critical infrastructure.

In addition to the HAZUR software, OPTICITS also developed a Certification Programme in urban resilience, accompanied by a network of Certified Urban Resilience Experts.

Sources: HAZUR. Introduction to Urban Resilience with HAZUR online course. Retrieved from: https://learn.canvas.net/courses/921/pages/4-dot-3-study-cases-barcelona; HAZUR Resilient Systems homepage. Retrieved from: http://opticits.com/ Ajuntament de Barcelona. http://resilient-cities.iclei.org/fileadmin/sites/resilient-cities/files/Resilient_Cities_2012/Program_Updates/Presentation/F/F3/Manuel_Valdes_response_to_crises_in_infrastructures.pdf

on deterministic assessments, they provide a valuable context for sector-specific risk assessments. In the united kingdom, for example, annual detailed, scenario-based national-level risk assessments serve as the foundation of infrastructure sector resilience plans (zaballos & juen, 2016). Other countries, such as finland, run critical infrastructure risk and vulnerability assessments as part of their national risk assessments and consider both cascading effects and cross-border interdependencies and critical infrastructure specific risks (european commission, 2012; oecd (*forthcoming*).

4.3.2 Understanding Interdependencies And Cascading Impacts

The unprecedented degree of interdependency and interconnectedness across critical infrastructure systems has increased the prevalence of potential vulnerabilities and in particular, the prospective for cascading events (gordon & dion, 2008; u.S. Department of homeland security, 2013). Cascading effects are observed when a disruption in one, or more, infrastructure systems gives rise to subsequent disruptions within systems and processes with linkages to the initially affected system(s) (gordon and dion, 2008). More recently, the marked application of information systems and communications technologies has greatly improved efficiency while at the same time subjecting critical infrastructure to new potential sources of disruption tied to the potential compromise of underlying systems or networks (u.S. Department of homeland security, 2013). There is a need to dynamically identify critical infrastructure interdependencies to avoid developing narrowly focused solutions that may give rise to se-

vere, unintended consequences (nrc, 2009). The hazur methodology described in box 2 provides a practical example of how critical infrastructure interdependencies can be identified and mapped.

Interdependency assessments help identify and raise awareness among stakeholders about possible linkages and cascading impacts within and among critical infrastructure sectors. Such assessments allow for the development of processes and the implementation of technological failsafe mechanisms to mitigate potential cascading effects. Interdependency assessments may lead to the classification of additional critical infrastructure in instances where the critical importance of a specific infrastructure in a network context is revealed.

Critical infrastructure interdependencies could take the following forms (rinaldi et al. 2001; Macaulay, 2016):

- Physical: two infrastructures are physically interdependent if the state of each is dependent on the material output(s) of the other;
- Cyber: an infrastructure has a cyber-interdependency if its state depends on information transmitted through the information infrastructure;
- Geographic: infrastructures are geographically interdependent if a local environmental event can create state changes in all of them;
- Logical: two infrastructures are logically interdependent if the state of each depends on the state of the other via a mechanism that is not a physical, cyber, or geographic connection.

Box 3 provides examples of contemporary critical infrastructure independency assessment approaches in the united states.

Box 3. Interdependency Assessment Approaches in the United States of America

- **Criticality Accessibility Recoverability Vulnerability Espyability Redundancy (CARVER2).** CARVER2 is designed to provide critical infrastructure analysis from a policy maker's perspective. It employs an all-hazards approach, covering both terrorist threats and natural disasters, and allows users to compare and rank critical infrastructure within and across sectors. Critical infrastructure is assessed according to six criteria, with impact assessment at the heart of the assessment. To implement the methodology a stand-alone PC tool and a server/client version (CARVER2Web) have been created.

- **Critical Infrastructure Modelling Simulation (CIMS).** Used by Idaho National Laboratory, the CIMS approach was developed policy and decision makers at the city or county level to enable swift decision making and emergency response in the recovery phase. It provides visualization of infrastructure interoperability and can develop models in real time using open source information (e.g. simple maps or aerial photos combined with information at a high level of aggregation). CIMS is inherently cross-sectoral given its focused on interdependencies, albeit at a high level of abstraction, and should be viewed as an interdependency and impact assessment tool with a focus on societal resilience.

Source: Giannopoulos, Filippini & Schimmer, 2012

Risk, vulnerability, and interdependency assessments serve as the foundation of effective critical infrastructure resilience strategies and implementation plans. Through these assessments, policy makers and operators alike are able to efficiently shape national, sub-national, sectoral, and cross-sectoral approaches to bolster the resilience of critical infrastructure based on identified risks, vulnerabilities, and interdependencies. Armed with an understanding of these factors, critical infrastructure stakeholders can develop resilience objectives that address threat probabilities and potential impacts, prioritizing those that are most important to their particular context.

Risk, vulnerability and interdependency assessments that provide a quantification of potential exposure to disaster risks are a critical for future assessments of the relative costs and benefits of particular investments in resilience as well as for determining whether to transfer some exposure to insurance and/or capital markets. Formal catastrophe modelling approaches, which take into account hazard, (structural) vulnerability and financial impact, can provide the estimates of average annual loss and probable maximum loss necessary for effective financial management of disaster risks.

4.4 Governance Arrangements

Critical infrastructure ownership and operation models vary across countries. In some countries, most critical infrastructure is owned and operated by national or sub-national level governments, or other public agencies and authorities with responsibility for the assets, systems, and the services they provide. In others, an increasing share of critical infrastructure is also either privately owned or operated. Public-private partnerships (ppp's) have also become an increasingly frequently used instrument to operate infrastructure assets. In chile and mexico, for example, 20% of public sector infrastructure investment takes place through ppp's (hawkesworth, 2011; oecd, 2015c).

Independent of the institutional arrangements natural disaster recovery costs for critical infrastructure remain often borne by national governments. Infrastructure related costs make up the majority of government spending in the aftermath of a disaster, especially in the absence of risk transfer mechanisms such as insurance (g20/oecd, 2012). The intertwined nature of critical infrastructure ownership, operation, and financial responsibility in combination with the public interest provides national governments with a defensible rationale for ensuring proper financial and technical capacity for critical infrastructure resilience among actors in charge of owning or running them.

Effective institutional arrangements are needed to ensure resilience in a country's infrastructure assets and operations. In a first step, it is essential to identify concerned parties, and second parse out respective critical infrastructure roles and responsibilities as part of the policy framework development process. An important way of determining "who is responsible for what, how and when" in critical infrastructure resilience is enshrined in legislations and regulations of countries. An assessment of formal roles and responsibilities is hence an important part of establishing an effective governance structure. The examination of such policies and legal frameworks will also serve to identify potential existing gaps in defining roles and responsibilities. These steps should include an examination of the responsibilities across

different levels of governments, government sectors, as well as the determination of roles played by public and private infrastructure owners and/or operators.

To ensure that the identified responsible actors integrate resilience measures in the infrastructure they own or operate, governments have a number of instruments at hand to facilitate the process. Technical and economic regulation is a key instrument for governments to ensure critical infrastructure resilience. Mainstreaming resilience through public investment processes is also a key instrument to ensure that new infrastructure is gets designed in better and more resilient ways. Finally the government needs to provide platforms for actors to coordinate and collaborate effectively.

Technical regulation issued by the government can include resilience measures that take account of the potential disaster impacts. For example, nuclear energy regulators have looked at how flood risks and rivers' temperatures impact the future safety of nuclear power plants. Switzerland issued new regulation to take into account the potential changes in river temperatures induced by climate change, which in turn have an impact for hydroelectric dams and reservoirs (oecd, 2016).

Regulators can also set an obligation of results regarding service reliability. In finland, for example, electricity providers have to ensure that disruptions do not exceed 6 hours in densely-populated areas, or 36 hours in other areas. In france, critical operators have to produce protection plans to prepare for all kinds of hazards, of which natural hazards are a part (oecd, 2016).

Economic regulation is another means for governments to ensure critical infrastructure providers integrate resilience measures. However, sensitive issues of influencing competition and consumer pricing come into play. Governments need to provide sufficient flexibility for providers to adhere to economic regulations in meeting regulatory requirements (oecd, 2016). Considering cost-sharing arrangements for investments in critical infrastructure resilience are equally a part of establishing effective governance systems.

Mainstreaming resilience in public investment processes is equally critical. Making new infrastructure development resilient is the most effective way in minimising future economic losses caused by disasters. In peru, for example, all public investment projects undergo an assessment of the potential impact of natural disasters and based on its results appropriate risk reduction measures are identified and integrated into their design (lavell et al., 2016).

