Quantifying Risk and Resilience in Multilayer Systems

Igor Linkov

Risk and Decision Sciences Team Lead, US Army

Igor.linkov@usace.army.mil, 6172330969

Supported in parts by DTRA under

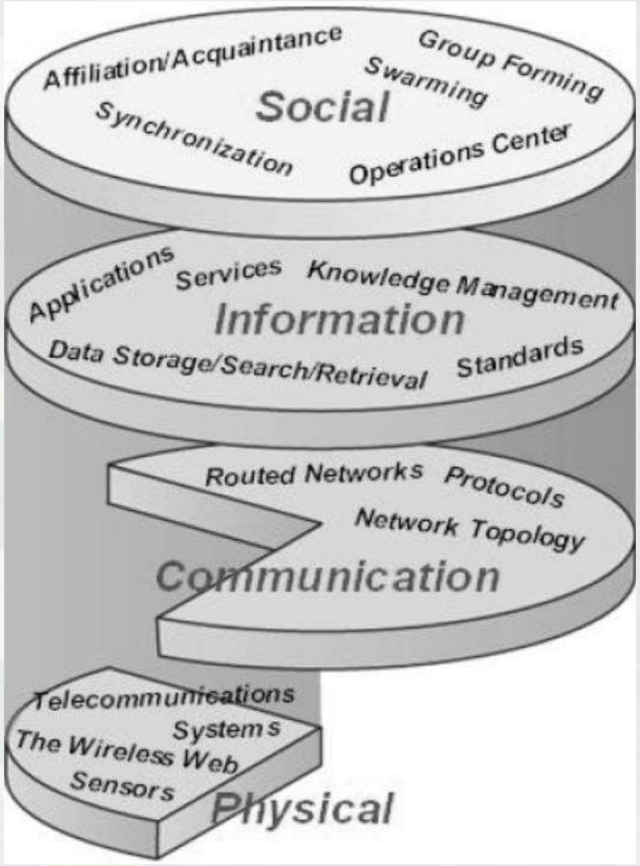
6.1 Network Science Trust (PM Paul Tandy) and

JIDO JLB Program

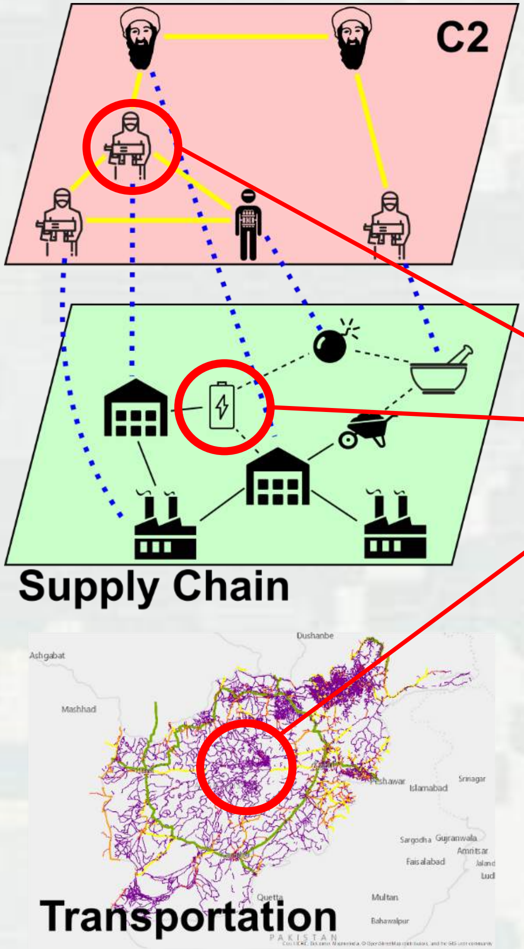
US Army Corps of Engineers®

Vision for SMA Needs

Real world



Model



Operations

Portfolio of Targets to Reduce or Alternatives to Increase Resilience

NATURE CLIMATE CHANGE | VOL 4 | JUNE 2014 | www.nature.com/natureclimatechange

COMMENTARY:

Changing the resilience paradigm

Igor Linkov, Todd Bridges, Felix Creutzig, Jennifer Decker, Cate Fox-Lent, Wolfgang Kröger,

The human body is resilient in its ability to persevere through infections or trauma. Even through severe disease, critical life functions are sustained and the body recovers, often adapting by developing immunity to further attacks of the same type. Our society's critical infrastructure — cyber, energy, water, transportation and communication — lacks the same degree of resilience, typically losing essential functionality following adverse events.

"Your body has an incredible system called white blood cells that attack and try to manage that virus in such a way that prevents it from harming the body. The systems in 2030 will have something very similar."

