Critical Infrastructure Resilience:

A Regional and National Approach

Emily Frye

Approved for Public Release; Distribution Unlimited. 14-4047

November 2014

McLean, VA

MITRE

Executive Summary

In 1992, Broward County was preparing for a Category 5 Hurricane. The following morning Hurricane Andrew shifted south and devastated Miami Dade.

Eleven years later the Blackout of 2003 darkened NYC.

These are just two of the countless examples of incidents for which the United States was not fully prepared. There were rippling impacts on Critical Infrastructure (CI) that devastated the regions long after the events were making headlines. CI Resilience is often discussed as a national priority – and it is – but MITRE proposes that we can't tackle resilience at the national level alone, we must also address it at a regional level. Consider the most severe disaster you have personally experienced. Were you living in Homestead, Florida when Hurricane Andrew made landfall, in New Orleans during Katrina, or in the San Fernando Valley during the Northridge earthquake? Were you working in lower Manhattan on 9/11 when the first plane hit the World Trade Center? Many Americans have experienced these tragedies first-hand, and many more have watched in horror as these and other events around the world, such as the Fukushima, Japan disaster, the Haiti earthquake, and the tsunami in Indonesia, unfolded on their television screens. These local events had cascading effects on the wider economy and security of their respective countries.

When these disasters occur they not only destroy personal property and disrupt communities' way of life, they also disrupt the vital infrastructure that enables our economic stability. The below paper describes MITRE's recommendations for how to meaningfully promote national resilience by empowering regions to assess, and then enhance, their overall resilience posture.

KEY MILESTONES

1997
The President s Commission on Critical Infrastructure Protection (PCCIP) recognized the central value of infrastructure.

2001
Critical Infrastructures Protection Act codified a national policy approach to minimize disruptions to Critical infrastructure.

MITRE in its role as a trusted advisor with government leaders throughout the Federal Government, combined with its insights into regional priorities and concerns, offers three essential recommendations for addressing CI resilience:

1. Resilience should be assessed and addressed at a regional level.
2. Resilience assessments should be function-based (rather than asset-based), and should encompass both physical and cyber terrain.
3. The federal government role is to empower greater governance, planning, and implementation by regions- for regions; and to dovetail national priorities with regional priorities where both can benefit.

History has shown that our focus must be on bolstering the capability of maintaining essential functions through adverse circumstances, and when that is impossible, to ensure recovery as rapidly as possible. A well-organized, collaborative and plan-based approach to CI resilience may be our best hope.

The argument for building domestic Resilience is widely embraced, and it now is enshrined in presidential directives and planning frameworks. However, in key respects, achieving Resilience is more demanding than traditional protection efforts. It requires more holistic planning and harder choices than we are traditionally used to making. That requires tough choices for defining and aligning acceptable levels of risk. This includes weighing the capacity of CI to withstand or recover from traumatic events against the public's willingness and ability to prepare mentally and invest materially in Resilience beforehand. It will also require both a regional and enterprise systems-based approach to achieving Resilience.

Why Regional Resilience?

Early experiences in disasters, and studies in modeling and simulation, demonstrate that failure of an individual asset can sometimes cause a major discontinuity in the operation of a system (e.g., the loss of one refinery after Hurricane Katrina led to the shift of entire manufacturing industries due to the non-availability of sufficient quantities of specific chemicals). However, sometimes an asset of apparently similar value and utilization would cause no intermediate consequences (e.g., while a nuisance, the I-35 Mississippi River Bridge collapse resulted in marginal impacts on Minneapolis' economy and way of life). These examples depict that resilience, dependent on regional systems, can support the preservation of property and of each community's way of life; and, essentially, that regions differ.

