5. Policy Toolkit on Governance of Critical Infrastructure Resilience

This chapter presents the OECD Policy Toolkit on Governance of Critical Infrastructure Resilience that can inspire governments' policy reforms towards improved continuity of these essential services. Developed in the context of the OECD High-Level Risk Forum, this Toolkit provides a comprehensive policy framework to strengthen critical infrastructure resilience and overcome related governance challenges. The Toolkit emphasizes the importance of adopting a system approach for critical infrastructure resilience, based on partnerships between governments and critical infrastructure operators.

Context for the development of the OECD Policy Toolkit

This chapter presents the OECD Policy Toolkit on Governance of Critical Infrastructure Resilience, developed through the OECD High-Level Risk Forum (HLRF). The HLRF brings together government officials to identify and share good practices in deepening the understanding of emerging and complex risks, and to share good practices in their governance and management. It invites experts from the private sector, civil society, think tanks and academia to identify gaps in risk governance and to explore solutions to current and future challenges. The HLRF takes an inclusive approach to policy analysis, which reflects its suggested best practice as embodied in the OECD Recommendation on the Governance of Critical Risks, adopted by the OECD Council in 2014 (OECD, 2014[1]).

Due to the high economic costs and social harms that disruptions to critical infrastructure produce, the OECD Recommendation underlines the importance for governments to reinforce resilience and security in critical infrastructure networks. In 2016, the OECD conducted a survey to take stock of implementation of the OECD Recommendation by Adherents. The survey results revealed that a major hurdle to implementation of the Recommendation is sharing responsibility between governments and businesses to protect critical infrastructure assets and ensure quick restoration of service (OECD, 2018[2]).

To address this challenge, the High-Level Risk Forum called for the OECD to conduct research and develop a good practice report on how governments and businesses can structure effective partnerships in building more secure and resilient critical infrastructure. Further to this call, the OECD ran a cross-country survey on critical infrastructure resilience, organized thematic workshops, conducted regional research projects and pilot country case-studies, and contributed to relevant OECD multidisciplinary activities. These activities helped deepen the evidence base on critical infrastructure resilience presented in this report and extend the OECD network of policymakers with responsibility for critical infrastructure, as well as regulators, operators from the public and private sectors and researchers working on this topic.

The process began with a stocktaking report, which was discussed at the High-Level Risk Forum in 2017 and constitutes the basis of this report. The Forum agreed for OECD to organise a dedicated workshop on "System-thinking for Critical Infrastructure Resilience and Security" in partnership with the European Commission's Joint Research Centre (OECD and EU JRC, 2018[41]). The workshop took place on 23-24 September 2018 with a focus on tools, methodologies and data requirements to assess system's resilience and on the policy instruments that governments can mobilise for critical infrastructure resilience. Participants suggested that the OECD High-Level Risk Forum develop a "Policy Toolkit on Governance of Critical Infrastructure Resilience" based on the workshop's discussions and OECD analysis.

Policy challenges for critical infrastructure resilience

Recent shock events caused by natural hazards, industrial accidents, cyber-threats, or other security risks, illustrate how disruptions to key systems and essential services, such as water, energy, transport or information and telecommunication systems can result in substantial economic damage, in addition to loss of lives in some cases. The interconnectedness of supply chains, technological and financial systems, which form the foundation of the global economy, increases critical infrastructure exposure and vulnerability to such unanticipated events, yielding negative impacts across sectors and borders, which at times can resonate globally. This hyper-connectivity between

infrastructure assets, sectors and countries calls for comprehensive public policies to strengthen critical infrastructure resilience and limit the risk of disruptions of the essential services they provide.

Beginning in the 2000s, several governments established public policies to promote protection of critical infrastructure and actions to implement them. Generally, these include an effort to define critical infrastructure sectors, the development of an inventory of critical infrastructure assets and adopting regulations, national programmes or incentive mechanisms to strengthen the resilience of these assets. However, critical infrastructure protection policies have not always proven to be sufficiently effective to address challenges of the 21st century risk landscape.