Tom Vice*, president of Northrop's aerospace sector, on 6th Gen Fighter*

Calls for Increased Resilience

The White House

Office of the Press Secretary

For Immediate Release October 31, 2013

Presidential Proclamation -- Critical Infrastructure Security and Resilience Month, 2013

CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE MONTH, 2013

BY THE PRESIDENT OF THE UNITED STATES OF AMERICA

A PROCLAMATION

Over the last few decades, our Nation has grown increasingly dependent on critical infrastructure, the b
our national and economic security. America's critical infrastructure is complex and diver
both cyberspace and the physical world -- from power plants, bridges, and interstates to
massive electrical grids that power our Nation. During Critical Infrastructure Security and
resolve to remain vigilant against foreign and domestic threats, and work together to furt
systems, and networks.

"**resilience**" means the ability to anticipate, prepare for, and adapt to changing conditions and withstand, respond to, and recover rapidly from disruptions.

The White House

Office of the Press Secretary

For Immediate Release May 11, 2017

Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure

EXECUTIVE ORDER

(vi) Effective immediately, it is the policy of the executive branch to build and maintain a modern, secure, and more **resilient executive branch IT architecture**.

Risk -- "a situation involving exposure to danger [threat]."

Security -- "the state of being free from danger or threat."

Resilience -- "the capacity to recover quickly from difficulties."