Other lessons have emerged as well. Together, they lead us to a set of key precepts:

1. Resilience can often be best addressed on a regional or local basis.
2. The federal government has an important role in promoting regional Resilience.
3. Resilience should be addressed in a comprehensive, cyber-physical manner.
4. Every region should understand its own Resilience. This regional functions-based assessment should include an analysis of the ability of essential lifelines to endure, sustain, and regenerate against a range of significant stresses, risks and threats and reflect local knowledge and priorities. Every region should regularly conduct functions-based Resilience assessments that:
    a. Include essential lifeline sectors (Energy, Water, IT/Communications, Transportation, and Emergency Services), and
    b. Acknowledge and incorporate local knowledge and priorities, such as: core economic activity and jobs basis; local cultures; and preexisting analysis by localities.
5. Every region should also have an action plan for what can be addressed over time (during design and build opportunities). The Resilience action plan for a region could be developed using a public-private governance approach that includes regional and state entities and lifeline sector owners and operators.
6. Regional Resilience assessments and action plans should result in priorities that inform both national understanding and planning; where appropriate, grants should be made available to address Resilience priorities shared by the region and the nation.

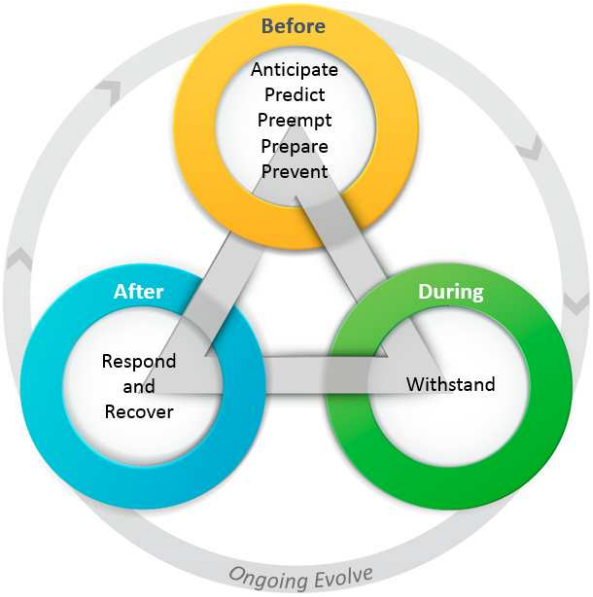
Not all threats are preventable; however, MITRE recognizes that those closest to the functions and assets are best informed and equipped to understand the needs and provide the response and recovery mechanisms which are employed at the local and regional level. In addition, the idea of "resilience" is essential. Efforts must focus on bolstering the capability to maintain essential

functions through adverse circumstances - and rapidly reconstituting them when that is not possible.

An increased emphasis on Resilience provides the best approach to developing affordable and sustainable capabilities for the nation to withstand and recover from the full range of threats it faces. For the nation to become resilient it requires a multifaceted approach beginning with private and public enterprises and communities, and spanning state and regional levels, and connecting regions at the national level.

A shift of focus is required: from assets to systems,[1] from protection to Resilience, from individual facility impacts to regional disruption. This paradigm shift reinforces the need for effective partnerships at multiple levels.

Dimensions of Resilience



When critical infrastructure fails (e.g., Sandy, Katrina) significant money is spent on responding to the event. However, MITRE proposes if more funding was invested in resilience planning, the impact could be minimized with faster recovery times. MITRE leverages the resilience model which allows system managers to *predict* weak spots, plan counter-measures (*protection and/or resilience*) in advance, fix errors, and prepare to *rapidly respond and recover* from diverse and heterogeneous threats and disasters.

Viewing CI as the complex interface of socio-technical-economic systems necessitates that owners and operators develop partnerships, plan and prepare with the community, and look more broadly at the region in which they are embedded to fully understand and take advantage of all the means available to make systems as resilient as possible. By leveraging this framework and planning for overall critical infrastructure resilience (vs. just response to an event), regions and the nation will be able to better prepare, withstand, and recover from events.

