Critical Infrastructure and Disaster Resilience:
Issue Brief by Private Sector (ARISE)

Intended audience:

- **Governments** who are implementing the Sendai Framework, and who own, manage, operate and maintain many critical infrastructure systems;
- **National focal points** and related agencies in these governments, deciding which critical infrastructure and basic services should be included in their Sendai Framework monitoring process;
- **Cities** wishing to become more resilient, and who also own many critical infrastructure systems;
- **Private sector companies** (including semi-private and semi-public entities often found in the energy or utility sectors) that own or operate critical infrastructure systems or that depend on them.

Relevant Sendai Framework Targets:

- **Global target B:** Substantially reduce the number of affected people globally by 2030, aiming to lower the average global figure per 100,000 between 2020-2030 compared with 2005-2015
- **Global Target D:** Substantially reduce disaster damage to critical infrastructure and disruption of basic services, among them health and educational facilities, including through developing their resilience by 2030

Nature of the problem:

Critical infrastructure resilience is a complex problem, the dimensions of which directly impinge upon achieving the Sendai Framework for Disaster Risk Reduction's overall goal: *The substantial reduction of disaster risk and losses in lives, livelihoods and health and in the economic, physical, social, cultural and environmental assets of persons, businesses, communities and countries*.

Critical infrastructure functions as interrelated "systems of systems" – energy, water, communications, transportation, healthcare, law and order, data, and so on[1]. From this one fact, the following issues arise:

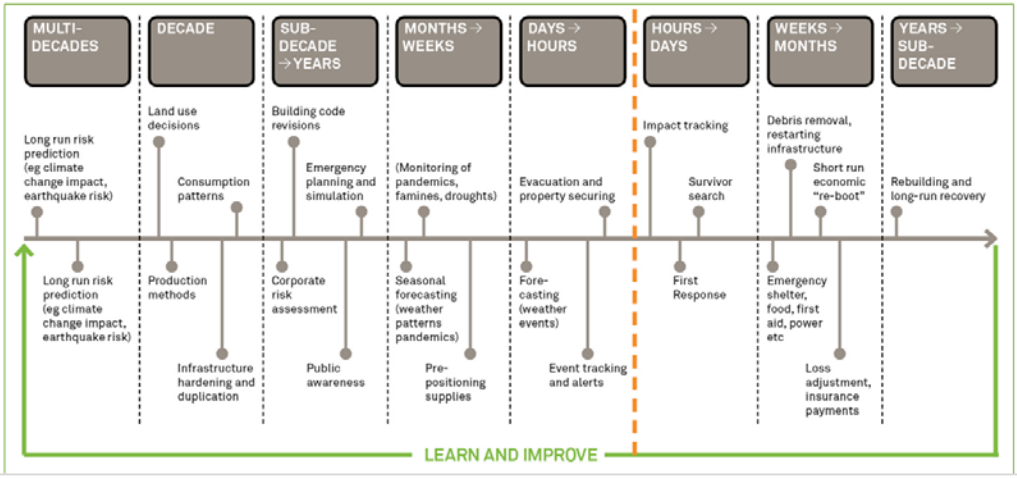
i. Each system may interact with other systems in ways that allow the possibility of cascading "failure chains", where for example an electrical substation is flooded, which knocks out a water treatment plant, which in turn disables a hospital. ***Many countries and cities can identify their critical systems and assets, but very few can identify how they are linked to each other.*** *Achieving critical infrastructure resilience requires investing time and effort to identify and maintain data on these linkages.*

[1] A listing of possible critical infrastructure systems is provided at the end of this document.

ii. Each critical infrastructure system in the "system of systems" – and the critical assets that make them up - may be in different ownership, either within the city government, or in some other tier of government, or in a private sector utility or other organization. ***Critical infrastructure resilience is inherently, therefore, a multi organizational endeavor.***

iii. The definition of "critical" in critical infrastructure resilience is not fixed in time. A road or a flood pump may become critical over time, perhaps over a period of years as a nearby suburb expands to accommodate people from the city; or as the road or pump becomes more endangered over time as sea levels rise or weather patterns change. *Critical infrastructure resilience needs to be approached as a process in which* ***resilience levels (and asset-to-asset dependencies) change – and are recovered – over time, rather than as a one-time exercise****.*

