Northeastern University

Center for Resilience Studies

Perspectives on Critical Infrastructure and Cyber-Resilience and Future Focus Areas

A Presentation to

National Infrastructure Advisory Council (NIAC)

U.S. Department of Homeland Security
Washington, D.C.

September 16, 2016

Stephen E. Flynn, Ph.D.
Professor of Political Science &
Director, Center for Resilience Studies
Northeastern University
s.flynn@northeastern.edu
617-470-7675

The Resilience Imperative

"The abiding strategy of our parents' generation was 'containment' of communism in order to be free. The abiding strategy of our generation has to be 'resilience.' We will only be free to live the lives we want if we make our cities, country and planet more *resilient*."

* Thomas L. Friedman, *The New York Times*, May 24, 2014

Resilience Defined

"The term *resilience* refers to the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions. Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents.*

* Presidential Policy Directive 21 - Critical Infrastructure Security and Resilience February 12, 2013

Threat Centric vs. Resilience Centric Approach to Managing Risk

***Threat-Centric* approach emphasizes the role of intelligence to detect and intercept threat in order to drive down risk**

Risk = Threat x Vulnerability x Consequence

Threat = Intent x Capability

The probability that something will be targeted for an attack is dependent on the adversary possessing both the *intent* and the *capability* to attack it.

- If something is very *vulnerable*, than an adversary needs less *capability* to attack it.
- If an attack is likely to generate significant *consequences*, than a determined adversary will be motivated to carry it out; i.e., the adversary will have greater *intent*.

Needs and Objectives for Advancing Critical Infrastructure Resilience

Resilience helps reduce the risk of terrorism by undermining the threat

Lower Vulnerability & Lower Consequence = Lower Threat

Actions taken to reduce vulnerability will translate into an adversary needing to possess greater *capability* to overcome the safeguards. This reduces the number of likely adversaries.

Less consequence will undermine *intent*; i.e., there is little motivation for carrying out an attack if it does not achieve mass destruction and disruption.

Lower Threat, Lower Vulnerability & Lower Consequence = Reduced Risk

Investments in resilience measures that lower vulnerability and consequence end up reducing risk and therefore serve as a ***deterrent.***

The limits of a threat-centric approach to safeguarding critical infrastructure

January 2014 Elk River, West Virginia chemical spill

Superstorm Sandy and Metro NY-NJ Liquid Fuels Distribution Oct 2012

Superstorm Sandy's Impact on NY/NJ Liquid Fuels Distribution System

SUPPLY (42m gallons of petroleum products per day)

- Port closure during and following the storm halted all maritime shipments. (60+%)
- Bayway Refinery and Hess Port Reading Refinery disabled due to loss of commercial and generator power, damage to marine terminal, and damage to electrical equipment. (20%)
- Colonial Pipeline stopped deliveries to northern NJ due to damage to receiving terminals and power outages impacted its operations. This slowed product movement throughout entire pipeline back to the Gulf Coast (15%)

DISTRIBUTION:

- Damage to dock facilities disrupted barge movements of gasoline
- Gas station closures: 60% of NJ; 70% of Long Island
- Gas rationing implemented in New Jersey (11 days) and New York (15 days)

http://www.eia.gov/special/disruptions/hurricane/sandy/petroleum_terminal_survey.cfm

Five Impediments to achieving critical infrastructure and cyber resilience

1. Overconfidence in Current Capacities to Respond
2. Lack of an integrative approach
3. Pervasive Disincentives
4. Dearth of Appropriate Governance Frameworks
5. Inadequate Training and Education

1. Overestimation of Current Capacities to Respond

- Public complacency is fueled by a tendency of public officials and “professional protectors” to overstate their ability to manage risk.
- Building consensus for investing in more resilient infrastructure is undermined by vocal naysayers who discount scientific evidence that substantiates risk; e.g., climate change.
- Near term preoccupations with cost avoidance overwhelm long term considerations of the value of investing in infrastructure generally and infrastructure resilience specifically.

2. Lack of an integrative approach

- Approaches to resilient infrastructure have been largely sector specific and in response to discrete hazards.
- Security sensitivities associated with critical infrastructure work against raising cross-sector awareness of interdependencies and the associated risk of cascading failures.
- Most ongoing resilience research is isolated within specific academic disciplines.
- Too little understanding of cyber risk amongst physical infrastructure owners and operators.

3. Pervasive Disincentives

- Public and private entities have become skilled at transferring risk.
- The transfer of risk undermines collaborative work to take on risk directly and comprehensively.
- There are few accepted resilience standards or validated best practices for which markets can provide rewards to those organizations that invest in resilience.

4. Inadequate Governance Frameworks for Organizing Collective Efforts

- The management of efforts to enhance resilience within and amongst interdependent systems and networks do not align with existing governance frameworks that are sector specific.
- Most infrastructure systems, such as energy and water, sprawl multiple and differing political jurisdictions.
- Ownership and operations are public and private, large and small, and highly regulated and loosely regulated, inhibiting local actions due to incompatibility across stakeholders.