Governments do not necessarily retain the technical capacity to define or monitor complex resilience targets, and must therefore rely on collaborative relationships with the specialised expertise available in the private sector, to carry out these tasks. Governance arrangements that facilitate regular exchanges; sharing information and creating mutual trust, such as described in box 4, are necessary to ensure the effective integration of resilience measures in infrastructure planning. Government actors can facilitate the development of technical solutions (e.G., Information sharing and collaboration portals) that serve as a trusted and secure environment where private- and public-sector stakeholders can easily and regularly exchange ideas, information, and experiences relevant to critical infrastructure resilience (bach et al., 2013; Lewis, 2006)

Reciprocal critical infrastructure education and awareness programs designed to increase knowledge across the full spec-

Following a Box 4. Critical Infrastructure Stakeholder Engagement and Information Sharing

Seeking to facilitate efficient and effective relationships across stakeholder groups with shared responsibility for critical infrastructure resilience, several countries have developed programs and approaches to foster trust-based connections between government and private owners and operators.

- **United States Department of Homeland Security Protective Security Advisor (PSA) Program:** The program provides for proactive engagement among government partners and private sector owners and operators with responsibility for critical infrastructure. PSAs plan, coordinate, and conduct security and resilience surveys and assessments of nationally significant critical infrastructure. The program also delivers outreach activities and provides owners, operators, and other stakeholders with access to critical infrastructure security and resilience resources, training, and information. During and after an incident, Advisors serve as liaisons between government officials and private sector critical infrastructure owners and operators.

- **Australia's Trusted Information Sharing Network (TISN) for Critical Infrastructure Resilience.** The TISN provides a secure, non-competitive environment in which all critical infrastructure stakeholders can collaborate and engage in resilience building initiatives. The Network allows owners and operators across sector groups to regularly share information and cooperate within and across sectors to address security and business continuity challenges.

- **Canada Critical Infrastructure Gateway.** The Gateway meets one of the objectives under the Canadian National Strategy and Action Plan for Critical Infrastructure is the timely advancement of information sharing and protection among critical infrastructure partners. It is a collaborative, unclassified web-based workspace that includes members of the critical infrastructure community.

- **The European Union's Critical Infrastructure Warning Information Network (CIWIN).** CIWIN is an information-sharing system developed as a supporting component of the European Programme for critical Infrastructure Protection. The CIWIN facilitates the exchange of information on shared threats, vulnerabilities and appropriate measures and strategies to mitigate risk to critical infrastructure among European Union members and the European Commission. In addition to its information-sharing function, the CIWIN serves as a rapid alert system for early warnings regarding acute risks and threats.

- **Information Sharing and Analysis Centers (ISACs).** Sector-specific ISACs may be extensions of the national-level government, as in the case of the U.S. Telecommunications ISAC, which is managed by the National Communications System within the U.S. Department of Homeland Security, or entirely run by industry as the is the U.S. Water ISAC, a non-profit extension of the water sector's professional society. ISACs are viewed as a source for security-related best practices and for hazard and threat indications, warnings, and assessments.

Sources: U.S. DHS, Protective Security Advisors. Retrieved from: https://www.dhs.gov/protective-security-advisors; Australian Government, Trusted Information Sharing Network. Retrieved from: http://www.tisn.gov.au/Pages/default.aspx; Australian Government (2015). Critical Infrastructure Resilience Strategy Policy Statement. Retrieved from: http://www.tisn.gov.au/Documents/CriticalInfrastructureResilienceStrategyPolicyStatement.PDF; Canadian Critical Infrastructure Information Gateway, Retrieved from: https://cigateway.ps.gc.ca/_layouts/pscbranding/psclogon.aspx?ReturnUrl=%2f_layouts%2fAuthenticate.aspx%3fSource%3d%252F&Source=%2F; Canadian Critical Infrastructure Information Gateway Terms and Conditions of Service, Retrieved from: https://cigateway.ps.gc.ca/_layouts/pscbranding/trms-eng.pdf; Critical Infrastructure Warning Information Network, retrieved from: http://ec.europa.eu/dgs/home-affairs/what-we-do/networks/critical_infrastructure_warning_information_network/index_en.htm; Smedts, B. (2010). Critical Infrastructure Protection Policy in the EU: State of the Art and Evolution in the (Near) Future. Royal High Institute for Defence, Center for Security and Defence Studies Focus Paper 15. Retrieved from: http://www.irsd.be/website/images/livres/focuspaper/FP15.pdf; Lewis, T.G. (2006). Critical Infrastructure Protection in Homeland Security, Defending a Networked Nation. John Wiley & Sons. Sample retrieved from: http://samples.sainsburysebooks.co.uk/9780471789536_sample_381483.pdf; U.S. Department of Homeland Security. (2013) National Infrastructure Protection Plan: Partnering for Critical Infrastructure Security and Resilience. Retrieved from: https://www.dhs.gov/publication/nipp-2013-partnering-critical-infrastructure-security-and-resilience

trum of private- and public-sector stakeholders can provide the basis for improved readiness, and by extension, resilience (lewis, 2006). Owners and operators need to develop an understanding of local, regional, and national critical infrastructure resources, requirements, and plans. Policy makers must develop sufficient knowledge to develop sound critical infrastructure policies that promote security and resilience without imposing unrealistic burdens on owners and operators and also without inadvertently building in additional vulnerabilities (lewis, 2006). Box 4 provides several examples of successful critical infrastructure stakeholder engagement and secure information sharing approaches.

National governments generally convene cross-jurisdictional and cross-sectoral commissions with a mandate to coordinate the country's critical infrastructure landscape. National level commissions formed to

Figure 2 Critical Infrastructure Governance Structure In The United States

United States Critical Infrastructure Governance

Sector Coordinating Councils (SCCs)	Critical Infrastructure Cross-Sectoral Council	Government Coordinating Councils (GCCs)	Federal Senior Leadership	State, Local, Tribal, and Territorial Government Coordinating Council (SLTTGCC)	Regional Consortium Coordinating Council (RC3)	Information Sharing Organizations
Private sector councils	Private sector councils	Governmental councils	Federal council	Federal council	Partnership council	Nonprofit organizations
owners and operators and their representatives	chairs and vice chairs of the SCCs	representatives from various levels of government	senior officials from SSAs & other Federal departments and agencies	representatives from SLTT government entitites	regional groups & coalitions from around the country	e.g. Information Sharing and Analysis Centers (ISACs)
principal collaboration points between government & private sector: policy coordination and planning and a range of related sector-specific activities	coordinates cross-sector issues, initiatives, and interdependencies	enable inter-agency, intergovernmental, and cross-jurisdictional coordination within and across sectors; partner with SCCs on public-private efforts	facilitates communication and coordination across the Federal Government	promotes the engagement of SLTT partners; provides organizational structure to coordinate across jurisdictions on State & local government strategies	coordinates between regional groups & coalitions engaged in various initiatives to advance CI security and resilience	operational & dissemination functions; faciliate sharing of information between government and private sector; collaborate on a cross-sector basis through a national council

Source: U.S. Department of Homeland Security (2013), National Infrastructure Protection Plan: Partnering for Critical Infrastructure Security and Resilience

Figure 3 critical infrastructure governance structure in australia

Australian Critical Infrastructure Governance			
Trusted Information Sharing Network (TISN)	Sector Groups	Expert Advisory Groups	Communityies of Interest (CoI)
Cooperation forum	Cooperation forum	Advisory groups	Cooperation forum
owners and operators of CI: seven CI Sector Groups and two Expert Advisory Groups	government actors and individual owners and operators of CI	experts	government actors and individual owners and operators of CI
cooperation and coordination between owners and operators of CI; information sharing on threats and vulnerabilities; joint strategy & solutions development; promote CIR to owners and operators, incl. promoting the need for investment in resilient, reliable infrastructure	bridge between government and individual owners; assist owners and operators in sharing information on issues relating to generic threats & vulnerabilities; identify appropriate measures to mitigate risk	provide advice on broad aspects of CI requiring expert knowledge (on subject matters from both within and outside the TISN)	cross-sectoral consultation between government actors and individual owners and operators of CI on specific matters; convened when specifc CI issue demands attention and may be disabandoned once issue has been adequately addressed

Source: Australian Government (2010), Critical Infrastructure Resilience Strategy

initiate the process of developing a country's critical infrastructure resilience planning and management framework may exist beyond initial efforts and can serve as a permanent advisory body tasked with providing real-time insights into changes in the critical infrastructure landscape. Alternatively, these national level commissions may serve a term appointment that concludes with their findings. In the united states, for example, the president issued an executive order in 1996 creating the president's commission on critical infrastructure protection (pccip), which marked the beginning of a strategic focus on critical infrastructure as a key determinant of national security (pccip, 1997).

The composition of an effective governance structure will necessarily vary by country and will be influenced largely by the balance of the respective public and private critical infrastructure roles and responsibilities. Regardless of the national balance between publicly and privately owned or operated critical infrastructure, governing their resilience requires a transparent and collaborative approach that incorporates a variety of stakeholders such as the national government, different government sectors and levels of government and technical experts. Figures 2 and 3 provide examples of governance structures in the united states and australia.

4.5 National Critical Infrastructure Resilience Strategies And Plans

An increasing number of countries and regions have acknowledged the need for coordinated and joint critical infrastructure protection through national level critical infrastructure strategies or plans (wiseman and mclaughlin, 2014; oecd, 2017). The development of a critical infrastructure resilience strategy at the national level implicitly acknowledges that resilience cannot be fully achieved at the infrastructure operator or asset level due to shared responsibilities for, and interdependencies among, critical infrastructures (giannopoulos et al., 2012).