Disaster resilience is a *process*, spanning multiple activities and time-scales. The same applies to critical infrastructure



iv. At the other end of the scale an otherwise unremarkable access road may, if it becomes blocked by debris and impedes access to a critical asset such as the flood pump, *itself* become critical in real time, and remain that way for a period of days. ***Critical infrastructure resilience needs to include the "may become critical" assets that can impinge on critical ones.***

v. Risk to critical assets needs to be assessed on a very granular scale. Each asset in the same system and in the same region may have different seismic capabilities or ability to accommodate flooding. Therefore, *critical infrastructure resilience needs to be* ***assessed at the individual asset level****.*

vi. Many organizations have weak asset management processes, for example with deficiencies in inspection routines, or in collecting data on asset status and maintenance, or in reserving funds for maintenance and upgrades. This means that critical assets may fail or be impaired when needed (for example, when the spillway for the Oroville Dam in California collapsed early in 2017 when used during a wet winter, necessitating evacuation of 188,000 people); or in extreme cases, they may fail randomly, as for example when a gas pipeline exploded in San Bruno, California in 2010 killing 8 people. ***Critical infrastructure resilience is a function of***

organizational process discipline and stewardship of its assets**, as well as hardening or relocating those assets**.

vii. Many critical assets and systems may be in areas that are known to be disaster prone but have not had a disaster for some years. Their owners may not have practiced disaster resilience in the period since the last real alert; or they may not have documented how they addressed the problems that arose last time - and those who had that knowledge may have left the organization or retired. In either case, with the next disaster, the infrastructure owner will be "learning all over again". Related to the previous point, therefore, ***critical infrastructure resilience is therefore also a function of organizational readiness.***

Recommended tools and approaches:

As the private sector stakeholder group for UNISDR, ARISE identifies and recommends, through its collective operational experience, the following tools as effective towards critical infrastructure resilience:

At the "system of systems" management level

Use of methodologies to understand critical system and asset interlinkages

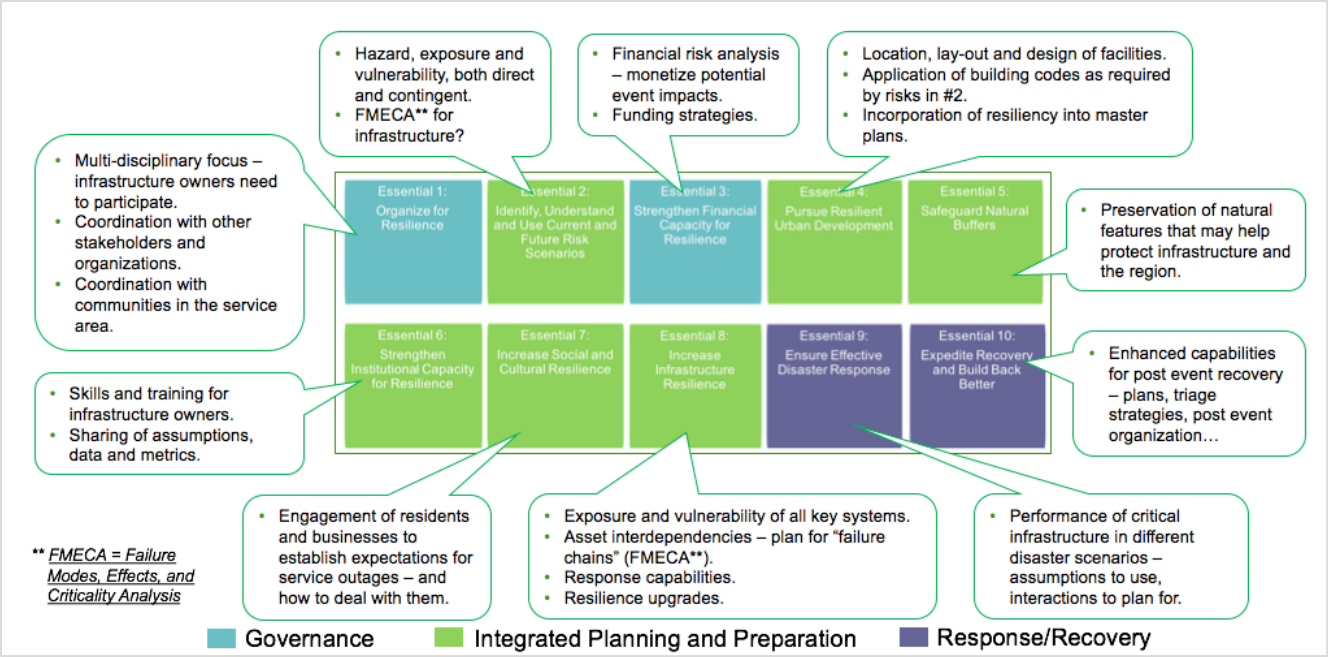
More widespread use needs to be made of engineering methodologies for detecting and managing linkages between critical assets. The military has used established methodology such as Failure Modes, Effects and Criticality Analysis (FMECA) for the management of complex engineered "systems of systems" such as aircraft carriers, and there are several other options from the civil engineering world. A standard method (or set thereof) needs to be identified and promulgated.