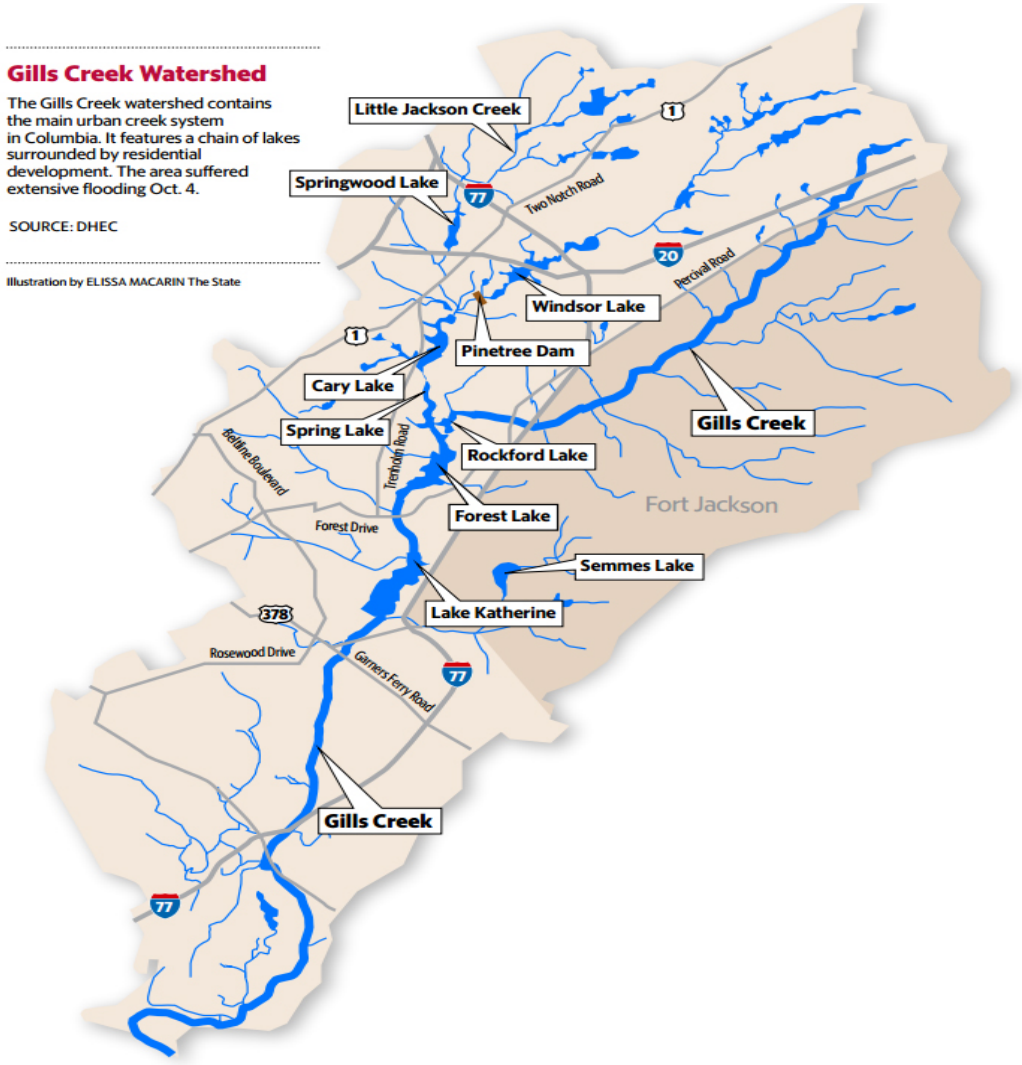
5. Lack of Adequate Training and Education

- Training and education programs favor specialization over developing a general understanding of cyber-physical relationships and associated risks.
- Universities manage separately the kinds of technical, non-technical, professional, and research programs that are all needed for developing a deeper understanding and building more comprehensive capabilities for advancing critical infrastructure and cyber resilience.

South Carolina Flooding 2015:

- On October 1-5, 2015, a low pressure system combined with Hurricane Joaquin causing record rainfall and flooding throughout the state.
- The Midlands region of South Carolina received 17 – 24 inches of rain and other areas gathered 6 – 15 inches of rain
- The extreme precipitation caused widespread flooding that resulted in cascading failures throughout infrastructure systems.
- 160,000 homes were damaged, over 500 roads and bridges had to be closed, 36 dams failed, and 19 lives were lost.

These homes on Lake Katherine were surrounded by floodwaters.
(Source: Churck Burton/AP via ABCNews)



Gills Creek Watershed (Source: Elissa Macarin, The State)

Findings:

1. The resilience of the infrastructure systems located in and around watersheds requires a coordinated system of watershed governance.

2. The tension between local and private interests versus the requirements of a holistic approach to regional watershed management can compromise effective post-disaster recovery and adaptation.