National critical infrastructure protection strategies are usually introduced by a definition of critical infrastructure, accompanied by nationwide criteria to evaluate the criticality of infrastructure, and finally a list of the sectors and infrastructures that are deemed critical in the specific country context. The swiss basic strategy for critical infrastructure protection, for example, considers ten sectors as critical and ranks the criticality for twenty-eight subsectors as very high, high and regular, with criticality referring to the relative importance of the subsector for citizens and the economy (federal office for civil protection, 2012).

National critical infrastructure strategies provide a common policy framework that enables a collaborative approach to strengthening the resilience of critical infrastructure. This is the case across countries with critical infrastructure protection or resilience strategies. For example, canada's national strategy for critical infrastructure explicitly identifies the role of partnerships across the federal government, provincial/territorial governments and critical infrastructure

Box 5. National Critical Infrastructure Protection Strategies

• **The Canadian National Strategy for Critical Infrastructure** sets the direction for enhancing the resilience of Canada's critical infrastructure against current and emerging hazards. To this end, the Strategy presents a collaborative approach to strengthening the resilience of critical infrastructure in Canada, ensuring that federal, provincial and territorial critical infrastructure activities are complementary and respect the laws of each jurisdiction. It outlines mechanisms for enhanced information sharing and information protection. It highlights that resilience of critical infrastructure can be achieved through the appropriate combination of security measures to address intentional and accidental incidents, through business continuity practices to deal with disruptions and emergency management planning to ensure adequate response procedures are in place to deal with unforeseen disruptions and natural disasters. At the national level, the Strategy classifies critical infrastructure within the ten following sectors: energy and utilities, finance, food, transportation, government, information and communication technology, health, safety, water, manufacturing.

• **The Swiss Basic Strategy for Critical Infrastructure Protection** outlines strategic goals and key principles for the protection of critical infrastructure in Switzerland. The Strategy covers the definition of comprehensive protection approaches, the identification and compilation of critical infrastructure elements and objects in a classified inventory, the establishment of cross-sectoral, public-private platforms, and information sharing on risks, notably risk assessment and warning systems, among stakeholders. The Strategy also addresses federal support to handle disruptions to critical infrastructure, in case critical infrastructure resources are overwhelmed. The strategy considers ten sectors as critical: government, energy, waste management, finance, health services, industries, information and communication, food, public safety and transportation.

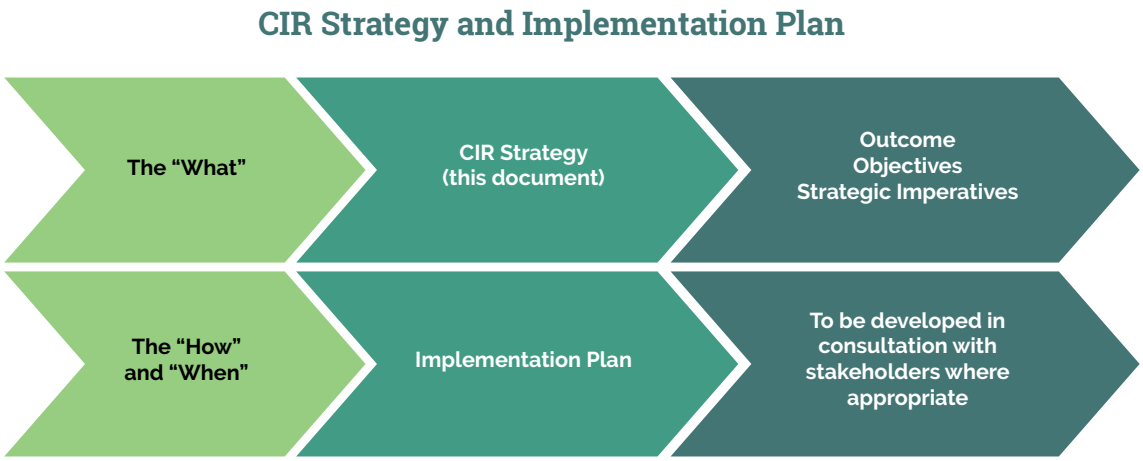
Sources: Canadian Government, 2009; Federal Office for Civil Protection, 201

operators as a necessary condition for achieving critical infrastructure resilience (canadian government, 2009). The canadian strategy identifies the country's critical infrastructure resilience and security objectives under three main focus areas that include: (i) building cross-sector and cross-governmental partnerships; (ii) implementing an all-hazards approach to risk management that employs public and private sector collaborative efforts, and (iii) sharing and protecting stakeholder information (canadian government, 2009). The german national strategy for critical infrastructure protection (cip strategy) also details specifically the need for strategic guidelines that as a means of promoting successful joint action among critical infrastructure stakeholders. As a second and related step in ensuring the security of critical infrastructure, the german cip strategy serves a foundation for the development of sub-goals that are implemented under additional critical infrastructure programs and plans (federal republic of germany, 2009) such as a national critical infrastructure resilience strategy implementation plan, sector-specific plans, and cross-sector plans.

Critical infrastructure strategies should lay the foundation for ongoing stakeholder coordination and communication and broadly identify stakeholders and describe their respective roles and responsibilities. These elements are common across many national level strategies. The polish national critical infrastructure protection programme (ncipp), for example, pays particular attention to building partnerships between stakeholders and established a national forum for infrastructure protection that brings representatives from publicly and privately owned critical infrastructure together to coordinate the resilience of critical infrastructure in poland (oecd, 2017).

Among countries with critical infrastructure protection, and some more recently critical infrastructure resilience frameworks,

Figure 5. Relationship between A CIR Strategy and A CIR Implementation Plan: the australian case



Source: Australian Government. (2015b). Critical Infrastructure Resilience Strategy.

the two-part approach to defining a critical infrastructure resilience strategy and a separate, but linked, critical infrastructure resilience implementation plan is not the exclusive approach used. Some countries set forth an implementation plan that is linked to their broader national level security strategy and represents a hybrid strategic-operational approach such as in the united kingdom or in the united states. Critical infrastructure resilience in the united kingdom is guided at the strategic level by the national security strategy which explains that one of the nation's key tasks is to "improve the resilience of the infrastructure most critical to keeping the country running against attack, damage or destruction" (united kingdom, 2011) and the national risk assessment which serves as the framework for risk-based implementation planning (united kingdom, 2016). The government published *keeping the country running: natural hazards and infrastructure* (kcr) as guidance for the implementation of a critical infrastructure resilience program in the united kingdom. The kcr is somewhat of a hybrid approach that details both strategies and provides specific practical guidance for enhancing resilience in critical infrastructure sectors (united kingdom, 2011). The united kingdom's implementation of critical infrastructure resilience activities is further defined by the regular refinement of sector resilience plans (united kingdom, 2016). Where used, the national critical infrastructure resilience strategy implementation plan operationalises the critical infrastructure resilience strategy by detailing specific actions with associated timelines for completion. New zealand, for example, employs strategic guidance detailed in its *the thirty year new zealand infrastructure plan 2015* and implements *plan's* guidance through an action plan appendix to the *plan* as well as its *ten-year capital intentions plan* (new zealand, 2015). Figure 5 illustrates the relationship between the national level critical infrastructure resilience (cir) strategy and the cir implementation plan in australia (australian government, 2015b).

Implementation plans may also entail the development of sector-specific plans, cross-sector plans, and cross-governmental plans. Implementation plans should provide specific, measurable, attainable, realistic and timed goals for promoting critical infrastructure resilience. Additionally, implementation plans should provide concrete, actionable guidance for critical infrastructure stakeholders. For example, the united kingdom's kcr includes a resilience checklist for critical infrastructure owners and operators in addition to guidance on information-sharing and guidance on assessing dependencies and interdependencies. Building on the, sector resilience plans in the united kingdom incorporate sector-specific performance standards and broader national and international standards (united kingdom, 2016). Critical sectors in the united kingdom apply british standards institution (bsi) and iso specification standards, in addition to risk, security and crisis management, corporate governance and organisational resilience standards (united kingdom, 2016). A national critical infrastructure resilience strategy implementation plan can serve as a benchmark that critical infrastructure stakeholders can use as reference for developing relevant ongoing monitoring and measurement programs. In this way, implementation plans serve a tangible link between the national strategy which factors risk, vulnerability, and interdependency assessment and ongoing monitoring programs and results.

4.6 Critical Infrastructure Financing

As previously mentioned, in many oecd countries, critical infrastructure systems are often owned or operated by a mixture of public and private sector arrangements. Railway networks, for example, can be owned publicly, but train services are operated privately. Energy production might be owned privately, but prices could be heavily regulated. From a public interest perspective, major investments to build resilience into critical infrastructure systems, or public investments in general, should entail an openly debated and structured negotiation on who bears what portion of the disaster risk-related cost *ex ante* in the investment, construction and maintenance process for preventive measures, as well as *ex post* for reconstruction and rehabilitation costs. Furthermore, the enforcement and implementation of agreed standards and targets should be objectively monitored and verified. The challenge is to define suitable governance arrangements for these pre-investment and post-investment processes, which are essential to protecting the public interest.