Definitions by Oxford Dictionary

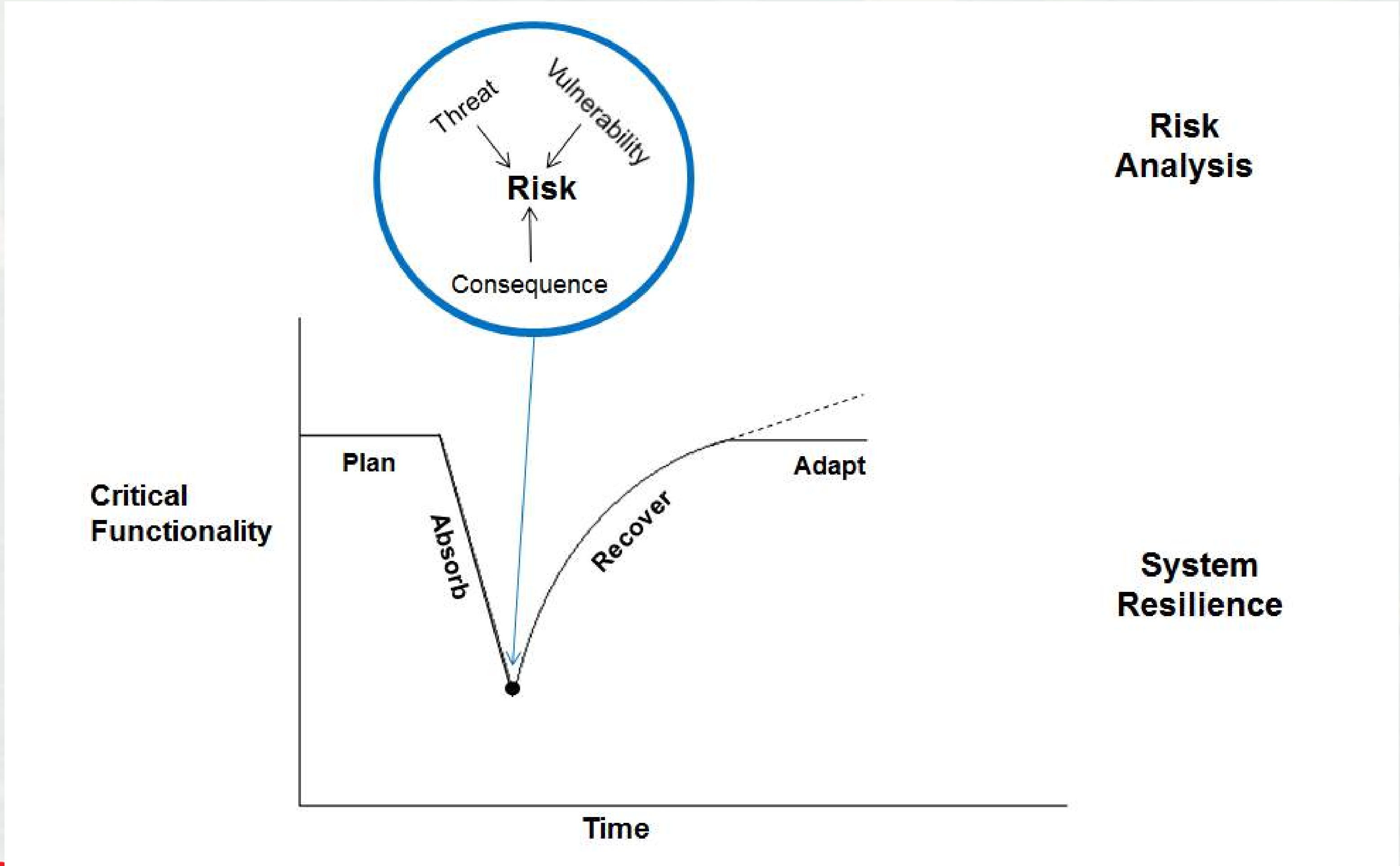
30 | NATURE | VOL 555 | 1 MARCH 2018

Don't conflate risk and resilience

'Risk' and 'resilience' are fundamentally different concepts that are often conflated. Yet maintaining the distinction is a policy necessity. Applying a risk-based approach to a problem that requires a resilience-based solution, or vice versa, can lead to investment in systems that do not produce the changes that

Igor Linkov, Benjamin D. Trump *US Army Corps of Engineers, Concord, Massachusetts, USA.*
Jeffrey Keisler *University of Massachusetts Boston, USA.*
igor.linkov@usace.army.mil

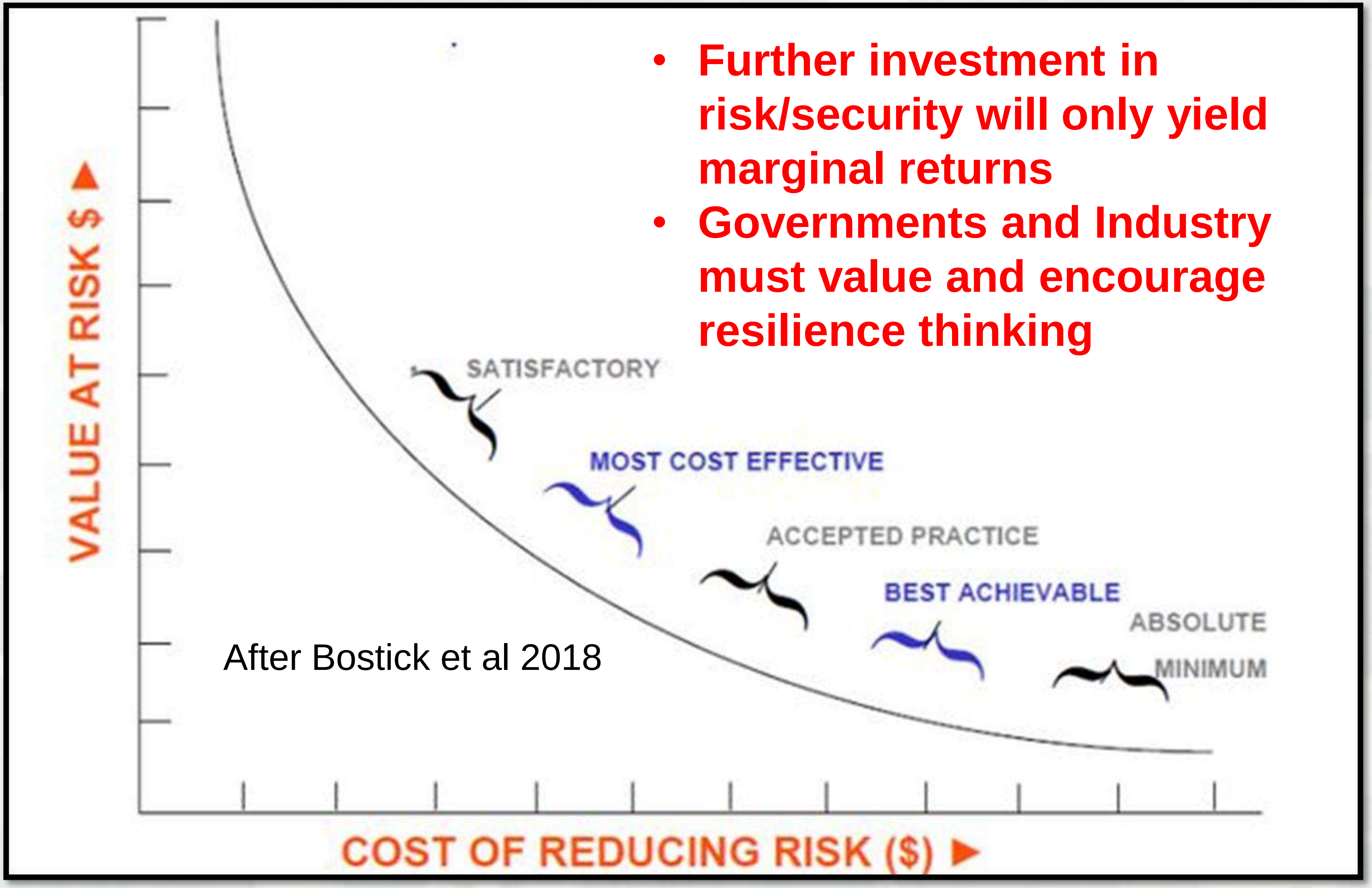
System Risk/Security and Resilience



After Linkov et al, Nature Climate Change 2014

Buying Down Risk vs Managing Resilience?

