2. Governance challenges for critical infrastructure resilience

This chapter reflects upon the changing context for critical infrastructure policies and presents a series of governance challenges for policy design and implementation in this area. Addressing the increased interdependencies and complexity of critical infrastructure requires a shift from protection of individual assets to a system' approach to resilience. This chapter proposes a series of building blocks to adopt such system's approach and discusses the roles of governments and infrastructure stakeholders in critical infrastructure resilience. It concludes by highlighting governance challenges that policy-makers need to overcome to adjust critical infrastructure policies to the dynamic risk landscape of our time.

From critical infrastructure protection to resilience

Rising uncertainties require more adaptive critical infrastructure policies

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. A new approach appeared necessary given the rising costs of disasters, large-scale terrorist attacks such as the 9/11 attacks in 2001 in the United States, the 2005 London bombings, and increasingly frequent cyber-attacks targeting critical infrastructures. Governments began to shift the focus from critical infrastructure protection to critical infrastructure resilience in order to adjust these policies to this changing risk landscape (Critical Five, 2014[34]).

The resilience focus does not preclude protection, or security considerations. It rather broadens the lens of critical infrastructure frameworks by integrating concepts such as adaptability, flexibility and robustness (Flynn, 2008[35]) (Barami, 2013[36]). 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 to prevent critical infrastructure disruptions altogether.

The shift towards a resilience-based perspective is prompted by the considerable degree of uncertainty about the intensity and the complexity of future disasters and their potential impacts on infrastructure. For instance, uncertainties around climate change have to be factored in, when long-term infrastructure investments are planned and when measures associated with the continuity of their services are designed. The nature of the uncertainties surrounding disaster events requires incremental approaches that prepare assets and systems with capacities to be restored and rehabilitated swiftly.

Defining critical infrastructure resilience

Resilience can be defined as the capacity of critical infrastructure to absorb a disturbance, recover from disruptions and adapt to changing conditions, while still retaining essentially the same function as prior to the disruptive shock (OECD, 2014[20]); (Chang et al., 2014[37]). This definition includes the indispensable ability to withstand shocks without loss of functionality, limiting the duration of service interruption as well as minimising the recovery time.

Thus, when a shock occurs, on can measure resilience objectives for critical infrastructure on two dimensions: limiting the extent of the damages, and limiting the duration of the service interruption caused by the damages. It is important to note that recovery does not necessarily mean resuming to exactly the prior state before the shock, but may involve changing, adapting to new conditions and improving systems' functionality overtime.

In this context, ensuring the resilience of critical infrastructures is done by ensuring the combination of several key qualities (OECD, 2011[9]):

- *Robustness* describes the ability to keep operating or to remain standing in the face of disaster. This entails designing structures or systems, which are strong enough to sustain a foreseeable shock. It also entails investing in and maintaining elements of critical infrastructure so that they can withstand low probability but high-consequence events.

- *Redundancy* describes the ability to keep operating through a substitute or redundant systems that can be brought to bear should something important break down or stop working.
- *Resourcefulness* describes the ability to manage skilfully a shock event as it unfolds. This includes identifying options, prioritising what should be done both to control damage and to begin mitigating it, and communicating decisions to the people who will implement them. Resourcefulness depends primarily on people, not on technology. Rapid recovery is the capacity to get things back to normal as quickly as possible after a disaster. Contingency and business continuity plans, efficient emergency services, and the means to get the right people and resources to the right places are crucial.
- *Adaptability* describes the means to absorb new lessons that can be drawn from a catastrophe. It involves revising plans, modifying procedures, and introducing new tools and technologies needed to improve robustness, resourcefulness, and recovery capabilities before the next crisis.