Before An Event: Anticipate, Predict, Preempt, Plan, Prepare, Prevent

Being able to predict a threat or crisis can sometimes inform prevention of it from happening, or allow activities that significantly mitigate some, if not all, of the consequences. Such actions taken beforehand contribute to Resilience by reducing the threat to systems and assets.

Three discrete examples of how the functions could add value to regional resilience are:

- Near-term awareness - Regional Cyber Threat Sharing Centers. These regional centers would allow members to share threat and response information and build a distributed database and sharing community.

[1] There are some exceptions, such as the Section 9 list from EO 13636.

- Long-term awareness - Extreme Weather and Long Term Forecasting. Prediction and forecasting capabilities by the federal government (e.g., National Weather Service, National Hurricane Center) help in the ability to predict extreme weather.
- Warning – In the immediate run-up to an event, Integration of Social Media into Public Warning Social media, with its ubiquitous availability on smart phones, can provide public warning directly to individuals. It can work from both the Government to the public and the public to the Government

The ability to predict does not guarantee appropriate protective action will always occur, but effective prediction makes informed choices possible.

During An Event: Withstand and Mitigate

Perhaps more than the other elements,' withstand' depends on advanced planning. Advanced planning, and the ability to mitigate, depends on understanding the strengths of the systems, the weaknesses of the systems, the interdependencies of the systems, and the bolstering options that are kept in reserve.

Our CI systems, especially those in the Lifeline Sectors, should be designed, implemented, maintained, and operated in such a way that they continue to sustain their core functions even during disaster or attack. To be able to withstand disaster and attack, they need to incorporate a combination of physical engineering strategies, Cybersecurity, and operational strategies. Employing all three in combination will help protect systems from accidental failure, engineering failures, natural disasters, and physical and Cyber-attack.

After An Event: Rapidly Respond, Recover, and Restore

Being able to respond to and recover from incidents quickly allows citizens to get back to work and to their normal lives. In the aggregate, rapid lifeline-function restoration is essential to the American way of life and the nation's economy.

The federal government needs to establish policies, plans, and practices for collaborating in the nation's response to adverse incidents that are both cyber and physical in nature. This dynamic is applicable at the local/regional level as well. Regions also need to understand the newer element of cyber incident and cyber response. Many have very low cyber situational awareness at this time, which makes timely response impossible.

Ongoing – Learn and Evolve

The threats we face, both natural and man-made, are not constant. Rather, they are constantly evolving. Weather is becoming more severe, the climate is changing, and man-made threats adapt and innovate to countermeasures put up against them. Therefore, Resilience also must evolve to keep pace but in a manageable and practical manner so that sound investments can be made without being wasted. The next section addresses how.

Identify the Regions; Assess & Bolster Governance

Stakeholder coordination, shared understanding, and collaboration is at the heart of improved Resilience. The first order of business then, is to identify the appropriate regions in which to support and grow Resilience programs. Regions should be identified based on:

a. Concentrations of interconnectedness and interdependencies of CI.
b. Preexisting and new organic organizations that include both public and private stakeholders.

Fortunately, both of these criteria have already been met in some regions.

Identify Regions Based on Preexisting and New Organic Organizations[2]

There are a number of different regional constructs that have been developed for various purposes (for example, the FEMA regions). For purposes of enhancing regional resilience we recommend starting with eight regions[3] that are already demonstrating active self-governance and coordination, and expanding by considering the Regional Consortium Coordinating Council (RCCC) regions as the breakout.

The current U.S. geographic coverage of the RCCC regions is shown below

RCCC Regions

The federal government should also be involved to support outreach, grant writing, and technical assistance for governance groups. For purposes of this paper, we will call the regional governance groups "Regional Consortia," or RCs.

In general, the goals of any regional resilience consortia should be to:

[2] In truth, a uniform approach such as the one described here has appeal from a management standpoint – but is unlikely to play out uniformly. A true "region" is organic and variable in size and constituencies. It can be as small as a single urban area or as large as the North Atlantic coast.