The diversity and complexity of shock events, the increased interdependences and interconnectedness, climate change, the fast pace of innovation that fundamentally transforms critical infrastructure sectors, as well as ageing infrastructure, are among the challenges with which critical infrastructure resilience policies have to contend. Many researchers on this topic conclude that a shift in focus from protection to resilience would help policymakers to better account for uncertainty by integrating concepts such as adaptability, flexibility and robustness into the design of critical infrastructure and their regulatory frameworks.

Following the adoption of the OECD Recommendation on the Governance of Critical Risks, several international fora gave recognition to the importance of infrastructure resilience. The G7 Ise-Shima Principles for Promoting Quality Infrastructure Investments emphasizes resilience against natural hazards , terrorism and cyber-attack risks to ensure reliable operation and economic efficiency in view of life-cycle cost (G7, 2016[38]). Similarly, the UN Sendai Framework for Disaster Risk Reduction calls countries to "substantially reduce disaster damage to critical infrastructure and disruption of basic services" (United Nations Office for Disaster Risk Reduction, 2015[39]). The OECD Framework on the Governance of Infrastructure also highlights infrastructure resilience as one if its 10 key governance challenges (OECD, 2017[11]).

Today there is strong demand for practical policy guidance to enhance resilience throughout the life-cycle of critical infrastructure. Governments and infrastructure stakeholders are facing key governance challenges when it comes to investing in resilience and designing relevant policies. Evidence-based guidance and the sharing of good practices across countries can provide useful insights in response to challenging questions such as:

- What is the proper role for governments in boosting critical infrastructure resilience?
- How can governments effectively engage critical infrastructure operators – public and private – in strengthening their resilience efforts?
- What are the most appropriate mechanisms to share sensitive information about risks, vulnerabilities, and resilience measures between government and operators?
- How to share costs and benefits of investing in resilience between governments, operators and end-users?

The recent increase of infrastructure investments globally, digitalisation and a changing risk landscape provide opportunities to rethink critical infrastructure policies across OECD countries and beyond, and to integrate resilience in upfront planning and designs.

Box 5.1. System approach for critical infrastructure policies

To shift from a protection centric strategy to one that emphasizes resilience, critical infrastructure policies need to feature the following qualities from a system-thinking perspective:

- **All-hazards and threats**: Single-hazard policies are not sufficient to build infrastructure resilience. An all-hazards and threats forward-looking approach to critical infrastructure resilience and security enables policy makers and operators to better prepare for the unexpected.
- **System-level**: Infrastructure assets are usually only the components of a wider complex system, which should be considered in its entirety in a comprehensive resilience strategy. A system approach allows for prioritising the most critical components, and addresses weak points that create critical vulnerabilities for the entire system.
- **Multi-sectoral coordination**: Addressing interdependencies in policies requires policy makers and operators to go beyond a silo-based approach and to target the critical infrastructure sectors together. While operators tend to be well aware of their own dependencies upon critical sectors, they may not be as conscious of the dependencies others have upon their own services.
- **Public-private cooperation**: Although governments continue to own, invest in, and operate critical infrastructure in some sectors, a large share of critical infrastructure is either privately owned or operated. 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.
- **Life-cycle approach**: Different resilience measures may apply at different phases of the infrastructure life-cycle: robustness and redundancies requires investments in the design phase, while business continuity planning and maintenance pertains to the operations, and adaptability can be based on infrastructure retrofitting. Thus, it is important to set-up a comprehensive policy that enables resilience throughout infrastructure life-cycle.
- **Entire risk management cycle**: A comprehensive resilience policy should incorporate measures throughout the entire risk management cycle, from risk assessment, to risk prevention, emergency preparedness, response, recovery and reconstruction.
- **Risk-based and layered approach**: Given the considerable degree of uncertainty about future risks, the manifold dimensions of infrastructure systems vulnerability, and all the interrelationships between these systems, the prioritisation of resilience measures is essential. A risk-based and layered approach helps account for complex interdependencies, for all-hazards and across the infrastructure life-cycle.
- **Transboundary dimension**: Risks arising from interdependencies and interconnectedness cannot be fully mitigated without incorporating their international dimension. Fostering international cooperation is key to infrastructure resilience.