International frameworks supporting critical infrastructure resilience

Based on this definition, public policies to enhance the resilience of critical infrastructure should combine measures to incentivise redundancies, system robustness, back-up capacity, rapid recovery and adaptability to new risks or changing risk factors. The OECD Recommendation on the Governance of Critical Risks recognises the importance of achieving critical infrastructure resilience to strengthen risk governance at the national level and reduce knock-on and cascading impacts from disaster events (OECD, 2014[1]). To achieve this goal, the Recommendation calls on governments:

- To identify where disruptions to critical infrastructure and supply chains could lead to knock-on effects across sectoral and geographic borders, and produce cascading effects.
- To develop fiscal and regulatory options that promote reserve capacity, diversification or back-up systems to reduce the risk of breakdowns and prolonged periods of disruption in critical infrastructure systems.
- To coordinate design of critical infrastructure networks (e.g. energy, transportation, telecommunications and information systems) with urban planning and territorial management policies.
- To leverage private sector capabilities in building resilient infrastructure.
- To encourage businesses to take steps to ensure business continuity, with a specific focus on critical infrastructure operators by developing standards and toolkits designed to manage risks to operations or the delivery of core services.
- To ensure that critical infrastructure, information systems and networks still function in the aftermath of a shock.
- To ensure first responders maintain and exercise emergency plans in case of a shock event that disrupts the functioning of critical infrastructure networks.

Following the adoption of the OECD Recommendation on the Governance of Critical Risks in 2014, several international fora gave recognition to the importance of infrastructure resilience. The G7 Ise-Shima Principles for Promoting Quality Infrastructure Investments (G7, 2016[38]) emphasizes resilience against natural hazards, terrorism and cyber-attack

risks to ensure reliable operation and economic efficiency in view of life-cycle cost. Similarly, the UN Sendai Framework for Disaster Risk Reduction (United Nations Office for Disaster Risk Reduction, 2015[39]) calls countries to "substantially reduce disaster damage to critical infrastructure and disruption of basic services" and the UN Sustainable Development Goal 9 to build resilient infrastructure. Regarding specifically terrorism, the UN Security council Resolution 2341 recognised the "growing importance of ensuring reliability and resilience of critical infrastructure and its protection from terrorist attacks for national security, public safety and the economy of the concerned States as well as wellbeing and welfare of their population" (United Nations Security Council, 2017[40]). The overarching OECD Framework on the Governance of Infrastructure (OECD, 2017[11]) also highlights infrastructure resilience as one if its 10 key governance challenges.

Adopting a system's approach to critical infrastructure resilience

The shift from critical infrastructure protection to resilience aims to address key changes of the risk landscape, marked by increased uncertainties. In order to better integrate the complexity, interdependencies and interconnectedness of critical infrastructure, adopting a systemic approach to critical infrastructure resilience provides complementary perspectives.

Barami (2013) emphasises 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[36]).

The OECD High-Level Risk Forum workshop on "System-thinking for Critical Infrastructure resilience" (OECD and EU JRC, 2018[41]), extended this notion of system approach applied to critical infrastructure resilience, and proposed a series of key attributes that public policies should consider in this area:

- *All-hazards and threats*: Single-hazard policies are not sufficient to build infrastructure resilience. The critical infrastructure impacts of Superstorm Sandy in New York, which had engaged in substantial protection activities following 9/11 demonstrated that protective activities alone are not sufficient to address the range of potential critical infrastructure disruptions and associated cascading risks. Adopting an all-hazard and threat approach to critical infrastructure resilience enables policy makers and operators to better prepare for the unexpected.
- *System-level*: Initially, critical infrastructure protection policies focused primarily on setting up protection measures at asset-level. However infrastructure assets are usually only the components of a wider complex system, which should be considered in its entirety in a comprehensive resilience strategy. Some of the system's assets are more critical than others, because of dependencies or (non)-existing redundancies for instance. A system approach allows for prioritising the most critical components, through dependency modelling and criticality assessments, as well as to address weak points that otherwise create critical vulnerabilities for the entire system.