- Further investment in risk/security will only yield marginal returns
- Governments and Industry must value and encourage resilience thinking

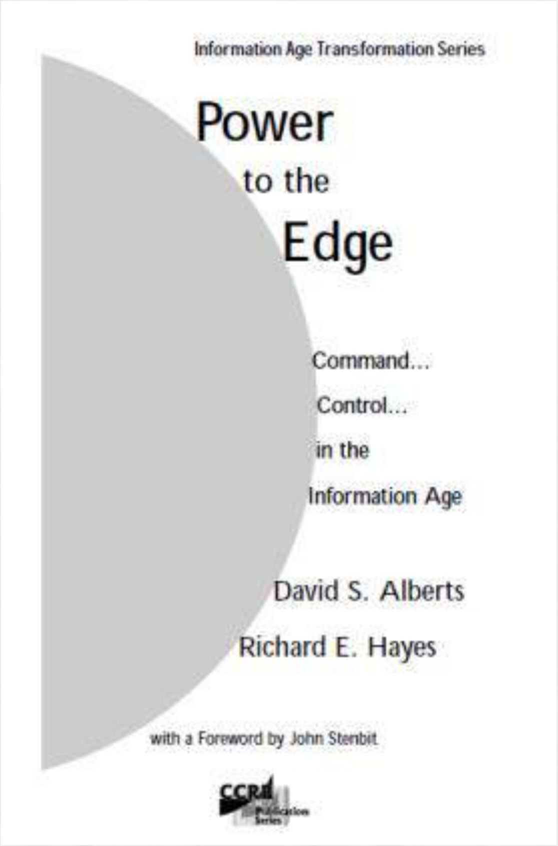


After Bostick et al 2018

Agenda

- Risk vs. Resilience
  - Terminology
  - Costs
- How to Measure Resilience
  - Resilience Matrix
  - Network Science
- One Layer: Transportation
- Two Layers: Stability of the Giant Connected Component
- Multiple Layers: Social, Command , Supply Chain, etc
- Smartness and Resilience
- Questions

Military Systems Doctrine as a Foundation for Resilience



Command and Control actions in a highly networked system is governed by *domains of warfare* that organize system components and establish a basis for measurement.

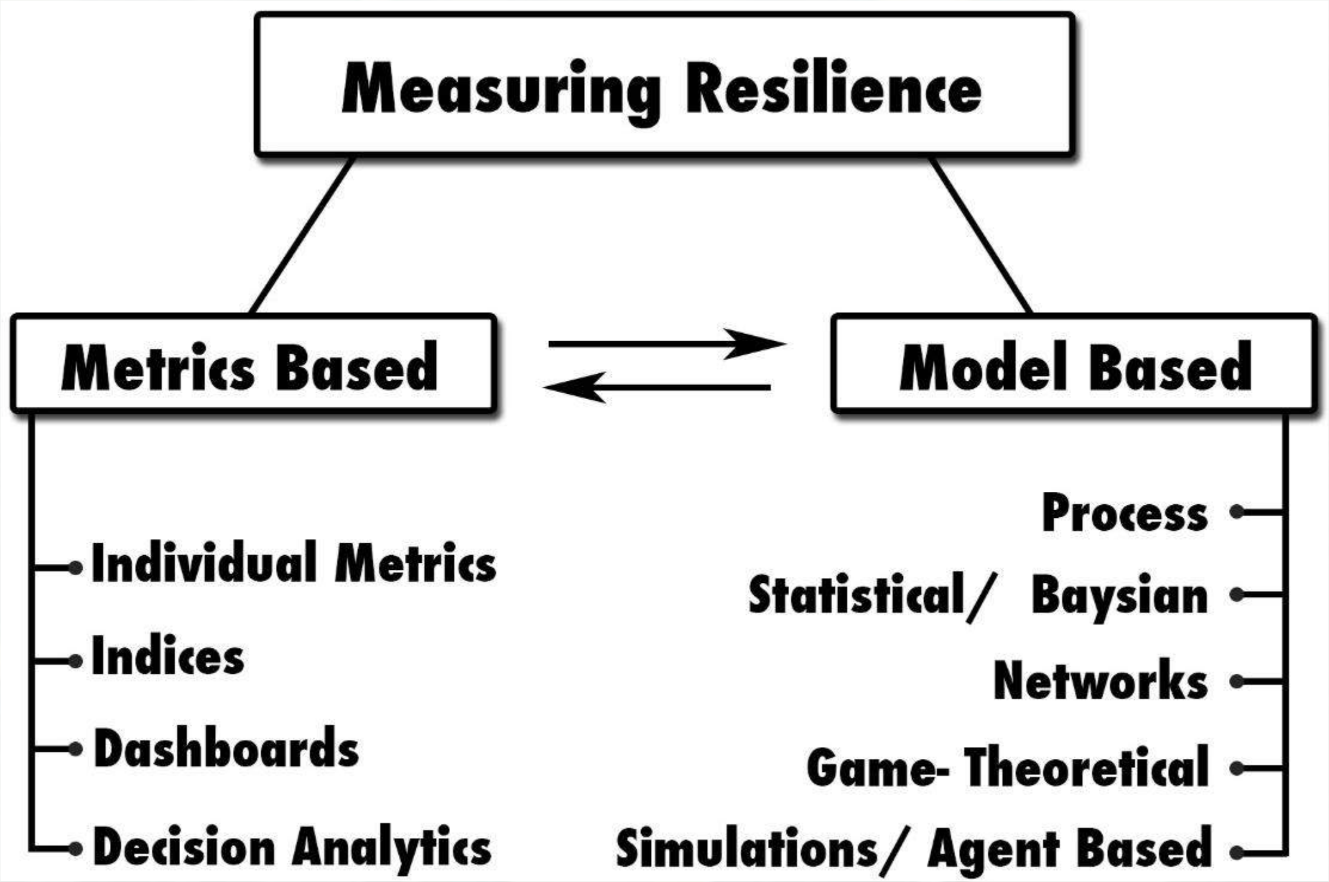
Physical: system performance in space and time.

