

OECD workshop on good governance for critical infrastructure resilience and security

5th April 2019, Washington DC, USA

AGENDA

Policy context

Natural hazards, cyber-attacks, terrorism and hybrid threats may severely disrupt increasingly interdependent critical infrastructures, requiring holistic systems approaches to boost their resilience. The interconnectedness of supply chains, technological and financial systems that form the foundation of the global economy increases critical infrastructure exposure and vulnerability to unanticipated events. A single shock event can yield negative impacts across sectors and borders, generating systemic risks. Systems approaches are important to strengthen the resilience of complex and dynamic critical infrastructure networks. A more holistic approach to disaster risk management across the entire infrastructure life cycle is needed in order to mitigate potential cascading impacts of infrastructure disruptions. To design effective resilience policies a systems approach provides key tools to understanding the interactions between infrastructures and sectors.

Innovation, digitalisation and a changing risk landscape require adjustments to public policies to continually ensure resilience of critical infrastructure. Many countries have defined critical infrastructure sectors, established an inventory of assets and set-up regulations, national programmes or incentive mechanisms to strengthen the resilience of critical infrastructure to shock events. Nonetheless, the diversity and complexity of shock events and increased interdependencies between systems, mainly due to digitalisation and the emergence of global value chains, continue to pose new concerns that policies need to account for. In parallel, the fast pace of innovation continues to transform critical infrastructure sectors with in-built complexities and unprecedented potential for domino effects.

The need to renew a significant stock of infrastructure in mature economies and growing infrastructure needs in emerging economies call for a critical rethink of critical infrastructure policy to fully integrate resilience. With infrastructure investments on the rise globally comes a great opportunity to re-evaluate critical infrastructure policies across OECD countries and beyond. Strategic thinking is required to integrate resilience upfront in the infrastructure design, and also in the maintenance of existing infrastructure. What is the role for governments in boosting critical infrastructure resilience? How can critical infrastructure operators – public and private – be engaged in strengthening their resilience efforts? How can government and operators share the costs of resilience investments? How can governments and operators avoid the infrastructure investment traps and keep maximum flexibility to ensure resilience in the future? These are key governance issues that governments are confronted with when designing their critical infrastructure policy.

Reinforced partnerships between public and private operators and stakeholders, and the scientific community are fundamental to the effective governance of critical infrastructure resilience. Engagement across stakeholders between public and the private sectors in an open dialogue can help overcome challenges and promote effective critical infrastructure resilience and security policies. Knowledge and insights from the scientific community can support policy makers and private operators. This wealth of knowledge spreads from detailed modelling approaches to high level risk and resilience assessment frameworks. A tiered approach leveraging existing knowledge and tools in multi-stakeholder information sharing and cooperation platforms could help reconcile different objectives and knowledge bases with the need to increase resilience.

OECD Workshop on Good governance for critical infrastructure resilience and security

This OECD invites experts from critical infrastructure operators, the policy community and academia in North America to exchange on risks threatening critical infrastructure, discuss interdependencies, and share good policy practices for strengthening the resilience of these interconnected networks.

The OECD High-Level Risk Forum brings together policy makers from government, practitioners from the private sector and civil society, and experts from think tanks and academia to identify and share good practices in risk governance. Its work is underpinned by the OECD Recommendation on the Governance of Critical Risks, adopted by the OECD Council in 2014, which acknowledges the importance of critical infrastructure resilience and security as a key element of national resilience.

This meeting is open to participation from experts, policy makers, critical infrastructure operators, and civil society representatives from Canada, Mexico, and the United States. The workshop aims to stimulate a comprehensive dialogue among stakeholders to address the multiple facets of critical infrastructure resilience. The workshop will provide an opportunity to exchange on critical infrastructure policies and technical tools and practices to support evidence-based policy-making.

Registration and additional information

Workshop's venue: OECD Washington Center, 1776 I Street, N.W., Suite 450, Washington D.C. 20006, United States.

AGENDA

9h00 – 9h30 Welcome and registration

9h30 – 9h40 Opening remarks

- *Mr. Jack Radisch, Manager of the OECD High Level Risk Forum*

9h40-10h00 Keynote: the value of partnerships and international cooperation in risk management

- *Dr. Dan Kaniewski, Deputy Administrator for resilience, US Federal Emergency Management Agency*

10h00 – 10h20 Presentation: the OECD Policy Toolkit on the Governance of Critical Infrastructure Resilience

This introductory presentation will provide an overview of critical infrastructure resilience policies across OECD countries. Based on an OECD cross-country survey, the presentation will highlight the various approaches taken by countries to foster resilience. It will present the results of on-going OECD work on how to use a system approach for critical infrastructure resilience and share the recommendations from the OECD Policy Toolkit on Governance for Cortical Infrastructure Resilience.

- *Mr. Charles Baubion, OECD High-Level Risk Forum*

10h20-10h30 Session break

Which policy tools for critical infrastructure resilience?

10h30 – 11h30 Session 1: Partnerships between governments and operators for critical infrastructure resilience: success factors and bottlenecks

This session will discuss the success factors and bottlenecks in establishing partnerships between government and infrastructure operators to foster critical infrastructure resilience.

The discussion will focus on how to build trust between stakeholders so that information-sharing is effective and common resilience objectives can be agreed upon.

Moderator: *Mr. Jack Radisch, OECD*

Panellists:

- *Mr. Mark Kneidinger, Deputy Director, National Risk Management Center at Department of Homeland Security*
- *Mr. Trent Abbott, Senior Policy Advisor, Critical Infrastructure Policy Division, Public Safety Canada*

11h30 – 12h30 Session 2: How to foster investments in critical infrastructure resilience in the United States and how should costs be shared?

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. Excessive requirements imposed by governments to strengthen resilience can result in additional costs of service borne by customers, citizens and businesses. This session will discuss how governments can best mobilise and tailor public policy instruments to provide effective incentives for operators to invest in resilience, while managing the repercussions on the cost of service.

Moderator: *Mr. Jack Radisch, OECD*

Panellists:

- *Mr. Henry H. Willis, Associate Director, Homeland Security Operational Analysis Center, Rand Corporation*
- *Mr. Mark Kneidinger, Deputy Director, National Risk Management Center at Department of Homeland Security*
- *Mr. Chris Boyer, Global Public Policy, ATT Service Inc.*
- *Mr. Ron T. Jennings, Manager Gas Supply & Transportation, Baltimore Gas and Electric Company*

12h30 – 14h00 Lunch

Which technical tools for critical infrastructure resilience?

14h00- 15:45 Session 3: Mapping interdependencies between critical infrastructure sectors and assessing systemic risk

Mapping interdependencies among and between sectors is crucial to understanding the critical risks faced by infrastructure systems. The mapping requires a systematic approach based on common standards and metrics. This session will present methods and models to identify the critical systems and assets that should be prioritised for resilient investments, and assess their resilience.

Moderator: *Mr. Charles Baubion, OECD*

Panellists:

- *Prof. Aleksandar Jovanović, Chief Executive Officer, European Virtual Institute for Integrated Risk Management*
- *Dr. Frédéric Petit, Argonne National Laboratory*
- *Dr. Maria K. Dillard, National Institute of Standards and Technology*

Conclusion and way forward

15:45-16:00: Applying the OECD Policy Toolkit on the Governance of Critical Infrastructure Resilience

- *Mr. Jack Radisch, Manager of the OECD High Level Risk Forum*