- *Multi sectoral*: Addressing interdependencies requires policy makers and operators to go beyond a system-level approach and to target the critical infrastructure sectors together in a comprehensive resilience policy. While infrastructure operators tend to be well aware of their own dependencies upon critical sectors (e.g.: electricity, payment systems), they may not be as conscious of the dependencies others have upon their own services. From interdependency mapping to developing shared business continuity objectives, a multi-sectoral approach is essential to a comprehensive critical infrastructure resilience policy.
- *Transboundary dimension*: Similarly, interdependencies and interconnectedness cannot be fully understood without incorporating their international dimension. Hazards and threats do not stop at national borders. In some cases, critical infrastructure systems cross borders, providing services in multiple countries. Infrastructure operators can also manage critical infrastructure in several countries. This makes it more compelling to integrate international cooperation in critical infrastructure resilience policies. Sharing good practices, adopting common approaches, developing joint standards in critical infrastructure resilience are among the policy options that can foster international cooperation in this area.
- *Life cycle approach*: Different resilience and security measures can apply to the different phases of the infrastructure life-cycle: integrating robustness and redundancies requires investments in the design phase, while developing business continuity planning pertains more to the operation phase and adaptability can be based on infrastructure retrofitting. Thus, it is important to set-up a comprehensive policy that enables resilience throughout the life cycle of critical infrastructures, with applications from the design phase to its operations and maintenance, and retrofitting.
- *Entire risk management cycle*: A comprehensive resilience policy should incorporate measures throughout the entire disaster risk management cycle, from risk assessment, over risk prevention, emergency preparedness and response, to recovery and reconstruction (Moteff, 2012[42]). Critical infrastructure resilience has specificities in each of these phases. Risk assessment should incorporate dependencies and criticality assessment. Risk prevention includes robustness measures in the design phase as well as dedicated awareness raising dialogues with infrastructure operators. Emergency preparedness and response required tailored warning systems, business continuity measures and back-ups, and dedicated emergency teams and capabilities. The recovery and reconstruction phase should integrate degraded mode, rapid restoration plans as well as dedicated financing schemes, including for building back better.
- *Risk-based and layered approach*: Given the considerable degree of uncertainty about the intensity and the complexity of future disasters, the manifold dimensions of vulnerability of infrastructure systems, and all the interrelationships between these systems, the prioritisation of resilience measures is essential. Only a risk-based and layered approach can account for complex infrastructures interdependencies, while considering potential solutions applicable through the infrastructure systems across the life-cycle (Barami, 2013[36]).

Governance challenges for critical infrastructure resilience policies

The multiple stakeholders for infrastructure resilience

Infrastructure design, investment, construction, ownership, operations or regulation involve multiple stakeholders, which all have a role to play in building resilience. As

identified in the OECD Framework for better Governance of Infrastructure (OECD, 2017[11]), there are many ways to provide infrastructure services. The public sector's role can vary and hybrid forms exist. With infrastructure ownership moving from government provision through state-owned enterprises to privatisation in the last decades, government's control over infrastructure assets goes decreasing. Similarly, the mode of infrastructure delivery, from traditional public procurement to concessions or public-private partnerships, will influence how resilience can be integrated in infrastructure design and operations. In this context, risk governance and resilience become intrinsically linked to the broader issue of infrastructure governance and policy-making. With the current trends towards increased global investments in infrastructure, making sure resilience investments are adequately scaled requires that infrastructure governance models make resilience one of the decision-making criteria.

Critical infrastructure owners and operators bear the primary responsibility for protecting their assets and maintaining the continuity of the services they provide. Be they public, private or of a hybrid form, owners would normally want to protect their capital asset against suffering damages or destruction from a disaster, or another shock event. Similarly, operators have a strong interest in maintaining the continuity of their services and avoid disruptions, not only because of the losses they can potentially suffer when services stop, but also because they are concerned with their reputation and image towards their clients or users. Nevertheless, owners and operators cannot address all their vulnerabilities on their own and may not have incentives to assess a complete overview of the full extent of their interdependencies. Interdependencies between critical infrastructure sectors and the potential cascading effects that may follow in case of disaster require cooperation across sectors.

Which role for governments?