[3] The eight regions that MITRE has already identified as likely leaders in collaborative regional approaches to resilience are: the Bay Area Center for Regional Disaster Resilience; the Pacific Northwest Region; the Great Lakes Consortium; Chicago First; New Orleans; the Hampton Roads 16-County Coalition; the Boston-area (Advanced Cyber Security Center and others); and the Mid-Atlantic Cyber Center.

- ***Strengthen Existing Regional Partnerships:*** While the existing or new RCs will provide the nuclei for the partnerships in each region there are several more partnerships that need to be formed in order to strengthen and make each region fully effective. Each RC should consider inviting additional entities to become members (e.g., State Fusion Centers within their region as well as other region-wide emergency planning and mitigation organizations not already RC members [(e.g., the Central U.S. Earthquake Consortium for the South East Regional Research Initiative RC)].
- ***Organize Lifeline Sectors to Participate:*** The term "lifeline sector" generally refers to a sector that provides vital services that enable the continuous operation of critical business functions, and would risk human health and safety or economic security if disrupted or not rapidly recovered. These sectors provide the most indispensable services that underlie a regional economy (e.g., Energy, Transportation, Communications, Water, and First Responders). Hence, these sectors should be organized at both the national and regional levels to enable regional Resilience to include these most essential sectors. Other sectors might be considered lifeline for a particular region or disaster. Additionally, the nature of a disaster condition could elevate one or more sectors to become a lifeline sector under a particular circumstance.

Develop a Portfolio of Tools that Regions Can Readily Use

Having described the regional Resilience starting point (above), the next step is to establish goals, and assess the region against desired regional Resilience goals.

HSPD-5

2003
Homeland Security Presidential Directive 5 (HSPD 5) recognized that first responders could not communicate with one another during a crises and that this problem the failure of interoperability endangered both first

Revisit the Parable of Interoperability: One of the most important DHS' successes to date is the Interoperability Continuum for first responders. In 2003, in response to HSPD-5, DHS developed the Interoperability Continuum – a framework and toolset to address these challenges, and forged teams of facilitators to support debate and planning among first-responders in the development and implementation of this tool. It represents a microcosm of the universe covered by "regional resilience," and is instructive. Pairing the tool with the human element (and therefore coordinative element) resulted in repeated success in community after community. We believe that a similar approach – tools combined with committed facilitation and planning teams – is the optimal kind of investment for this type of multifaceted challenge. The Interoperability Continuum has enabled conversations in communities around the nation – conversations that shed light on the problems of interoperability, highlight the challenges of developing a shared understanding, and promote the ability of communities to define their own goals and path to progress. We suggest that a similar visual tool should be developed for Resilience.

Establish a Grants or Alternate Funding/Incentives Approach for Joint Regional-National Priorities including Lifeline Sector Participation

Once regional resilience plans exist– it will be necessary to create a mechanism for funding high-priority item that regions themselves cannot fund alone.

As they go through discovery, negotiation, planning, and prioritization, regions may identify immediate, mid-term, and long-term capabilities. Some of these needs will logically fall on one or more stakeholders in the region. For instance, a medium-term capability that can be covered by a regulated utility within its rate base is a need that does not require external funding assistance.

In other cases, the regional stakeholders will not be able to afford a priority action. For this reason, it will be important to create a funding stream at the federal level to support priority actions within regional plans that support *regional and national resilience*.

Identify Resilience Gaps and Weaknesses, and Identify the Funding and Operational Plan to Remediate

The end product of the assessment should be a report (or set of reports) documenting and identifying the Resilience gaps and weaknesses within each region, framing the implications/consequences of these shortfalls, and prioritizing them for action.