Objectives of the Policy Toolkit

The aim of the Policy Toolkit on Governance of Critical Infrastructure Resilience is to help governments design their national critical infrastructure resilience policies and implement them through effective partnerships with operators.

It proposes practical guidance, supported by country good practices and indicative benchmark indicators, which governments can use to:

- Identify critical infrastructure, map out (inter-)dependencies and prioritise the critical services and functions, systems, and assets, where investments in resilience and security are the most required.
- Forge effective partnerships with critical infrastructure operators to build mutual trust, share information on risks and vulnerabilities and agree on a common vision and policy objectives.
- Share responsibilities to protect critical infrastructure assets and ensure quick restoration of service.

The Policy Toolkit proposes that governments adopt a system approach to critical infrastructure resilience, i.e. their policies should address all-hazards and threats, ensure multi-sectoral coordination and public-private cooperation, integrate planning for the whole infrastructure life-cycle, target measures across the risk management cycle and foster transboundary cooperation (Box 5.1).

Going forward, the OECD will work with the High-Level Risk Forum to support countries' implementation of this Policy Toolkit and benchmark their progress in increasing the resilience of critical infrastructure.

Policy toolkit on governance of critical infrastructure resilience

Definitions

It proposes to use the following definitions:

- **Critical infrastructure**: Critical infrastructure are systems, assets, facilities and networks that provide essential services for the functioning of the economy and the safety and well-being of the population. While definitions of critical infrastructure differ across countries, this definition is not prescriptive and aims to encompass the largest set of definitions identified in the OECD Survey on Critical Infrastructure Resilience.
- **Resilience**: the capacity of systems to absorb a disturbance, recover from disruptions and adapt to changing conditions while retaining essentially the same function as prior to the disruptive shock (adapted from OECD, 2014[20]). This definition includes the ability to withstand shocks with as little loss of functionality as possible under the specific circumstances, limiting the duration of potential service interruption by minimising the recovery time, as well as adapting to new conditions and improving systems' functionality.

Seven steps for critical infrastructure resilience policies

To strengthen critical infrastructure resilience, a comprehensive policy framework should address the following seven interrelated governance challenges:

1. Setting up a multi-sector governance structure for critical infrastructure resilience
2. Understanding complex interdependencies and vulnerabilities across infrastructure systems to prioritise resilience efforts
3. Establishing trust between government and operators by securing risk-related information-sharing
4. Building partnerships to agree on a common vision and achievable resilience objectives
5. Defining the policy mix to prioritise cost-effective resilience measures across the life-cycle
6. Ensuring accountability and monitoring implementation of critical infrastructure resilience policies
7. Addressing the transboundary dimension of infrastructure systems

1. Setting up a multi-sector governance structure for critical infrastructure resilience

Governments should adopt a whole-of-government approach to critical infrastructure resilience. Ideally, such governance would involve the sectoral ministries and agencies overseeing infrastructure delivery and regulation in the multiple critical sectors, as well as those in charge of resilience to all-hazards and threats. Coordination at the Center-of-Government would allow to manage the interests of all stakeholders and make the relevant trade-offs for effective resilience policies.

Why is this important?

Governments have a key role to play in critical infrastructure resilience. They have a responsibility to provide security and safety to citizens, and are often infrastructure regulators. Governments, at central or sub-national level, can also be owners and operators of critical infrastructure, either directly or through publicly owned companies. Furthermore, investments in major infrastructure are often dependent upon major public funds. Finally, governments are also an important user or client of critical infrastructure, with expectations on their reliability for the continuity of government activities.