Information: creation, manipulation and sharing information.

Cognitive: translating, sharing, and acting upon information to enable system management.

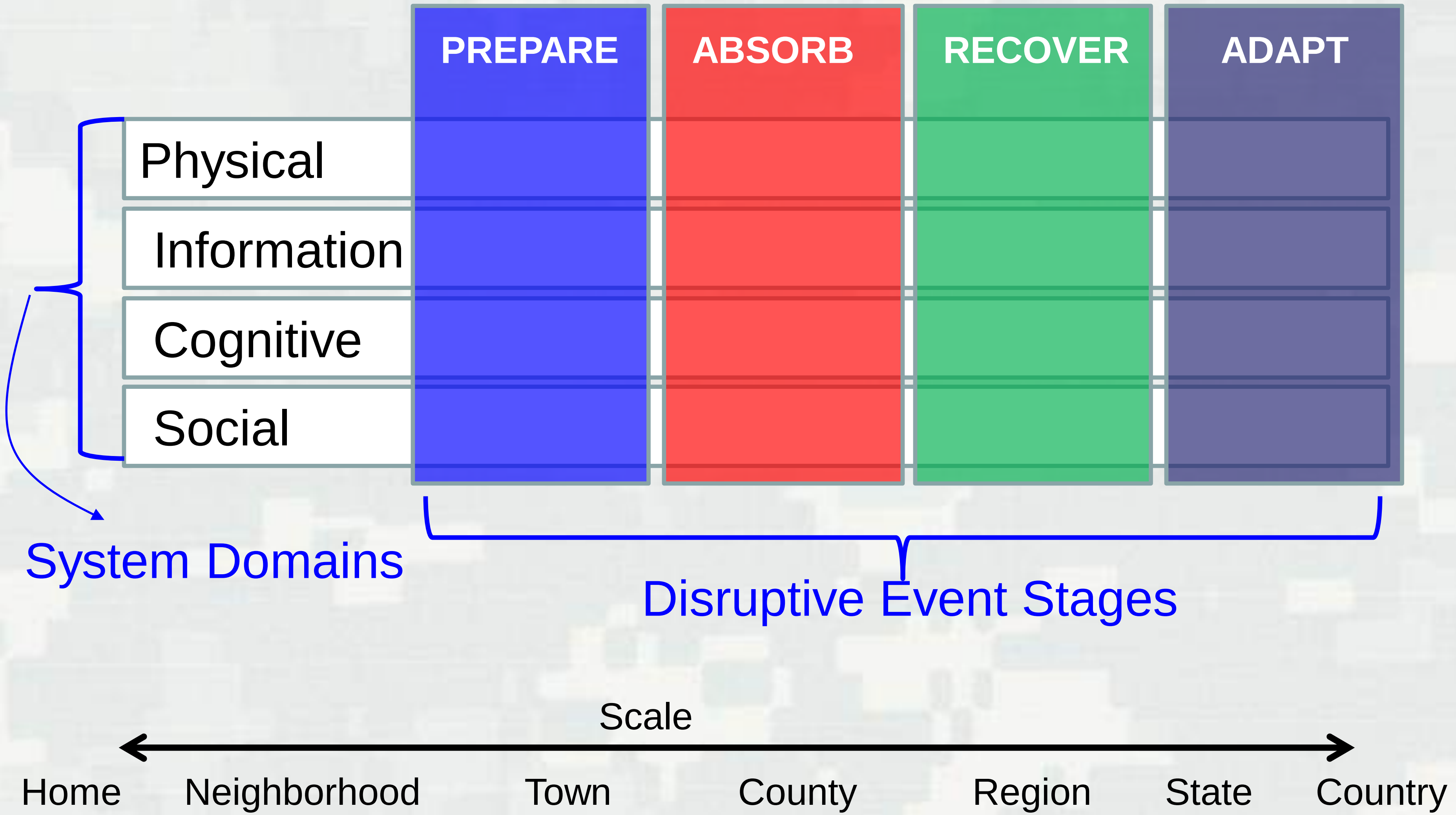
Social: interaction, collaboration and self-synchronization between individuals and entities.