Develop and Implement Regional Resilience Plans to Address Gaps and Weaknesses

- ***Develop and Implement Regional Resilience Plans to Address Gaps and Weaknesses:*** Essential enabling doctrine for each RC will be its Regional Resilience Plan. Hence, once the expanded partnership is underway and after carrying out its Resilience assessment, that doctrine should be its next priority. The doctrine could take the form of a 5-year plan that describes all the activities that the RC plans to undertake through its membership, with assistance from lifeline infrastructures, state governments, and the federal government.
- ***Implement the Regional Resilience Plan by Addressing Gaps and Weaknesses:*** Given the Regional Resilience gaps and weaknesses report, the funding and incentives should be applied to filling the gaps and overcoming the weaknesses to the extent possible. The extent possible is determined not just by the amount funding available but by the limits of current best practices and technology.
- ***Continue to Identify Requirements for New Capabilities and Technologies:*** Each RC should encourage its membership to be on the lookout for new systems, technologies, and techniques that can enhance the region's Resilience. When an RC member identifies a promising new capability that appears well-suited to the particular region, the RC should discuss it and decide whether to acquire it for the benefit of the members and the region. When a new capability is determined to benefit many or all of the members, then cost-sharing among the members should be considered as a means of distributing costs and facilitating the acquisition. In this way, the region's Resilience can be enhanced over time.
- ***Develop Regional Resilience Metrics:*** Each RC will want to know how much their regional Resilience is increasing over time. For this purpose measurable Resilience

metrics are needed. RC regions are likely to have many common Resilience goals. A "common core" of regional resilience measurement may, in fact, be one of the most valuable tools that the federal government can consolidate over time.

Federal Government Role in Regionalization

The question may be asked - why should the Federal Government be engaged in resilience, when the recommendation is that resilience be tackled at a regional level?

The two are not mutually exclusive. Rather, to be effective, national and regional resilience should complement one another. The federal government has essential national interests that should be addressed within regions, and regions' concerns and priorities should be clear as well for federal personnel at the national level seeking to effectively manage CI and emergency response risks.

Whole communities (including state and local leaders and the private sector) play the key roles in executing resilience programs. However, the federal government has two critical functions to enable communities for true national resilience:

1. to standardize "the Base" i.e., capabilities addressing routine, week-to-week, emergency management requirements, such as responding to multi-car accidents, multi-jurisdictional fires, storm-based regional power outages, and so on, by providing standard descriptions of the problems, enabling cross-state, multi-region dialogues on critical issues, and providing guidance ; and
2. to build up "the Margins" i.e., lower probability/higher consequence catastrophes, such as large-scale earthquakes and Category 5 hurricanes that truly tax the limits of both regional and national systems, by defining activities and creating capabilities that address them.

In fact, the federal government is in a position to set up and enable these functions better than any other individual entity.

Conclusion

Resilience matters. It is not a new idea, but is newly receiving revived attention. We have learned that tackling large, complex problems can be overwhelming; but we know as well that breaking complex problems down into too many subparts results in suboptimal, fragmented solution sets. We propose that regions, with organic concentrations of Critical Infrastructure and population, are the right-size unit for enhancing Resilience.

To increase resilience, every region should conduct, or have conducted, functions-based resilience assessments that include essential lifeline sectors and incorporate local private and public knowledge and priorities. This will assist the regions in understanding their resiliency levels and which action plans need to be addressed in the short and long term. Regional resiliency assessments and action plans should be used to inform national understanding and planning. Grants and technical assistance then should be made available to address applicable resiliency priorities shared by the region and the nation.

No one knows when or where the next major disaster will take place. We do know that state and local parties from both government and private sector Critical Infrastructure operators are almost always the first to respond; that the federal government can play a meaningful and empowering role in regional resilience; and that a coordinated regional-federal response helps everyone. As regional programs and federal executives look to realize the benefits of CI planning before an event, MITRE will be able to leverage lessons learned across multiple Federal agencies and regions to continue to assist organizations to achieve sound critical infrastructure resilience.

Do you have other questions related to critical infrastructure resilience or about MITRE's work in homeland security? Please email us at hssedi_info@mitre.org or visit our webpage http://www.mitre.org/hssedi