The investment and implementation plans for critical infrastructure as well as public investments at large, and should include financing strategies, i.E. Who is responsible for what share of the disaster risk-related costs, both in terms of *ex ante* investments in resilience measures and in terms of funding recovery costs. With fiscal constraints ever more common in the public sector, governments need to consider ways to boost the mainstreaming of resilience in critical infrastructure. . Some countries, such as peru and costa rica, are already taking steps to ensure that resilience aspects are considered in public investments. In peru, risk analysis and risk reduction are standard elements of the public investment project cycle, while in costa rica all investments need to be in line with the national development plan, which, among other things, requires a consideration of climate change and disaster related risks (zapata, 2016; martínez, 2016).

Governments may have different financing tools to contribute to greater critical infrastructure resilience. In terms of ex ante resilience financing *governments* may choose to subsidize the construction of protective infrastructure and other resilience measures, such as hardening and reconfiguration, for privately- or sub-nationally owned critical infrastructure. Governments may chose to fully cover the costs of protective measures for publicly-owned critical infrastructure or for critical infrastructure ranked as vital or major, independent of its ownership structure. In some countries, such as austria, a dedicated reserve fund serves as both a fund for financing disaster recovery and relief, and for funding *ex ante* investments in prevention and mitigation measures (oecd, 2016).

National governments may also choose to fund activities that enhance critical infrastructure owners' and operators' (national, sub-national and private) awareness of risks, vulnerabilities, and resilience measures. Funding may support critical infrastructure risk assessments; dependency and interdependency assessments; critical infrastructure-or focused trainings and exercises that boost technical expertise. If combined with other measures the risk assessment tools can be a useful pathway to facilitate increased resilience of critical infrastructure. Governments may for example establish legal requirements to demonstrate that the necessary *ex ante* investments in disaster risk reduction measures have been made, taking into account the risks identified during the risk assessment phase. Another

Box 6. Risk transfer tool to manage public sector exposures

A number of risk transfer tools can be developed in order to manage the exposure to public finances related to post-disaster reconstruction of publicly-owned assets:

• **Insurance of public assets:** Individual government asset-owners can acquire specific insurance coverage for the assets that they are responsible for (individually or on a portfolio basis). The cost of insurance can be reduced by choosing high deductible levels for the insurance policies acquired (i.e. covering only more extreme events) or by including a diverse set of assets into a single policy. Countries can benefit from pricing advantages by centralising the acquisition of insurance in a single department (or even through a public insurance vehicle). For example, Costa Rica is establishing an insurance vehicle for insuring public assets through a public insurer and transferring only excessive losses to international financial markets. A number of other countries also operate public insurers, either at the national or sub-national levels, to provide insurance for public assets (e.g. Australia, Philippines, Indonesia). In Colombia, the government procurement agency is establishing a group insurance policy and providing access to this policy to individual departments to insure their assets.

• **Insurance of public expenditures:** Another approach is to enter into risk transfer transactions that provide a pay-out based on the occurrence of a disaster as a means of providing a source of funds to finance reconstruction expenses. In many cases, these transactions are structured to pay-out based on the occurrence of a disaster of a specific magnitude (e.g. earthquake of a specific magnitude, flood or storm surge causing inundation of a certain level), which provides the benefit of a faster pay-out (although the risk that the pay-out may not correspond to actual loss levels). The risk transfer approaches may be structured through a regional risk pooling initiative (such as the Caribbean Catastrophe Risk Insurance Facility) - which also creates benefits through a more diverse set of risk - as a (re)insurance arrangement based on a parametric trigger, or through the issuance of catastrophe bonds (which are basically bonds that default in the event of a the occurrence of the specified event, allowing the transfer of bondholder funds to the bond issuer affected by the disaster).

Countries should also consider how to ensure sufficient funding to finance the risks that are retained (i.e. not transferred through insurance or other risk transfer mechanisms). The contingent credit facilities offered by multilateral banks can provide a readily-available source of funding to re-establish the services disrupted by the disaster. For example, IDB has such facilities for total amount of USD 1,486 million covering Dominican Republic, Peru, Ecuador, Nicaragua, Honduras and Panama. Other multilateral banks such as The World Bank and The Development Bank for Latin America (CAF) and bilateral cooperation agencies such as the Japanese International Cooperation Agency (JICA) have similar financial mechanisms.

Source: G20/OECD, 2012; OECD, 2015a

related approach is to "reward" those owners/operators with more generous post-disaster recovery support funding that implemented the necessary resilience measures this approach creates a positive incentive system, but may have drawbacks with respect to critical infrastructure, as it may lead to different levels of resilience across critical infrastructure.

Given the potential exposure of national governments to costs related to rebuilding infrastructure damaged in a disaster, national governments may also want to devise financing or cost sharing strategies for recovery costs:

- For national publicly-owned critical infrastructure assets, national governments should assess the most cost-effective way to finance rebuilding costs. Governments need to decide whether self-insurance or risk transfer of some or all these exposures would be the best fit. For example, mexico has undertaken comprehensive modelling of public exposure, which includes critical infrastructure but goes beyond it, to disaster risks and has started transferring the higher layers of that exposure (i.E. Exposures related to more severe and less frequent events) to reinsurance and capital markets. There may be advantages in centralising the acquisition of insurance for nationally-owned public infrastructure (e.G. Through a single insurance vehicle or "group" policy) in order to benefit from the lower premiums that can usually be secured for a more diverse pool of assets. For example, in colombia, the ministry of finance requires that nationally-owned assets are appropriately insured.
- For sub-national publicly-owned infrastructure assets, national governments should aim to ensure that sub-national governments are appropriately managing their exposure to disaster risks. Cost-sharing arrangements between national and sub-national levels of government for rebuilding costs are necessary to ensure that disaster risks are appropriately managed. The cost-sharing arrangements could take into account the extent to which sub-national governments have made efforts to ensure their own resilience. In some countries, including el salvador, honduras, bolivia, colombia, costa rica, nicaragua, panama and peru, legal mandates requiring insurance of sub-national publicly owned infrastructure assets have been established. National governments may also want to monitor or establish requirements related to financial resilience, such as a requirement to demonstrate that sufficient self-insurance capacity would be available or to assess possible risk transfer options for those exposures. Similar to national governments, sub-national governments could also centralise the acquisition of insurance for their assets in order to reap pricing advantages in risk-transfer markets. For example, in australia, the treasury requires sub-national governments to submit regular reports on their insurance arrangements and may reduce the national cost-share rate for reconstruction costs in states where insurance arrangements are deemed to be insufficient.

- For privately-owned infrastructure assets, national governments may wish to impose requirements related to financial resilience, such as appropriate levels of insurance, or equivalent levels of demonstrated self-insurance capacity, to ensure appropriate management of the financial exposures by private operators and therefore reduce disruption in the event of a disaster. In the latin american and caribbean region, for example, only mexico and chile have established insurance standards for public services operated by private owners.

Private risk transfer mechanisms, such as insurance, can also help to change the current risk culture. If insurers have the ability to align premiums more closely with actual risks and associated losses then infrastructure owners/operators will be incentivized to act in a way that lowers the probability/consequence of insured risk in an attempt to reduce premiums (flynn, 2015). The public sector's role in this arrangement is to evaluate the risk reduction actions taken by the owners or operators. This will require research and development into new mitigation standards and the identification of low-cost means for achieving compliance (flynn, 2015). For countries that have tended to provide high levels of government funding for repairs and replacement following disasters, a move away from this trend is important (flynn, 2015). If infrastructure owners/operators not only discount actual risks, but also believe that the government will provide substantial post-disaster/event funding that will cover much of their loss, then the government is viewed as a de facto insurer that doesn't require premiums (flynn, 2015).

Box 7. Innovative Critical Infrastructure Resilience Financing Mechanisms

Following the critical infrastructure failures observed during Superstorm Sandy, the New Jersey government implemented financing mechanisms to encourage the development of resilient critical infrastructure. New Jersey's, first in the nation, Energy Resilience Bank (ERB) was created with USD 200 million in federal Community Development Block Grant-Disaster Recovery funds to support the development of distributed energy resources at critical facilities throughout the state that will enable them to remain operational during future outages.

"Financing options available through the ERB will consist of grants and loans to address unmet funding needs. Grants and forgivable loans will be offered to address up to 40 percent of unmet funding needs, while low-interest, amortizing loans will be available for the remaining 60 percent of unmet funding needs. Grants and loans may require equity contribution, and any principal forgiveness component will require evidence of meeting minimum performance requirements as indicated in the program guide."

Eligible technologies must include islanding (ability to operate isolated from the electric utility grid) and blackstart (ability to start up without a direct connection to the electric grid) capabilities, and have the capability to operate at critical load. The program includes a sliding scale of matching funds based on the characteristics (i.e., profit, not-for-profit) of the applicants and an assessment of the project needs, feasibility, and return on investment.