This presents governments with multiple and complex roles, across critical infrastructure sectors and for multiple hazards and threats. Risk managers and 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, policy objectives can be achieved from a resilience perspective while balancing the relevant trade-offs.

Key policy questions:

- *Is there a national strategy or policy document for critical infrastructure resilience?*
- *Is there a definition for critical infrastructure?*
- *Is a pre-defined list of critical infrastructure sectors in place?*
- *Is there a whole-of-government approach to the development of critical infrastructure resilience?*
- *Are all relevant hazards and threats considered in the critical infrastructure resilience policy?*

- *Is there a dedicated coordination entity responsible for designing, monitoring and adjusting the national critical infrastructure resilience policy?*

Benchmark indicators

- *National policy on critical infrastructure resilience*
- *Inter-departmental / ministerial committee / platform to design CI resilience policies*
- *Coordination entity at the Center of Government*

Examples of good practices

- *In the United States, the Presidential Policy Directive on Critical Infrastructure Security and Resilience tasks the Department of Homeland Security to coordinate CI policies at Federal level with sector agencies across 16 CI sectors.*
- *In France, the General Secretariat for Defense and National Security under the Prime Minister coordinates the CI resilience policy across 8 line Ministries for 12 infrastructure sectors and with a multi-hazard approach*.

2. Understanding complex (inter-)dependencies and vulnerabilities across critical infrastructure systems to prioritise resilience efforts

Governments should adopt methodologies and metrics to identify the critical functions, systems and assets that should be prioritised for investments in building resilience. This requires a good understanding of how disruptions can affect infrastructure assets and where dependencies and interdependencies are found that could amplify their impacts. Once priority nodes and hubs are identified across interdependent systems, there is a need to assess their resilience with relevant indicators and to compare actual and expected results to see where the gaps are.

Why is this important?

Defining methodologies for risk assessment that critical infrastructure stakeholders from government and operators can use in practice and clarifying the related data requirements are fundamental steps to prioritise investments in resilience. Understanding risks and vulnerabilities of critical infrastructures is a complex task, given the underlying interdependencies and requires a systemic view. A diverse set of tools exists to identify critical assets, understand their vulnerabilities to shock events and model the potential cascading impacts through interconnected networks. Recent research has focused on system complexity, risk modelling, and interdependency mapping, which provides rich analytical materials.

Nevertheless, governments and critical infrastructure operators are grappling with the need to choose the right tools for the identification of the most critical hubs and nodes of infrastructure systems and the assessment of their level of resilience. In practice, such analysis follows a three-tier approach, for which methodologies and tools need to be standardised. First, mapping the interdependencies (physical, digital, geographic, logical) between critical infrastructure assets and systems is key to estimating the full impact of service loss in case of disruption. Second, conducting a criticality assessment allows to classify systems, networks, and asset that are truly critical, based on the impact of their disruption on a range of pre-established criteria. Third, resilience analysis and stress-tests help identify weak points where potential failures are more likely to happen. Developing

relevant indicators for infrastructure assets and systems enables the best comparison of their level of resilience.

Key policy questions:

- *Is there a mapping of dependencies and interdependencies across the different critical infrastructure sectors?*
- *Are there defined criteria to assess the criticality of infrastructures?*
- *Are there multi-hazards stress tests conducted to identify weak points among critical infrastructure?*

Benchmark indicators

- *Identification of critical assets*
- *Existence of resilience indicators*

Examples of good practices

- *In the Netherlands, the National Coordinator for Security and Counterterrorism (NCTV) developed a 3-step methodology to first identify critical infrastructure and categorise them according to their criticality (A or B), second assess their vulnerabilities to multiple risks and third set priorities for resilience investments.*
- *Public Safety Canada (PSC) has undertaken high-level inter-dependency analyses of individual CI sectors with examination of cascading impacts. PSC is evaluating critical infrastructure inter-dependency modelling tools developed by the research community.*

3. Establishing trust between governments and operators and securing information-sharing on risks and vulnerabilities

Governments should establish information-sharing platforms with operators of critical infrastructure so that all relevant infrastructure stakeholders obtain a comprehensive and shared understanding of risks and vulnerabilities to conduct resilience analysis. It is crucial to ensure that the design of these platforms assures security and confidentiality of information shared with clear rules of access to allow a trusted sharing of sensitive information.