How to Measure Resilience?



After Linkov and Kott, 2018

Resilience Matrix



Resilience Matrix: Cyber

Table 1 The cyber resilience matrix

Plan and prepare for	Absorb	Recover from	Adapt to
Physical			
(1) Implement controls/sensors for critical assets [S22, M18, 20]	(1) Signal the compromise of assets or services [M18, 20]	(1) Investigate and repair malfunctioning controls or sensors [M17]	(1) Review asset and service configuration in response to recent event [M17]
(2) Implement controls/sensors for critical services [M18, 20]	(2) Use redundant assets to continue service [M18, 20]	(2) Assess service/asset damage	(2) Phase out obsolete assets and introduce new assets [M17]
(3) Assessment of network structure and interconnection to system components and to the environment	(3) Dedicate cyber resources to defend against attack [M16]	(3) Assess distance to functional recovery	
(4) Redundancy of critical physical infrastructure		(4) Safely dispose of irreparable assets	
(5) Redundancy of data physically or logically separated from the network [M24]			
Information			
(1) Categorize assets and services based on sensitivity or resilience requirements [S63]	(1) Observe sensors for critical services and assets [M22]	(1) Log events and sensors during event [M17, 22]	(1) Document incident's impact and cause [M17]
(2) Documentation of certifications, qualifications and pedigree of critical hardware and/or software providers	(2) Effectively and efficiently transmit relevant data to responsible stakeholders/ decision makers	(2) Review and compare systems before and after the event [M17]	(2) Document time between problem and discovery/discovery and recovery [S41]
(3) Prepare plans for storage and containment of classified or sensitive information			(3) Anticipate future system states post-recovery
(4) Identify external system dependencies (i.e., Internet providers, electricity, water) [S31]			(4) Document point of entry (attack)
(5) Identify internal system dependencies [S63]			
Cognitive			
(1) Anticipate and plan for system states and events [M18]	(1) Use a decision making protocol or aid to determine when event can be considered "contained"	(1) Rev physi in or decis	

Environ Syst Decis (2013) 33:471–476
DOI 10.1007/s10669-013-9485-y

PERSPECTIVES

Resilience metrics for cyber systems

Igor Linkov · Daniel A. Eisenberg ·
Kenton Plourde · Thomas P. Seager ·
Julia Allen · Alex Kott