Sources: New Jersey Board of Public Utilities. NJ Energy Resilience Bank Now Accepting Applications. News Release, October 20, 2014. Retrieved from: http://www.state.nj.us/bpu/newsroom/announcements/pdf/20141020_erb_press.pdf

An alternate approach is to require critical infrastructure owners/operators to maintain a prescribed level of insurance coverage.

The applicability of specific funding mechanisms will necessarily vary by country context and will be influenced largely by the balance of the respective public and private critical infrastructure roles and responsibilities.

4.7 Monitoring And Evaluation

Once assessment methodologies have been determined and risk management and resilience promotion activities, such as installing robustness or redundancy measures, have commenced, data should be collected to set a baseline against which comparisons can be made (nrc, 2009; oecd, 2014a). For example, in a post-disaster context, resilience can be assessed by quantifying post-disaster system functionality and tracking the amount of time necessary to achieve pre-disaster levels of performance (tierney and bruneau, 2007). Additionally, the identification and tracking of metrics, provides stakeholders with the means to both quantify how their activities and investments shape their performance and how their actions relate to their risk profile.

Authority for overseeing independent assessments and monitoring critical infrastructure resilience varies across countries and is dependent on the balance between privately and publicly owned and operated infrastructure. In many oecd countries statutory and regulatory frameworks apply to private sector security operations. In countries such as the united states the primary mechanism for collective action for enhancing critical infrastructure resilience has been and will likely remain voluntary

Table 4. Resilience Performance Criteria

Criteria	Expectation
Efficiency	This criterion requires that an infrastructure system perform its functions in order to meet its specified functional requirements (technical efficacy) at lowest cost (cost effectiveness). Metrics for efficiency include the costs of building and maintaining a complex infrastructure system within the constraints of its technical performance, reliability, and service-continuity.
Sustainability	This criterion evaluates the extent to which the system uses resources – natural, human, and manufactured – in a sustainable manner. Sustainability is defined as a resource-use pattern that "meets today's needs while protecting resources for future use." To be sustainable, critical infrastructures must be designed and operated within the context of their impacts on the surrounding ecosystems, now and in the future. The metrics for assessing an infrastructure's sustainability include the extent to which construction and operating inputs and resources are used in accordance with the long-term economic and environmental standards developed for the system.
Survivability	This criterion for resilient infrastructure is the ultimate test of safety, security, and survival of the people, infrastructure assets, and the ecosystem. In accordance with this criterion, an infrastructure meets the resiliency standards if it is capable of withstanding damages with minimal adverse impacts – lost lives, ecological impacts, structural damage – on the people, operations, economy, and the environment.

collaboration between public and private stakeholders (u.S. Department of homeland security, 2013).

Although specifically addressing resilience measurements and measurement tools in a community-level context, guidelines described by cutter (2015) apply to the measurement of critical infrastructure resilience. Cutter's guidelines include the following:

- Because critical infrastructure systems are not identical and the interdependences across critical infrastructure vary by sectors and national, sub-national, and regional contexts, measuring the resilience of critical infrastructure requires a toolkit comprised of a variety of indicators.
- Communities need simply concepts that are technically feasible to implement at the community level. Tools need to be adjusted and modified to fit communities' needs and promoted in a way that makes the business case for resilience.
- Necessary components of resilience tools include the ability to: assess and prioritise needs and goals; establish baselines; monitor progress and recognize success; weigh costs (investments) and benefits (results); and evaluate the effects of different policies and approaches (cutter, 2014).
- According to barami (2013), infrastructure systems that incorporate resiliency, are likely to meet the three high-level performance criteria detailed in the table 4, which could build the basis for performance monitoring and evaluation.

Ongoing monitoring of critical infrastructure resilience will require investment in data capture systems that capture cross-sectoral data that can be used to assess risk reduction with respect to cascading impacts while also enhancing stakeholders' understanding of evolving dependencies and interdependencies. Additionally, monitoring systems must include built-in capacity for near real-time data updates. Combined approaches that incorporate remote sensing technologies, geo-referencing, and data feeds require funding for the development of systems architecture, implementation of field level equipment, maintenance of relational databases, and training on the use of these applications.

4.8 The Use Of Exercises And Post-Event Lessons Learned

Critical infrastructure resilience is an ongoing, dynamic effort. Ensuring the sustainability and relevance of critical infrastructure programs requires a mechanism for capturing and internalizing lessons learned from tangible experiences such as exercises, trainings, and even real-world incidents. Exercises and trainings designed with a specific focus on critical infrastructure stakeholder coordination and communications, interdependencies and potential cascading impacts, and information-sharing help to enhance public and private critical infrastructure partners understanding of strategies, plans, and programs while also providing opportunities to practice actions that lend to the adaptability of the human element of critical infrastructure operational effectiveness. Exercises and trainings also further improve ready coordination among the wide variety of stakeholders involved in promoting the resilience of

critical infrastructure. Finally, it is important the critical infrastructure resilience programs are themselves adaptability to the evolving landscape. Exercises provide a "safe space" for testing the assumptions and actions built into critical infrastructure plans and the results of exercises are useful in identifying weaknesses and gaps in the planning and management of critical infrastructure.

Lessons learned from exercises, trainings, and real-world incidents are essential to improving resilience programs and the degree to which this information can be constructively used depends on the development and regular refinement of mechanisms designed to collect and analyse lessons learned. To this end, the public sector can lead the development and implementation of processes and systems that guide how lessons learned are collected and analysed as well as how analysis translates to the identification of corrective actions and adjustments to the national critical infrastructure resilience strategy, implementation plan, and other related initiatives. The german cip strategy notes that lessons learned should be derived from continuously updated threat analyses in addition to analyses of domestic and international incidents and those lessons learned should then be incorporated into critical infrastructure standards that collaboratively developed by stakeholders (federal republic of germany, 2009). The swedish action plan for the protection of vital societal functions & critical infrastructure echoes the importance of translating lessons learned into improvements noting that: "*the perspectives before, during and after serious disruptions need to be included in the work so that society will be able to resist, manage, recover, learn and develop from disruptions*" (swedish civil contingencies agency, 2014).

References

Acton, J. M., And Hibbs, M. (2012). Why Fukushima Was Preventable Carnegie Paper Carnegie Endowment For International Peace. Retrieved From: Http://Carnegieendowment.org/2012/03/05/Why-Fukushima-Was-Preventable-Pub-47361

Australian Government (2015B). Critical Infrastructure Resilience Strategy Policy Statement. Retrieved From: Http://Www.tisn.gov.au/Documents/Criticalinfrastructureresiliencestrategypolicystatement.pdf

Australian Government, Trusted Information Sharing Network. Retrieved From: Http://Www.tisn.gov.au/Pages/Default.aspx

Australian Government. (2010). Critical Infrastructure Resilience Strategy. Retrieved From: Http://Ccpic.mai.gov.ro/Docs/Australian+Government+S+Critical+Infrastructure+Resilience+Strategy.pdf

Australian Government. (2015A). Critical Infrastructure Resilience Strategy: Plan. Retrieved From: Http://Www.aph.gov.au/Documentstore.ashx?Id=A58ed84e-67Fe-42E2-8394-F9344db6d52d&Subid=407872

Bach, C., Bouchon, S., Fekete, A., Birkmann, J., And Serre, D. (2013). Adding Value To Critical Infrastructure Research And Disaster Risk Management: The Resilience Concept. Sapi En. S. Surveys And Perspectives Integrating Environment And Society, (6.1). Retrieved From: Https://Sapiens.revues.org/1626

Barami, B. (2013). Summary Prepared For Beyond Bouncing Back: A Roundtable On Critical Transportation Infrastructure Resilience Held At The Volpe Center On April 30, 2013. Excerpted From A Draft White Paper Entitled A Risk-Based Infrastructure Resiliency Framework. John A. Volpe National Transportation Systems Center, U.s. Department Of Transportation, 55 Broadway, Cambridge, Ma, 02142. Retrieved From: Https://Www.volpe.dot.gov/Sites/Volpe.dot.gov/Files/Docs/Infrastructure%20Resiliency_a%20Risk-Based%20Framework.pdf

Brown, G. And Cox, L. (2011). How Probabilistic Risk Assessment Can Mislead Terrorism Risk Analysts. Isk Analysis, Vol. 31, No. 2, 2011. Retrieved From: Https://Doi.org/10.1111/J.1539-6924.2010.01492.X

Cambridge Centre For Risk Studies, Cambridge Risk Atlas Part I: Overview And Results World Cities Risk 2015-2025, September 2015. Retrieved From: Cambridgeriskframework.com/Getdocument/24

Canadian Critical Infrastructure Information Gateway Terms And Conditions Of Service, Retrieved From: Https://Cigateway.ps.gc.ca/_Layouts/Pscbranding/Trms-Eng.pdf

Canadian Critical Infrastructure Information Gateway, Retrieved From: Https://Cigateway.ps.gc.ca/_Layouts/Pscbranding/Psclogon.aspx?Returnurl=%2F_layouts%2Fauthenticate.aspx%3Fsource%3D%252F&Source=%2F