Why is this important?

Information exchange is fundamental for governments to gain a comprehensive understanding of critical infrastructure vulnerabilities. It also helps operators to understand their own vulnerabilities, their dependencies on other infrastructures, and how disruptions to their services could affect other infrastructures or even themselves.

The challenge to fostering information-sharing is to build trust between parties, such that the security and proprietary of information shared voluntarily will not be publicly disclosed. Operators are not inclined to share sensitive information about their vulnerabilities, their critical dependencies and any disruptive incidents outside of safe circles, as disclosure of certain information may lead to liability, be important for competitiveness in the market or do damage to a firm's reputation. On the government side, information-sharing may involve classified information when it relates to national security. Risks of cyber threats are another concern, as they can also increase reluctance to share information on joint platforms, if guarantees on their security are not properly assured.

In some cases, disclosure of risk information can strengthen operators' accountability and reinforce resilience measures, for climate-related risks for instance. In a world characterized by interconnected systems, the resilience of interdependent infrastructures is as strong as its weakest link. Therefore, information sharing significantly contributes to bringing infrastructure operators up to a similar understanding of what is required to reach an acceptable level of security and resilience.

Key questions:

- *Are there mandatory or voluntary legislation, regulations, and policies for information sharing about risks and vulnerabilities?*
- *Are there information-sharing platforms for governments and critical infrastructure operators?*
- *Are there incentives for infrastructure operators to share qualitative information about their dependencies and vulnerabilities with the policy community?*
- *Are there safeguards in place to secure the confidentiality of shared information?*

Benchmark indicators

- *Presence of a secured information sharing mechanism*
- *Frequency, quantity and quality of shared information from infrastructure operators*
- *Utilisation/satisfaction of the information sharing platform*

Examples of good practices

- The United Kingdom Data and Analytics Facility for National Infrastructure (DAFNI) provides *a platform of data, models and technical tools for complex infrastructure analysis to analyse system performance and make wise investments.*
- *Australia Trusted Information Sharing Network (TISN) for Critical Infrastructure provides national level forums for critical infrastructure operators to share vital information on risks and mitigation* strategies with in a secure, non-competitive environment, and to develop collective solutions to shared problems.

4. Building partnerships to agree on a common vision and achievable resilience objectives

Governments should partner with critical infrastructure operators from the public and the private sectors to agree on a common resilience vision for critical infrastructure nationwide and on shared and achievable resilience objectives. Developing an understanding of public expectations to potential loss of infrastructure service can be a useful way to initiate dialogue.

Why is this important?

Beyond information-sharing on risks and vulnerabilities, critical infrastructure resilience depends upon governments partnering with infrastructure operators from the public and private sectors in resilience efforts. While operators and governments agree on the need to protect critical assets and maintain their services, views can differ on the level of resilience required, the means to achieve it, and on the regulatory requirements that should apply. These measures have financial implications, and raise questions about who will take on additional costs to invest in resilience.

Establishing partnerships between governments and operators (public and private) to encourage dialogue on these issues is a useful approach to develop a common vision towards resilience in critical infrastructure and define shared objectives. Policy issues to be addressed include deciding on the acceptable duration of 'down time', maintaining a level-playing field between operators, and circumventing situations of free-riding in competitive sectors. Ensuring stakeholders' engagement, including with the public, in regular meetings, institutionalized dialogues, and joint exercises can foster consensus.