Governments have a key role to play in critical infrastructure resilience, as responsible to provide security and safety to citizens, but also as an infrastructure policy-maker, and regulator, owner or operator in some cases, and major user or client. Officials in charge of the governance of critical risks have to coordinate across several functions in government and ensure that, on behalf of the general interest, all relevant policy objectives can be achieved at the same time, balancing the relevant trade-offs. This list highlights the manifold dimensions that governments need to incorporate in the design of their national critical infrastructure security and resilience policy.

First, as stated in the OECD Recommendation on the Governance of Critical Risks, governments have the responsibility to set the preparedness levels at the nation scale, as part of their national strategy for the governance of critical risks. In the new landscape of critical risks that governments are confronted to, setting up national objectives for critical infrastructure security and resilience is fundamental to contribute to the overall resilience of nations. Most OECD countries have now set-up critical infrastructure security and resilience strategies and programmes (see Chapter 3). In light of the interdependencies between the different infrastructure sectors, government has also an important role to play in guaranteeing that these interdependencies are properly disclosed and addressed, as well as to avoid related policy loopholes.

Second, governments have a key role in infrastructure policy-making and oversight. Making sure that infrastructure contributes best to productivity and ensures equal opportunities and equal access to services for citizens are key policy objectives for infrastructure delivery (OECD, 2017[11]). Government's oversight and regulatory function

can be delegated to a sectoral regulator, who will have the mandate to set-up key objectives and to regulate the operations in the sector. In this respect, the concern for resilience and the need to ensure sufficient reserve capacity, may have to be balanced with the need to maintain a level playing field and instil competition to drive prices down and improve consumer surplus, while not jeopardizing the acceptable level of risk.

Third, government can be an infrastructure owner and operator, either through direct provision, state owned enterprises, or other modes of infrastructure services. By applying resilience and security standards to the infrastructure systems that it is responsible for, government can lead the way as a role model. This can also be revealing for government on the costs incurred for resilient investments, which can potentially better inform decision-making and related cost-benefit analyses for critical infrastructure resilience investments.

Finally, governments are also infrastructure users or clients, and therefore depend upon various critical infrastructure to maintain their own continuity. As such, governments have specific expectations for the continuity of critical infrastructure underpinning government's key functions. Some countries for instance have designated government as one of the critical infrastructures sectors in their policy. A question for governments in the design of their critical infrastructure policy is whether its own continuity would request some specific resilience levels and/ or standards for critical infrastructure resilience compared to other sectors.

Partnering for critical infrastructure resilience and related governance challenges

Although governments continue to own, invest in, operate and regulate critical infrastructure in some sectors, an increasing share of critical infrastructure is either privately owned or operated. In some countries, the private sector operates most of these infrastructure systems. Therefore, the resilience of these systems depends upon governments partnering with infrastructure operators from the public and private sectors in resilience efforts through the establishment of relevant governance arrangements.

Critical infrastructure operators and governments often agree on the need to protect key assets and maintain their services, but views can differ on the level of security resilience required, the means to achieve it, and the requirements that should apply. Policy issues to be addressed include the criticality of specific installations to the broader network, maintenance of a level playing field between operators, the acceptable duration of 'down time', the distribution of costs to different stakeholders in paying for resilience and circumventing potential situations of free-riding.

Policy approaches that are limited to mandatory measures requiring critical infrastructure operators to put resilience measures in place are not always the most appropriate, as it can, among other issues, become a problem of competition and willingness and ability to pay by the providers. Complementary governance approaches that foster regular exchanges, information sharing, mutual trust, and potentially balanced public financial support for investments in critical infrastructure resilience can potentially lead to better outcomes when carefully designed. An effective collaboration between the government and critical infrastructure providers to develop and implement the policy should enable government services to more effectively fulfil their tasks (such as monitoring, early warning, prevention investment or emergency response) but in a way that does not compromise the private sector interests, including confidentiality.