Canadian Government. (2009). Canadian National Strategy For Critical Infrastructure. Retrieved From: Https://Www.publicsafety.gc.ca/Cnt/Rsrcs/Pblctns/Srtg-Crtcl-Nfrstrctr/Index-Eng.aspx

Canadian Government. (2014). Action Plan For Critical Infrastructure 2014-2017. Retrieved From: Https://Www.publicsafety.gc.ca/Cnt/Rsrcs/Pblctns/Pln-Crtcl-Nfrstrctr-2014-17/Pln-Crtcl-Nfrstrctr-2014-17-Eng.pdf

Centre Of European Policy Studies (Ceps). (2010). Protecting Critical Infrastructure In The Eu. Ceps Task Force Report, Bernhard Hammerli (Chair) And Andrea Renda (Rapporteur). Retrieved From: Https://Www.ceps.eu/System/Files/Book/2010/12/Critical%20Infrastructure%20Protection%20Final%20A4.Pdf

Chapin, E., Daniels, A., Elias, R., Aspilcueta, D., & Doocy, S. (2009). Impact Of The 2007 Ica Earthquake On Health Facilities And Health Service Provision In Southern Peru. Prehospital And Disaster Medicine, 24(04), 326-332. Retrieved From: Http://Citeseerx.ist.psu.edu/Viewdoc/Download?Doi=10.1.1.176.3202&Rep=Rep1&Type=Pdf

Chang, S.; McDaniels, T.; Fox, J.; Dhariwal, R.; Longstaff, H. (2013). "Toward Disaster-Resilient Cities: Characterizing Resilience of Infrastructure Systems with Expert Judgments". Risk Analysis. Vol. 34/3, Wiley. Retrieved from: http://onlinelibrary.wiley.com/doi/10.1111/risa.12133/full

Clancy, M. (2012). First: Define Critical Infrastructure. Sc Magazine, For It Professionals. Retrieved From: Http://Www.scmagazine.com/First-Define-Critical-Infrastructure/Article/250410/

Comerio, M. (2013). Housing Recovery In Chile: A Qualitative Mid-Program Review. Peer Report 2013/01. Pacific Earthquake Engineering Research Center. Retrieved From: Http://Peer.berkeley.edu/Publications/Peer_reports/Reports_2013/Webpeer-2013-01-Comerio.pdf

Critical Five (2014). Forging A Common Understanding For Critical Infrastructure. Retrieved From: Https://Www.dhs.gov/Sites/Default/Files/Publications/Critical-Five-Shared-Narrative-Critical-Infrastructure-2014-508.Pdf

Critical Infrastructure Warning Information Network, Retrieved From: Http://Ec.europa.eu/Dgs/Home-Affairs/What-We-Do/Networks/Critical_infrastructure_warning_information_network/Index_en.htm

Cutter, S. (2015). Developing A Framework For Measuring Community Resilience. From: Committee On Measures Of Community Resilience: From Lessons Learned To Lessons Applied; Resilient America Roundtable; Policy And Global Affairs; National Research Council. Washington (Dc): National Academies Press (Us); 2015 Mar 26. Retrieved From: Http://Www.ncbi.nlm.nih.gov/Books/Nbk285736/

Cutter, S. (February 2014). The Landscape Of Resilience Measures. Presentation At The Resilient America Roundtable Workshop On Measures Of Community Resilience. Retrieved From: Http://Sites.nationalacademies.org/Cs/Groups/Pgasite/Documents/Webpage/Pga_152239.Pdf

Davies, R. (2016). Floodlist: Brazil Floods And Landslides – 1 Dead, 3 Missing In Recife After 235 Mm Of Rain In 12 Hours Retrieved From: Http://Floodlist.com/America/Brazil-Landslide-Recife-Pernambuco-May-2016

Dilley, M., Chen, R.s., Deichmann, U., Lerner-Lam, A. L., And Arnold, M. (2005). Natural Disaster Hotspots: A Global Risk Analysis. Washington, Dc: World Bank. Retrieved From: Https://Openknowledge.worldbank.org/Handle/10986/7376

Economic Commission For Latin America And The Caribbean (Eclac) (2015). The Economics Of Climate Change In Latin America And The Caribbean Paradoxes And Challenges Of Sustainable Development. Retrieved From: Http://Repositorio.cepal.org/Bitstream/Handle/11362/37311/S1420655_en.pdf

Emergency Response Coordination Centre (Ercc), European Commission, Humanitarian Aid And Civil Protection. (2015). Echo Daily Map 27/3/2015 Chile – Floods. Retrieved From: Http://Erccportal.jrc.ec.europa.eu/Getdailymap/Docid/1109

European Commission. (2006). Communication From The Commission On A European Programme For Critical Infrastructure Protection Com (2006) 786 Final. Retrieved From: Http://Eur-Lex.europa.eu/Lexuriserv/Lexuriserv.do?Uri=Com:2006:0786:Fin:en:pdf

European Commission. (2012). Commission Staff Working Document: On The Review Of The European Programme For Critical Infrastructure Protection (Epcip). Retrieved From: Http://Register.consilium.europa.eu/Doc/Srv?L=En&F=St%2011887%202012%20Init

European Commission. (2015). Resilience Of Critical Infrastructure Protection: Guidelines. Retrieved From: Http://Www.recipe2015.Eu/Userdocsimages/Pdf/Guidelines_final_042006.Pdf

European Commission. (2016). Principles Of Resilience For Critical Infrastructures: Compendium Of Presentations. Retrieved From: Http://Www.recipe2015.Eu/Userdocsimages/Pdf/Conference%20Presentations.pdf

European External Action Service. About Eu Humanitarian Response In Haiti. Retrieved From: Https://Eeas.europa.eu/Delegations/Haiti/Documents/Page_content/Keys_facts_and_figures_about_eu_humanitarian_response_in_haiti_en.pdf

Federal Emergency Management Agency (Fema) (2013). Hurricane Sandy Fema After-Action. Retrieved From: Https://Www.fema.gov/Media-Library-Data/20130726-1923-25045-7442/Sandy_fema_aar.pdf

Federal Emergency Management Agency (Fema). (2004). Risk Management Series, Design Guide For Improving School Safety In Earthquakes, Floods, And High Winds. Retrieved From: Https://Www.fema.gov/Pdf/Plan/Prevent/Rms/424/Fema424_cvr-Toc.pdf

Federal Office For Civil Protection (2012). Nationale Strategie Zum Schutz Kritischer Infrastrukturen [National Strategy For The Protection Of Critical Infrastructure]. Retrieved From: Https://Www.admin.ch/Opc/De/Federal-Gazette/2012/7715.Pdf

Federal Republic Of Germany, Federal Ministry Of The Interior. (2009). National Strategy For Critical Infrastructure Protection (Cip Strategy). Retrieved From: Http://Www.bbk.bund.de/Shareddocs/Downloads/Bbk/En/Cip-Strategy.pdf?__Blob=Publicationfile

FEMA (2013). Hurricane Sandy FEMA After-Action. Retrieved from: https://www.fema.gov/media-library-data/20130726-1923-25045-7442/sandy_fema_aar.pdf

Fermandois, A. (2011). "Chile And Its Earthquake: Preparedness, Response And Lessons", Government Of Chile, Ambassador's Office. Retrieved From: Http://Dels.nas.edu/Resources/Static-Assets/Materials-Based-Onreports/Presentations/Ambassadorfermandois.pdf .

Flynn, S. E. (2008). America The Resilient: Defying Terrorism And Mitigating Natural Disasters. Foreign Affairs. Tampa, Fl: Council On Foreign Relations. Retrieved From: Www.foreignaffairs.com/Articles/63214/Stephen-E-Flynn/America-The-Resilient

Flynn, S.E. (2015). Bolstering Critical Infrastructure Resilience After Superstorm Sandy: Lessons for New York and the Nation. Retrieved from: https://hazdoc.colorado.edu/handle/10590/3003

G20/Oecd (2012). Methodological Framework For Risk Assessment And Risk Financing. Retrieved From: Http://Www.oecd.org/Gov/Risk/G20disasterriskmanagement.pdf

Garcia, Cesar. (2010). Ap/Nbc News Article: 20,000 Miles Of Highway Hit By Colombia Floods. Retrieved From: Http://Www.nbcnews.com/Id/40606798/Ns/Weather/T/Miles-Highway-Hit-Colombia-Floods/#.V972P_5thiu

Giannopoulos, G., Filippini, R., & Schimmer, M. (2012). Risk Assessment Methodologies For Critical Infrastructure Protection. Part I: A State Of The Art. European Commission, Joint Research Centre (Jrc), Institute For The Protection And Security Of The Citizen. Retrieved From: Http://Ec.europa.eu/Home-Affairs/Doc_centre/Terrorism/Docs/Ra-Ver2.Pdf

Gordon, K., & Dion, M. (2008). Protection Of Critical Infrastructure And The Role Of Investment Policies Relating To National Security. Oecd Publishing.