Key policy questions:

- *Are there institutionalised dialogues in place to engage critical infrastructure operators in resilience policy design?*
- *Are there processes in place to understand public expectations for critical infrastructure resilience?*
- *Is there a common vision of critical infrastructure resilience defined through multi-sector dialogue?*
- *Are there resilience objectives established to support the vision's implementation?*

Benchmark indicators

- Existence *of critical infrastructure stakeholders consultation fora*
- *Frequency of consultation fora and level of operator's participation*
- *Quality of the participatory* process

Examples of good practices

- In Switzerland, the national CIP strategy coordinated by the Federal Office for Civil Protection is based on partnerships and various platforms with CI operators, *federal and subnational authorities. Beyond risk analysis and information sharing, the CI Guideline is developed jointly and allows setting resilience objectives for CI operators.*
- *In Germany, the UP KRITIS is a National initiative between the state and carriers of Critical* Infrastructures for the protection of critical information infrastructures. The UP KRITIS consists of more than 450 associates.

5. Defining the policy mix to prioritise cost-effective resilience measures across the life-cycle

Governments should define a mix of policy tools to incentivize operators' investments in resilience and achieve shared resilience objectives. Such measures should address the entire infrastructure life-cycle from planning to operations, maintenance and renewal or retrofitting. Government prioritisation of resilience measures should be informed by cost-benefit analysis taking into account repercussions on the cost of service.

Why is this important?

Governments can choose from a variety of policy tools and mechanisms to advance implementation of resilience objectives, from voluntary frameworks and incentive mechanisms, to regulatory or legal tools. Operators have a keen interest in maintaining the continuity of their services and their reputation by investing in resilience. However, investments in resilience often imply costs up front, even if these should be compensated in terms of greater reliability of service and resilience to shocks. The question is how to find the right balance. Additional requirements imposed by governments to strengthen

resilience may result in additional costs ultimately borne by customers, citizens and businesses. It is important to tailor public policy instruments to provide effective incentives for operators to invest in resilience, while managing the financial repercussions.

The regulatory approach has strengths in that it provides clear and measurable obligations, for instance setting reliability requirements, or requiring business continuity plans, insurance mechanisms, and minimum security standards. However, when to prescriptive, it can also prove costly, not be up to speed with rapid technological developments and can create compliance challenges. Imposing a compensation scheme for customers whose service is disrupted, or other types of penalties can be efficient to incentivise resilience investments, notably in public-private-partnerships. Such approach also provides operators with the choice of the ways to increase their resilience. Voluntary frameworks such as the development of resilience guidelines, awareness raising activities or the sharing of good practices, is often a preferred option to favour stakeholder engagement, but has important uncertainties. Finding a balance between public financial support and private investments for such resilience measures, can use cost-benefit analysis methods to prioritise the most effective ways to share the costs of an overall collective effort towards achieving shared resilience objectives.

Key policy questions:

- *Are there resilience measures defined to increase the level of protection, robustness, redundancy or adaptability across critical infrastructure life cycle?*
- *Are there minimum security standards in place to ensure operators invest in resilience?*
- *Are sectoral regulators playing a role in incentivising critical infrastructure resilience?*
- *Are cost-benefit analysis used to prioritise resilience measures, evaluate their impact on costs of services, and find cost-sharing arrangements?*

Benchmark indicators

- *Implementation plans on critical infrastructure resilience*
- *Infrastructure regulations provisions on resilience*
- *Assessments of cost-benefits of resilience measures*

Examples of good practices

- *In Finland, the Energy Authority sets the requirements for business continuity and reliability standards in the electricity sector, and the National Emergency Supply Agency provides tools, guidance and methods for operators to comply with these regulations.*
- *In France, the State, CI operators and local authorities have agreed on measures to increase CI resilience for the risk of a major flood in Paris. This includes information-sharing, emergency preparedness and vulnerability reduction for existing and future infrastructure.*

6. Ensuring accountability and monitoring implementation of critical infrastructure resilience policies

Government should monitor implementation and evaluate progress in attaining resilience objectives, and define an accountability framework for critical infrastructure operators. Reviewing the effectiveness of the resilience policy tools should allow adjustments to a dynamic risk landscape and infrastructure innovations while taking into consideration the need for predictable and stable regulatory frameworks conducive to infrastructure investments.