Assessment using Commander Values

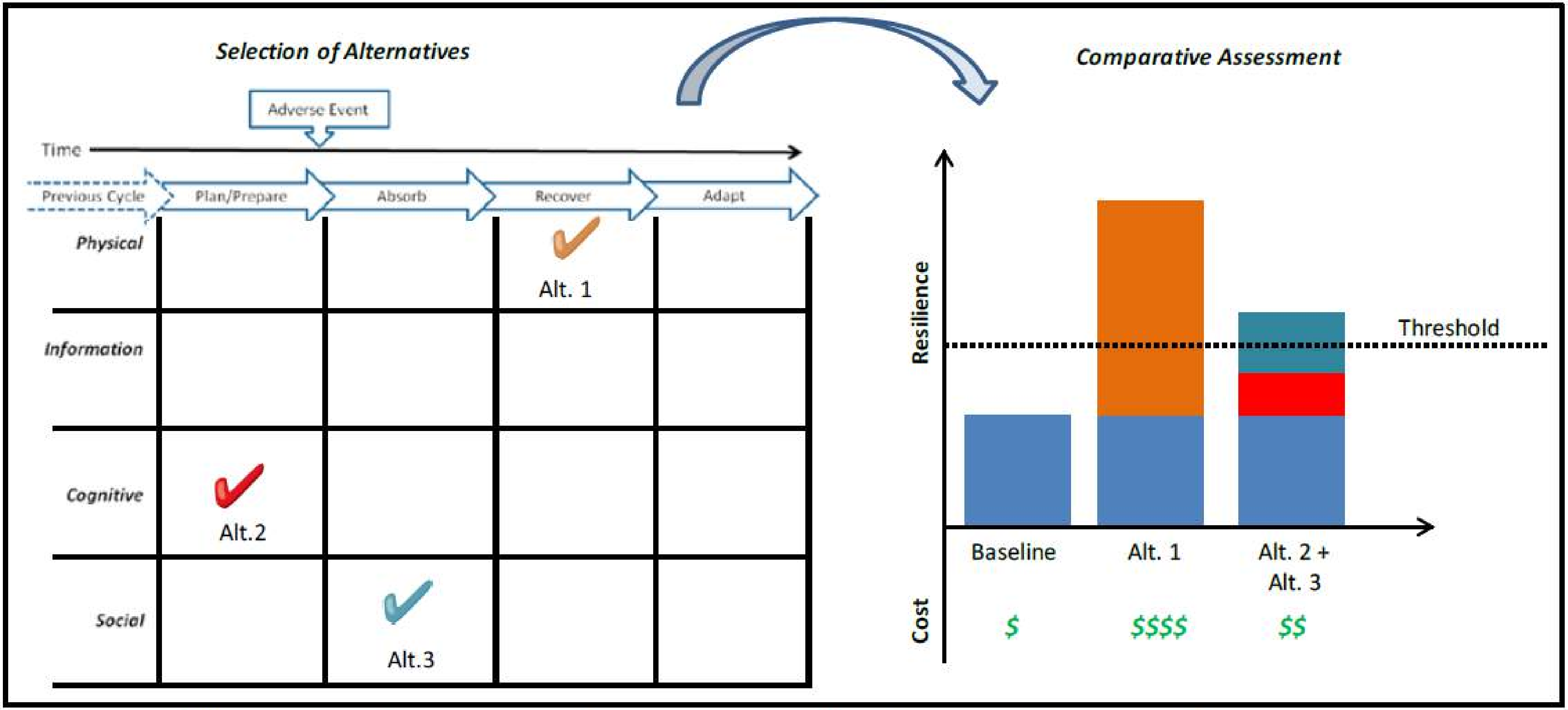


Figure 5: Comparative Assessment of Resilience-Enhancing Alternatives

Use developed resilience metrics to comparatively assess the costs and benefits of different courses of action

Results: Project Evaluation

- Baseline assessment can be used to evaluate proposed projects

	Prepare	Absorb	Recover	Adapt
Physical	71	16	60	10
Information	63	45	21	18
Cognitive	90	49	38	27
Social	82	54	12	52

43

Project 1

	Prepare	Absorb	Recover	Adapt
Physical	+10	+18	+9	+32
Information	+8		+17	
Cognitive				
Social				

	Prepare	Absorb	Recover	Adapt
Physical	81	34	69	42
Information	71	45	38	18
Cognitive	90	49	38	27
Social	82	54	12	52

51

Project 2

	Prepare	Absorb	Recover	Adapt
Physical				
Information		+5	+15	+22
Cognitive				
Social	+3		+12	+21

	Prepare	Absorb	Recover	Adapt
Physical	71	6	60	10
Information	63	50	36	40
Cognitive	90	49	38	27
Social	85	54	24	73

47

*Projects may have (+) or (-) in other matrices

Problems with Metrics-Based Approaches

- Measuring for security remains difficult: the gap between security measures and increased vulnerabilities can be hard to close