Hawkesworth, I. (2011), From Lessons To Principles For The Use Of Public-Private Partnerships, Public Governance And Territorial Development, Public Management Committee, 32Nd Annual Meeting Of The Working Party Of Senior Budget Officials, June, Luxemburg. Http://Www.oecd.org/Gov/Budgeting/48144872.Pdf

Hazur. Introduction To Urban Resilience With Hazur Online Course. Retrieved From: Https://Learn.canvas.net/Courses/921/Pages/4-Dot-3-Study-Cases-Barcelona; Hazur Resilient Systems Homepage. Retrieved From: Http://Opticits.com/#Hazur

Helm, P. (2008). Presentation At The International Disaster And Risk Conference, Davos, 28 August 2008. Critical Infrastructure Resilience: Perspective From New Zealand. Retrieved From: Https://Idrc.info/Fileadmin/User_upload/Idrc/Former_conferences/Idrc2008/Presentations2008/Helm_patrick_owen_critical_infrastructure_protection_a_perspective_from_new_zealand.pdf

Imf (2016). World Economic And Financial Surveys, Regional Economic Outlook, Western Hemisphere Managing Transitions And Risks Retrieved From Http://Www.imf.org/External/Pubs/Ft/Reo/2016/Whd/Eng/Pdf/Wreo0416.Pdf

Inter-American Development Bank (Idb). (2015). Index Of Governance And Public Policy In Disaster Risk Management. Technical Note N Idb-Tn-720. Retrieved From: Https://Publications.iadb.org/Bitstream/Handle/11319/6717/Igopp_index_governance_public_policy_disaster_risk_management.pdf

Kreft, S., D. Eckstein, L. Junghans, C. Kerestan And U. Hagen (2015). Global Climate Risk Index 2015. Who Suffers Most From Extreme Weather Events? Weather-Related Loss Events In 2013 And 1994 To 2013. Briefing Paper. Retrieved From: Https://Germanwatch.org/En/Download/10333.Pdf

Kunreuther, H., Michel-Kerjan, E., & Porter, B. (2003). Assessing, Managing, And Financing Extreme Events: Dealing With Terrorism (No. W10179). National Bureau Of Economic Research.

Lavell, A., Standon-Geddes, Z., Zapata-Rondón, N., And Karen Kraft (2016). Disaster And Climate-Risk Sensitive Planning For Public Investment Decisions: Learning From Two Public-Sector Experiences Of Lao Pdr And Peru. Understanding Risk Conference Contribution 2016. Https://Understandrisk.org/Wp-Content/Uploads/Disaster-And-Climate-Risk-Sensitive-Planning-For-Public-Investment-Decisions.pdf (Accessed 6 February 2017).

Lewis, T.g. (2006). Critical Infrastructure Protection In Homeland Security, Defending A Networked Nation. John Wiley & Sons. Sample Retrieved From: Http://Samples.sainsburysebooks.co.uk/9780471789536_Sample_381483.Pdf

Linkov, I., Eisenberg, D. A., Bates, M. E., Chang, D., Convertino, M., Allen, J. H., Flynn, S.e. & Seager, T. P. (2013). Measurable Resilience For Actionable Policy. Environmental Science & Technology, 47(18), 10108-10110.

Macaulay, T. (2016). Critical Infrastructure: Understanding Its Component Parts, Vulnerabilities, Operating Risks, And Interdependencies, Crc Press, Boca Raton

Martínez, F. (2016). *Diálogo Regional De Política: Gestión Del Riesgo De Desastres Y La Inversión Pública: Costa Rica* [Regional Political Dialogue: Disaster Risk Management And Public Investments: Costa Rica]. Retrieved From: Http://Idbdocs.iadb.org/Wsdocs/Getdocument.aspx?Docnum=40723154

Masoero, A. (2016). Floodlist: Argentina And Uruguay – Floods Displace Thousands After 4 Days Of Heavy Rain April 8, 2016. Retrieved From: Http://Floodlist.com/America/Argentina-Uruguay-Floods-April-2016

Mcgee, S., Frittman, J., Ahn, S., And Murray, S. (2014). Risk Relationships And Cascading Effects In Critical Infrastructures: Implications For The Hyogo Framework. Prepared For The Global Assessment Report On Disaster Risk Reduction 2015, United Nations Office For Disaster Risk Reduction. Retrieved From: Http://Www.preventionweb.net/English/Hyogo/Gar/2015/En/Bgdocs/Mcgee%20Et%20Al.,%202014.Pdf

Minkel, J. R. (2008). The 2003 Northeast Blackout--Five Years Later. Scientific American, 13. Retrieved From: Http://Www.scientificamerican.com/Article/2003-Blackout-Five-Years-Later/

Moteff, J. (2012). Critical Infrastructure Resilience: The Evolution Of Policy And Programs And Issues For Congress. U.s. Congressional Research Service Report No. R42683. Retrieved From: Https://Www.fas.org/Sgp/Crs/Homesec/R42683.Pdf

Muir-Wood, R (2011). "Designing Optimal Risk Mitigation And Risk Transfer Mechanisms To Improve The Management Of Earthquake Risk In Chile", Oecd Working Papers On Finance, Insurance And Private Pensions, No. 12, Oecd Publishing. Http://Www.oecd.org/Daf/Fin/Insurance/48794964.Pdf

Nacs (2013). 2013 Nacs Retail Fuels Report. Retrieved From: Http://Www.nacsonline.com/Yourbusiness/Fuelsreports/Gaspricies_2013/Pages/How-Hurricane-Sandy-Affected-The-Fuels-Industry.aspx

National Research Council (Nrc). (2009). Sustainable Critical Infrastructure Systems: A Framework For Meeting 21St Century Imperatives. Toward Sustainable Critical Infrastructure Systems: Framing The Challenges Workshop Committee. National Research Council, Washington, Dc

New Jersey Board Of Public Utilities. Nj Energy Resilience Bank Now Accepting Applications. News Release, October 20, 2014. Retrieved From: Http://Www.state.nj.us/Bpu/Newsroom/Announcements/Pdf/20141020_Erb_press.pdf

New Zealand. (2015). The Thirty Year New Zealand Infrastructure Plan 2015. Retrieved From: Http://Www.infrastructure.govt.nz/Plan/2015

Oecd (2011). Future Global Shocks Improving Risk Governance, Oecd Reviews Of Risk Management Policies. Retrieved From: Http://Www.keepeek.com/Digital-Asset-Management/Oecd/Governance/Future-Global-Shocks_9789264114586-En#.V99lj_5thiu#Page4

Oecd (2015A). Disaster Risk Financing. A Global Survey Of Practices And Challenges. Oecd Publishing.

Oecd (2015B). Establishing Effective Public Private Partnerships For Risk Management. What Are The Possible Options For Government? Discussion Note. High Level Risk Forum. Retrieved From: Https://One.oecd.org/Document/Gov/Pgc/Hlrf(2015)5/En/Pdf

Oecd (2015C). Towards A Framework For The Governance Of Infrastructure. Retrieved From: Https://Www.oecd.org/Gov/Budgeting/Towards-A-Framework-For-The-Governance-Of-Infrastructure.pdf

Oecd (2016). Boosting Resilience Through Innovative Risk Governance: The Case Of Alpine Areas In Austria. Oecd Publishing.

Oecd (2017). Toolkit For Risk Governance. Retrieved From: Https://Www.oecd.org/Governance/Toolkit-On-Risk-Governance/Goodpractices/#?Hf=10&B=0&Sl=Trig&S=-Desc(Document_lastmodifieddate)

Oecd (*Forthcoming*). Implementing The Recommendation On The Governance Of Critical Risk: Overview Of Country Progress, Oecd Publishing, Paris.

Oecd (*Forthcoming*). National Risk Assessments: A Cross Country Perspective. Oecd Publishing.

Oecd (*Forthcoming*). Oecd Recommendation On Disaster Risk Financing Strategies. Http://Www.oecd.org/Finance/Insurance/Public-Consultation-Drf.htm

Oecd. (2014A). Boosting Resilience Through Innovative Risk Governance. Oecd Publishing.