Use of map-based systems

A "system of systems" is best understood and managed by map-based tools, such as GIS (Geographical Information Systems). Map-based tools facilitate information sharing between those who own and manage critical infrastructure systems and assets, including local governments and private companies; useful for analysis and identification of critical assets; effective for record-keeping and maintenance; and encourage process-based (as opposed to one-time) infrastructure management. Of course, not all information needs to be open, nor shared, constantly. However, moving over the daily management of critical infrastructure systems, both public and private, to map-based systems built on common protocols and base maps is key in building critical infrastructure resilience.

Use of UNISDR's Ten Essentials of Disaster Resilience and City Resilience Scorecard

UNISDR created the Ten Essentials of disaster resilience, and also sponsored the creation of the City Disaster Resilience Scorecard. While these take a wider view than critical infrastructure alone, they can provide the context within which critical infrastructure resilience should be pursued. The graphic below illustrates how the Ten Essentials might apply here. The reference for the Scorecard is included at the end of this document.



Encouraging multi-organizational collaboration and organizational competence

Those who own and manage critical infrastructure systems and assets, including local governments and private companies, may prioritize investment towards resilience in their own hardware and physical readiness, over other possible actions, or in ignorance of the impact on other systems. Government leadership is essential in promoting the necessary prioritization and collaboration, which may not otherwise take place.

At each critical infrastructure system or asset level

Reinforcement of basic asset management disciplines

Owners and operators of critical infrastructure need to ensure that their basic asset management disciplines – budgeting, inspections, data capture and so on – are sound and reliable. Targets and metrics need to be promulgated for this purpose, probably drawing on existing standards.

Use of predictive maintenance

In particular with the growing use of sensors on machinery and structures, and analysis of the data provided, failures of equipment or infrastructure can frequently be predicted using predictive maintenance tools. Standards for critical infrastructure resilience need to specify the use of predictive maintenance.

Identifying "dividends" to encourage investment

Investments in critical infrastructure resilience frequently yield "dividends" in other areas, for example where a flood zone also functions as a park when not flooded, or where investment in a neighborhood microgrid makes part of the energy supply more resilient. Conversely, investments in other areas can yield "dividends" in critical infrastructure resilience, for example where underground parking garages