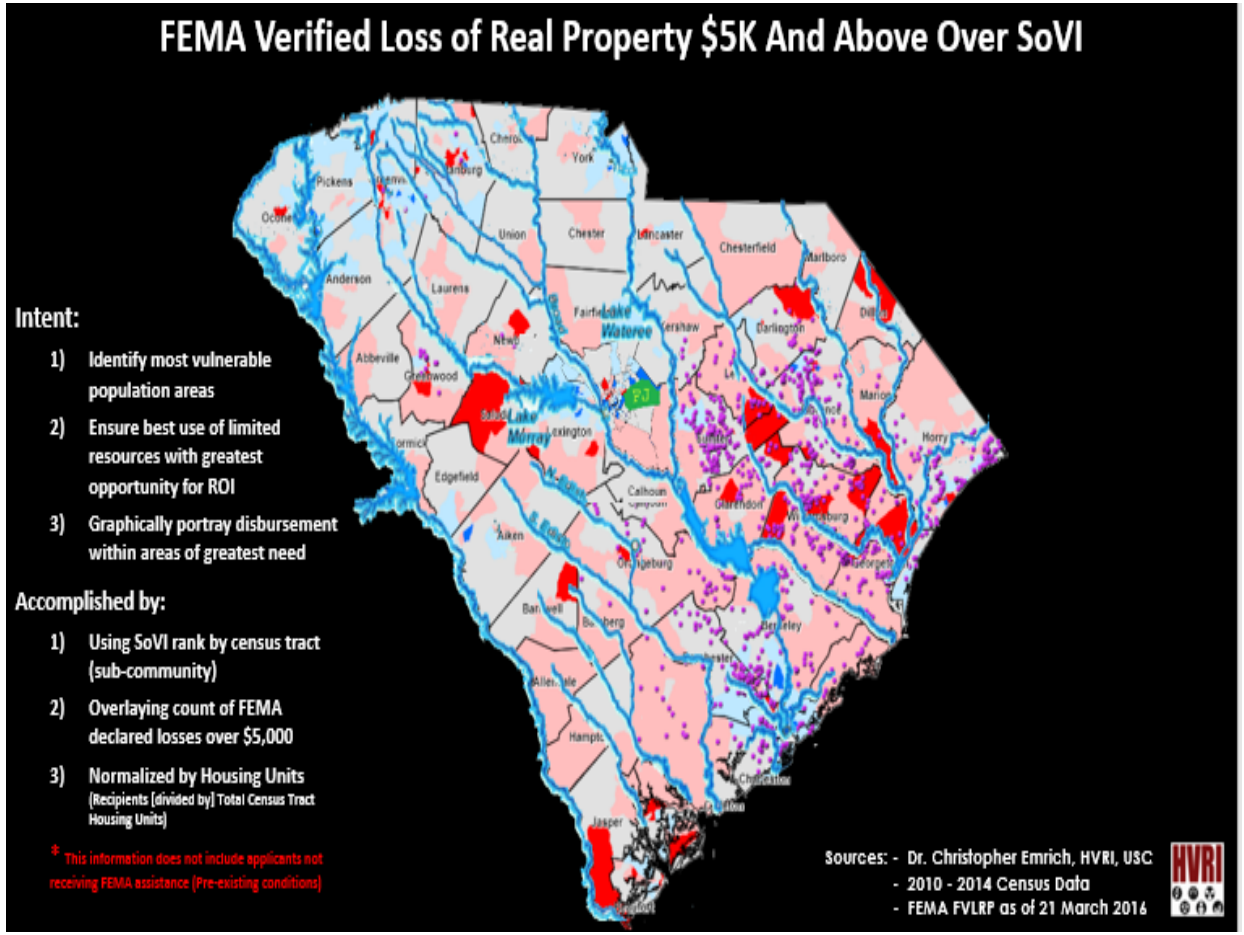
Findings Continued:

3. There is a very challenging bureaucratic environment for state and local officials to navigate, particularly with respect to moving from disaster response to long-term recovery and adaptation.

4. Decision makers and key stakeholders need information and visualization tools that advance an understanding of complex watershed interdependencies and how they can be best managed.

Governor Nikki Haley speaks with President Barack Obama on Monday, October 5, 2015
(Source: @RobGodfrey/Twitter via South Carolina Radio Network)

Findings Continued:



A view of the Social Vulnerability Index (SoVI) developed by the Hazards and Vulnerability Research Institute at the University of South Carolina (Source: Dr. Susan Cutter, HVRI, USC)

5. State and local expectations of federal support for recovery are misaligned relative to current federal planning and available resources.

6. Recovery and resilience planning at city, state, and regional levels would benefit from active dialogue and close cooperation with the academic community.

A research agenda for Resiliency

1. Modeling complex interdependent systems
2. Decision-support tools and analytic methods for complex system management
3. Engineering resilience by design
4. Measures and rewards
5. Resilience governance
6. Resilience training and education

CONCLUSIONS

- Large-scale disasters impact regional infrastructure systems and therefore require an enhanced capacity for undertaking preparedness, response, and recovery at a regional level.

- Resilience requires a deeper understanding and new governance frameworks to manage the interdependencies and associated risk of cascading failures.

- Companies and communities need to “bake-in” resilience into their critical systems and functions.

- Critical infrastructure resilience needs to recognized as both *security* and *competitiveness* imperatives. For those who have a choice, people and companies will seek to live and invest in those places that possess resilience and gravitate away from those that do not.