Why is this important?

A comprehensive policy framework is a first step towards enhancing critical infrastructure resilience. Whether critical infrastructure will actually be resilient hinges on the implementation of the objectives and requirements put forward in these policies. Accountability mechanisms need to be set-up to ensure that operators carry out the stipulated resilience measures, such as criticality and vulnerability assessments, business continuity plans, back-up operating systems, exercises and stress tests, mutual aid agreements, retrofitting of assets, or risk financing mechanisms.

Monitoring implementation can take diverse forms including regular reporting, inspections and performance assessments or peer reviews. To strengthen accountability, fines for non-compliance, recognition/awards for the implementation of good practices and peer pressure through the use of open access evaluations/rankings are other available incentives that may motivate operators to prioritize investments in resilience measures. Regular evaluations are also useful to assess the effectiveness of policy instruments to strengthen critical infrastructure resilience and adapt them to keep up with the pace of innovations and emerging risk patterns.

Key policy questions:

- *Is there a regular monitoring of the implementation of resilience measures by critical infrastructure operators?*
- *Are there accountability frameworks in place to ensure that resilience measures are implemented?*
- *Are there reviews of the effectiveness of resilience policy instruments planned to adjust to a dynamic risk landscape?*
- *Are there joint exercises to test crisis and continuity management mechanisms?*

Benchmark indicators

- *Accountability frameworks for critical infrastructure stakeholders*
- *Revisions of critical infrastructure policies*

Examples of good practices

- *In Korea, the Ministry of Interior and Safety evaluates disaster response capacities of critical infrastructure operators every year, with a ranking that goes public. The peer pressure creates important incentives for operators to keep up their public image.*
- *10 years after its adoption, the European Commission is evaluating its Directive on European Critical Infrastructures to assess whether it remains relevant and effective.*

7. Addressing the transboundary dimension of infrastructure systems

Government should coordinate national critical infrastructure resilience policies with neighbouring countries and beyond, to address transboundary dependencies. International information-sharing mechanisms should be set up to assess risks and vulnerabilities across borders as well as to develop common approaches for critical infrastructure resilience.

Why is it important?

Interconnected and interdependent infrastructures cross borders bringing an important international dimension to resilience. Hazards and threats do not stop at national borders and integrated supply chains can propagate their consequences. In some cases, critical infrastructure provide services in multiple countries and different jurisdictions. This makes it more compelling to integrate international cooperation in critical infrastructure resilience policies. Sharing information and good practices, adopting common approaches, developing joint standards in critical infrastructure resilience are among the policy options that can foster international and transboundary cooperation in this area.

Key questions:

- *Are there international forums to foster exchange of good practices and to build common approaches for critical infrastructure resilience policies?*
- *Are there international information sharing platforms on risks and vulnerability for interdependent critical infrastructure?*
- *Are there cooperation mechanisms in place to define joint standards for critical infrastructure resilience with neighbouring countries?*

Benchmark indicators

- *International policy frameworks for critical infrastructure resilience*
- *Joint critical infrastructure resilience plans*

Examples of good practices

- *The Canada – United States Action Plan for Critical Infrastructure promotes an integrated approach to critical infrastructure protection and resilience by enhancing coordination of activities and facilitating continuous dialogue among cross-border stakeholders.*
- *The European Programme for Critical Infrastructure Protection (EPCIP) is a long-term programme that encompasses various instruments for the protection of critical infrastructure in the EU, including regular meetings of national CIP Points of Contact. Its external dimension includes regular meetings with strategic partners and was recently widened to include cooperation with neighbouring countries.*

References

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

OECD (2018), *Assessing Global Progress in the Governance of Critical Risks*, OECD Reviews of Risk Management Policies, OECD Publishing, Paris, https://dx.doi.org/10.1787/9789264309272-en. [2]

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 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]