Establishing partnerships between governments and operators (public and private) to encourage dialogue on these issues is a useful approach to jointly build critical infrastructure resilience and security policies, and implement them. In any case, such dialogue will have to provide solutions to overcome the following governance challenges for critical infrastructure security and resilience:

- *Establishing trust* : critical infrastructure operators may not always be willing to share information on their vulnerabilities to hazards and threats with the government, as well as with other operators that depend on them or *vice-versa*
- *Security of information-sharing*: ensuring that information on vulnerability as well as on resilience investments by infrastructure operators remains confidential is a key aspect, especially in competitive sectors.
- *Cost-sharing mechanisms*: another important aspect, from an economic standpoint, will be to know at which "price" resilience can be achieved and who will pay for resilience investments.
- *International cooperation*: in light of the transboundary dimension of critical infrastructure systems, governance mechanisms must include an international dimension.
- *Rapid changes and advancements in technology*: with the rapid pace of innovation in many infrastructure sectors, strengthening their resilience requires adapted solutions, as classic regulations might not be able to keep up with innovations.

References

Barami, B. (2013), *Infrastructure Resiliency: A Risk-Based Framework*, US Department of Transportation, https://www.volpe.dot.gov/sites/volpe.dot.gov/files/docs/Infrastructure%20Resiliency_A%20Risk-Based%20Framework.pdf (accessed on 25 February 2019). [36]

Chang, S. et al. (2014), "Toward Disaster-Resilient Cities: Characterizing Resilience of Infrastructure Systems with Expert Judgments", *Risk Analysis*, Vol. 34/3, pp. 416-434, http://dx.doi.org/10.1111/risa.12133. [37]

Critical Five (2014), *Forging a Common Understanding for Critical Infrastructure Shared Narrative*, https://www.dhs.gov/sites/default/files/publications/critical-five-shared-narrative-critical-infrastructure-2014-508.pdf (accessed on 25 February 2019). [34]

Flynn, S. (2008), "America the Resilient, Defying Terrorism and Mitigating Natural Disasters", *Foreign Affairs*, https://www.foreignaffairs.com/articles/2008-03-02/america-resilient (accessed on 25 February 2019). [35]

G7 (2016), *G7 Ise-Shima Leaders' Declaration*, https://www.mofa.go.jp/files/000160266.pdf (accessed on 25 February 2019). [38]

Moteff, J. (2012), *CRS Report for Congress Critical Infrastructure Resilience: The Evolution of Policy and Programs and Issues for Congress*, Congressional Research Service, https://fas.org/sgp/crs/homesec/R42683.pdf (accessed on 25 February 2019). [42]

OECD (2017), *Getting Infrastructure Right: A framework for better governance*, OECD Publishing, Paris, https://dx.doi.org/10.1787/9789264272453-en. [11]

OECD (2014), *Boosting Resilience through Innovative Risk Governance*, OECD Reviews of Risk Management Policies, OECD Publishing, Paris, https://dx.doi.org/10.1787/9789264209114-en. [20]

OECD (2014), *Recommendation of the Council on the Governance of Critical Risks*, http://www.oecd.org/gov/risk/Critical-Risks-Recommendation.pdf (accessed on 25 February 2019). [1]

OECD (2011), *Future Global Shocks: Improving Risk Governance*, OECD Reviews of Risk Management Policies, OECD Publishing, Paris, https://dx.doi.org/10.1787/9789264114586-en. [9]

OECD and EU JRC (2018), *System thinking for critical infrastructure resilience and security - OECD/ JRC Workshop - OECD*, http://www.oecd.org/gov/risk/workshop-oecd-jrc-system-thinking-for-critical-infrastructure-resilience-and-security.htm (accessed on 25 February 2019). [41]

United Nations Office for Disaster Risk Reduction (2015), *Sendai Framework for Disaster Risk Reduction 2015 - 2030*, https://www.unisdr.org/files/43291_sendaiframeworkfordrren.pdf (accessed on 25 February 2019). [39]

United Nations Security Council (2017), *Security Council Resolution 2341 - Threats to international peace and security caused by terrorist acts*, http://unscr.com/en/resolutions/2341 (accessed on 25 February 2019). [40]