Oecd. (2014B). Recommendation Of The Council On The Governance Of Critical Risks. Retrieved From: Http://Www.oecd.org/Gov/Risk/Recommendation-On-Governance-Of-Critical-Risks.htm

Office Of The United Nations Recovery Coordinator (Unorc). (2007). United Nations Office Of The Resident Coordinator: Situation Report No. 21: Earthquake In Peru, 1–6; September 28, 2007. Retrieved From: Http://Reliefweb.int/Sites/Reliefweb.int/Files/Resources/Fa4ceb19ff916d-9c85257367007254f9-Full_report.pdf

Pelling, M., Basher, R., Birkmann, J., Cutter, S., Desai, B., Fakhruddin, S.h.m., Ferrugini, F., Mitchell, T., Oliver-Smith, T., Rees, J., And Kuniyoshi, T. (2014). Issue Brief: Disaster Risk Reduction And Sustainable Development. Prepared By The Integrated Research On Disaster Risk (Irdr) Programme For The Seventh Session Of The Un General Assembly Open Working Group On Sustainable Development Goals. Retrieved From: Sustainabledevelopment.un.org/Getwsdoc.php?Id=2133

President's Commission On Critical Infrastructure Protection (Pccip). (1997). Critical Foundations: Protecting America's Infrastructure. Retrieved From: Https://Www.fas.org/Sgp/Library/Pccip.pdf

Public Safety And Emergency Preparedness Canada. (2006). Incident Analysis: Ontario–U.s. Power Outage—Impacts On Critical Infrastructure, Number: Ia06-002. Retrieved From: Http://Cip.management.dal.ca/Publications/Ontario%20-%20Us%20Power%20Outage%20-%20Impacts%20On%20Critical%20Infrastructure.pdf

Rinaldi, S. M., Peerenboom, J. P., & Kelly, T. K. (2001). Identifying, Understanding, And Analyzing Critical Infrastructure Interdependencies. Ieee Control Systems, 21(6), 11-25. Retrieved From: Http://Www.ce.cmu.edu/~Hsm/Im2004/Readings/Cii-Rinaldi.pdf

Smedts, B. (2010). Critical Infrastructure Protection Policy In The Eu: State Of The Art And Evolution In The (Near) Future. Royal High Institute For Defence, Center For Security And Defence Studies Focus Paper 15. Retrieved From: Http://Www.irsd.be/Website/Images/Livres/Focuspaper/Fp15.Pdf

Standard & Poor's Ratings Services. (2015). "The Heat Is On: How Climate Change Can Impact Sovereign Ratings", Ratings Direct, 25 November.

Stanford University, Civil And Environmental Engineering. Performance Based Engineering. Retrieved From: Https://Cee.stanford.edu/Programs/Structural-Engineering-Geomechanics/Research/Performance-Based-Engineering

Stangl, R., Siedschlag, A., Silvestru, D., Fritz, F., And Jerković, A. (2012). Comprehensive Security Research To Contribute To Critical Infrastructure Protection: Contributions To Security Governance In Disaster Risk Reduction. 12Th Congress Interpraevent 2012 – Grenoble / France Conference Proceedings. Retrieved From: Http://Www.interpraevent.at/Palm-Cms/Upload_files/Publikationen/Tagungsbeitraege/2012_1_585.Pdf

Swedish Civil Contingencies Agency (Msb). (July, 2014). Action Plan For The Protection Of Vital Societal Functions & Critical Infrastructure. Retrieved From: Https://Www.msb.se/Ribdata/Filer/Pdf/27412.Pdf

Taucer, F., Alarcon, J. And So, A. (2009). 2007 August 15 Magnitude 7.9 Earthquake Near The Coast Of Central Peru: Analysis And Field Mission Report. Bull Earthquake Eng (2009) 7: 1. Retrieved From: Http://Link.springer.com/Article/10.1007%2Fs10518-008-9092-3

The Guardian (2017). Chile battles devastating wildfires: 'We have never seen anything on this scale'. Retrieved from: https://www.theguardian.com/world/2017/jan/25/chile-fire-firefighting-international-help

The Economist (2011). Colombia's floods: That damned Niña. Retrieved from: http://www.economist.com/node/21541419

Theocharidou, M. And Giannopoulos, G. (2015). Risk Assessment Methodologies For Critical Infrastructure Protection. Part Ii: A New Approach. European Commission, Joint Research Centre (Jrc), Institute For The Protection And Security Of The Citizen. Retrieved From: Http://Publications.jrc.ec.europa.eu/Repository/Bitstream/Jrc96623/Lbna27332enn.pdf

Theoharidou, M., Kotzanikolaou, P., And D. Gritzalis (2009). Risk-Based Criticality Analysis. In International Conference On Critical Infrastructure Protection (Pp. 35-49). Springer Berlin Heidelberg.

Tierney, K., And Bruneau, M. (2007) Conceptualizing And Measuring Resilience: A Key To Disaster Loss Reduction. Transportation Research Board, Tr News 250, May - June 2007. Retrieved From: Http://Onlinepubs.trb.org/Onlinepubs/Trnews/Trnews250_p14-17.Pdf

U.S. Department of Homeland Security (2013) National Infrastructure Protection Plan: Partnering for Critical Infrastructure Security and Resilience. Retrieved from: https://www.dhs.gov/publication/nipp-2013-partnering-critical-infrastructure-security-and-resilience

U.S. Department of Homeland Security (2014). Forging a Common Understanding for Critical Infrastructure, Shared Narrative. Retrieved from: https://www.dhs.gov/sites/default/files/publications/critical-five-shared-narrative-critical-infrastructure-2014-508.pdf

U.S. Department of Homeland Security (n.d.). Protective Security Advisors. Retrieved from: https://www.dhs.gov/protective-security-advisors

U.s.-Canada Power System Outage Task Force. (2004). Final Report On The August 4, 2003 Blackout In The United States And Canada: Causes And Recommendations. Retrieved From: Http://Energy.gov/Sites/Prod/Files/Oeprod/Documentsandmedia/Blackoutfinal-Web.pdf

United Kingdom, Cabinet Office. (2010). Strategic Framework And Policy Statement On Improving The Resilience Of Critical Infrastructure To Disruption From Natural Hazards. Retrieved From: Https://Www.gov.uk/Government/Uploads/System/Uploads/Attachment_data/File/62504/Strategic-Framework.pdf

United Kingdom, Cabinet Office. (2011). Keeping The Country Running: Natural Hazards And Infrastructure – A Guide To Improving The Resilience Of Critical Infrastructure And Essential Services. Retrieved From: Https://Www.gov.uk/Government/Uploads/System/Uploads/Attachment_data/File/61342/Natural-Hazards-Infrastructure.pdf

United Kingdom, Cabinet Office. (April, 2016). Summary Of The 2015-16 Sector Resilience Plans. Retrieved From: Https://Www.gov.uk/Government/Uploads/System/Uploads/Attachment_data/File/526351/2015_16_Summary_of_the_srp.pdf

United Nations (Un). (2015). Sendai Framework For Disaster Risk Reduction 2015-2030, United Nations. Http://Www.preventionweb.net/Files/43291_Sendaiframeworkfordrren.pdf

United Nations Office For Disaster Risk Reduction (Unisdr). (2008). Links Between Disaster Risk Reduction, Development And Climate Change. Retrieved From: Https://Www.unisdr.org/We/Inform/Publications/8383

Usgs (2007). Usgs Earthquake Hazards Program. Poster Of The Ica, Peru Earthquake Of 15 August 2007 - Magnitude 8.0. Retrieved From: Http://Earthquake.usgs.gov/Earthquakes/Eqarchives/Poster/2007/20070815.Php

Usgs (2016). Usgs Earthquake Hazards Program. Poster Of The Coastal Ecuador Earthquake Of 16 April 2016 - Magnitude 7.8. Retrieved From: Https://Earthquake.usgs.gov/Earthquakes/Eqarchives/Poster/2016/20160416.Php

Victoria, Australia State Government. (December, 2012). A Roadmap For Victorian Critical Infrastructure Resilience. Retrieved From: Http://Pandora.nla.gov.au/Pan/143319/20131029-1113/A_roadmap_for_victorian_critical_infrastructure_resilience.pdf

Wiseman, E. And Mclaughlin, T. (March, 2014). Critical Infrastructure Protection And Resilience Literature Survey: State Of The Art. Department Of National Defence Of Canada Contract Report Drdc-Rddc-2015-C160. Retrieved From: Http://Cradpdf.drdc-Rddc.gc.ca/Pdfs/Unc200/P801837_a1b.pdf

World Bank, Water And Sanitation Program. (2011). Economic Impact Of The 2007 Earthquake In Peru On The Drinking Water And Sanitation Sector: Full Study. Retrieved From: Https://Www.wsp.org/Sites/Wsp.org/Files/Publications/Wsp-Lac-Economic-Impact-Earthquake-Full-Study.pdf

World Bank. (2012). Disaster Risk Management In Latin America And The Caribbean Region: Gfdrr Country Notes. Retrieved From: Http://Www.gfdrr.org/Sites/Gfdrr.org/Files/Drm_lac_countryprograms.pdf

World Economic Forum (Wef) And Boston Consulting Group (Bcg). (2013). Strategic Infrastructure Steps To Prepare And Accelerate Public-Private Partnerships. Retrieved From: Http://Www3.Weforum.org/Docs/Af13/Wef_af13_strategic_infrastructure_initiative.pdf

Zaballos, A. G. And Jeun, I. (2016). Best Practices For Critical Information Infrastructure Protection (Ciip): Experiences From Latin America And The Caribbean And Selected Countries. Idb And The Korea Internet And Security Agency (Kisa). Retrieved From: Https://Publications.iadb.org/Handle/11319/7848

Zapata, N, (2016). *Caso peruano la gestión de riesgos en contexto de cambio climático en la inversión pública* [The case of risk management in the context of climate change in public investments in Peru]. Retrieved from: http://idbdocs.iadb.org/WSDocs/getDocument.aspx?DOCNUM=40723173

www.iadb.org