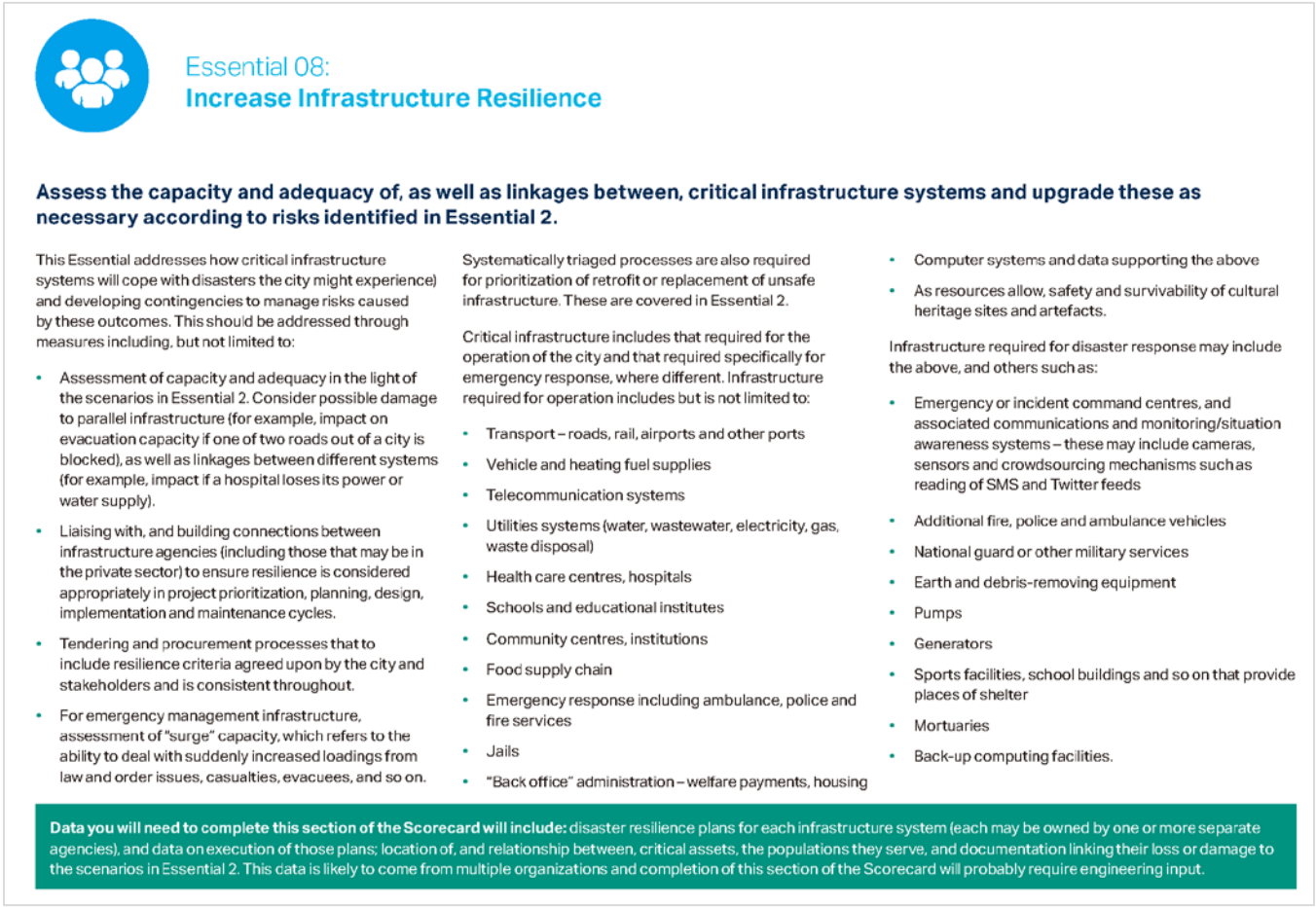
are designed also to function as storm-water cisterns. These dividends can help greatly with making the case for investing in critical infrastructure resilience.

Where to start:

Governments, economies and societies need to know that their critical infrastructure systems are designed to deal with the natural risk and threats that they may face; and to have confidence that they will perform as designed when adverse events occur.

We recommend that the national level Sendai Framework monitoring processes select elements of critical infrastructure and basic services (whether for reporting on global indicators or designing nationally determined indicators) that may reflect progress in the dimensions identified in this paper, drawing on existing standards wherever possible.

To identify elements that may be part of your unique critical infrastructure 'system of systems,' a good place to start is the list provided in UNISDR City Disaster Resilience Scorecard's **Essential 8** (below).



Essential 08:
Increase Infrastructure Resilience

Assess the capacity and adequacy of, as well as linkages between, critical infrastructure systems and upgrade these as necessary according to risks identified in Essential 2.

This Essential addresses how critical infrastructure systems will cope with disasters the city might experience) and developing contingencies to manage risks caused by these outcomes. This should be addressed through measures including, but not limited to:

- Assessment of capacity and adequacy in the light of the scenarios in Essential 2. Consider possible damage to parallel infrastructure (for example, impact on evacuation capacity if one of two roads out of a city is blocked), as well as linkages between different systems (for example, impact if a hospital loses its power or water supply).
- Liaising with, and building connections between infrastructure agencies (including those that may be in the private sector) to ensure resilience is considered appropriately in project prioritization, planning, design, implementation and maintenance cycles.
- Tendering and procurement processes that to include resilience criteria agreed upon by the city and stakeholders and is consistent throughout.
- For emergency management infrastructure, assessment of "surge" capacity, which refers to the ability to deal with suddenly increased loadings from law and order issues, casualties, evacuees, and so on.

Systematically triaged processes are also required for prioritization of retrofit or replacement of unsafe infrastructure. These are covered in Essential 2.

Critical infrastructure includes that required for the operation of the city and that required specifically for emergency response, where different. Infrastructure required for operation includes but is not limited to:

- Transport – roads, rail, airports and other ports
- Vehicle and heating fuel supplies
- Telecommunication systems
- Utilities systems (water, wastewater, electricity, gas, waste disposal)
- Health care centres, hospitals
- Schools and educational institutes
- Community centres, institutions
- Food supply chain
- Emergency response including ambulance, police and fire services
- Jails
- "Back office" administration – welfare payments, housing
- Computer systems and data supporting the above
- As resources allow, safety and survivability of cultural heritage sites and artefacts.

Infrastructure required for disaster response may include the above, and others such as:

- Emergency or incident command centres, and associated communications and monitoring/situation awareness systems – these may include cameras, sensors and crowdsourcing mechanisms such as reading of SMS and Twitter feeds
- Additional fire, police and ambulance vehicles
- National guard or other military services
- Earth and debris-removing equipment
- Pumps
- Generators
- Sports facilities, school buildings and so on that provide places of shelter
- Mortuaries
- Back-up computing facilities.

Data you will need to complete this section of the Scorecard will include: disaster resilience plans for each infrastructure system (each may be owned by one or more separate agencies), and data on execution of those plans; location of, and relationship between, critical assets, the populations they serve, and documentation linking their loss or damage to the scenarios in Essential 2. This data is likely to come from multiple organizations and completion of this section of the Scorecard will probably require engineering input.

Further recommended reading:

IBM 2010 “IBM Institute for Business Value executive report, "The world's US$4 trillion challenge: Using a system-of-systems approach to build a smarter planet" https://public.dhe.ibm.com/common/ssi/ecm/gb/en/gbe03278usen/GBE03278USEN.PDF

Peter Williams, DE, IBM 2017 “INTACT: The Role of IT and the IOT in Critical Infrastructure Resilience” http://www.intact-project.eu/intact/assets/File/other/20170323 - INTACT End Event - The Role of IT and the IOT in Critical Infrastructure Resilience - Peter Williams.pdf

UNISDR City Disaster Resilience Scorecard, Version 3 (updated for the Sendai Framework): http://www.unisdr.org/campaign/resilientcities/home/toolkitblkitem/?id=4

Why ARISE[2] is authoring this issue brief:

The private sector wishes to ensure that all above aspects of the problem above are addressed, because:

- It owns and/or operates critical infrastructure systems.
- It is dependent on critical infrastructure systems operated by the public sector and other entities within the “system of systems” in cities and countries. These dependencies may take the form of physical or data linkages between its own and other infrastructure systems; or it may take the form of temporary loss of workforce due to broken transportation systems or the overriding concern of workers for their own homes and families.
- It believes that it has the operational experience from its own critical infrastructure resilience activities, and from ensuring the resilience of facilities such as oil and chemical refineries, heavy manufacturing plants and data centers to contribute to a raising of standards in critical infrastructure resilience globally.
- Many sectors (retail, transportation) may be affected by the loss of livelihoods and economic activity following disasters.

[2] This issue brief was authored by ARISE members IBM and Kokusai Kogyo, with input from Dr. William Hynes of Future Analytics Consulting and leader of the EU’s HARMONISE and RESILENS Initiatives.