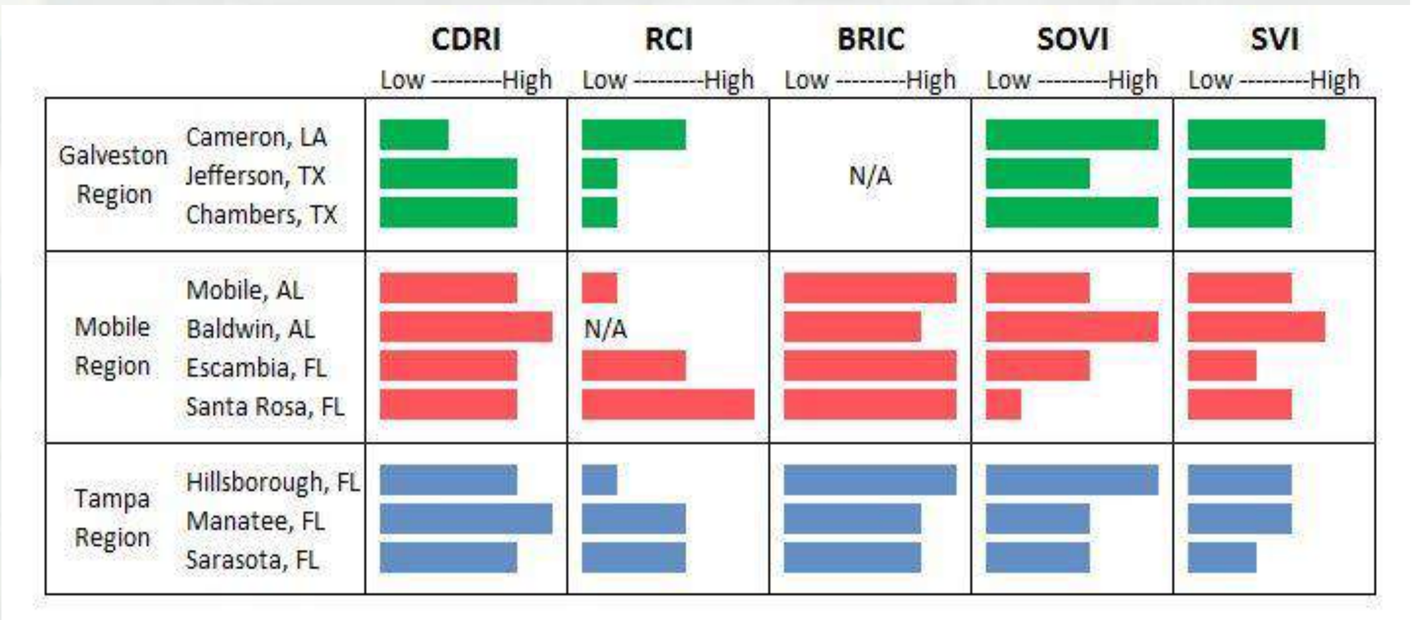
- Many measurement programs utilize data that does not contribute to informing decisions or changing behavior.

Not everything that counts can be counted, and not everything that can be counted counts.
Albert Einstein

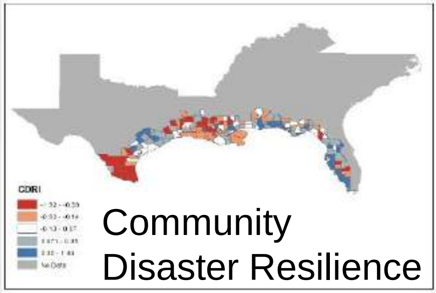
Validating Resilience Indices

- 5 county-level resilience and vulnerability indices
- Relative rather than absolute scores
- Different aggregations of much the same data

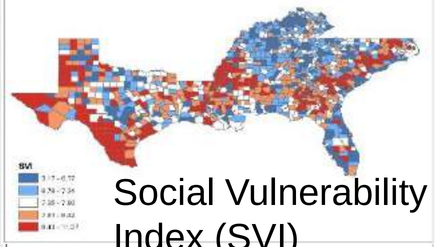
- **Results: Adjacent counties show different patterns of relative resilience/vulnerability**.



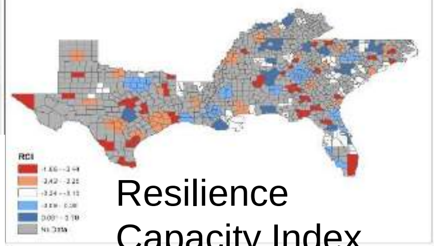
Bakkensen, Linkov et al (2016)



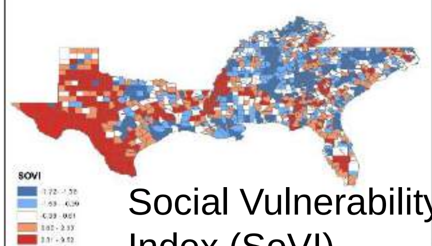
Community Disaster Resilience Index



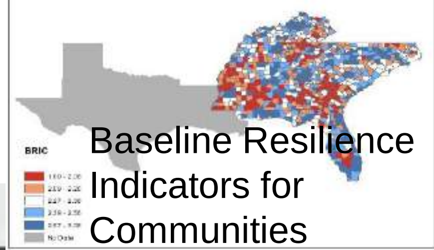
Social Vulnerability Index (SVI)



Resilience Capacity Index



Social Vulnerability Index (SoVI)



Baseline Resilience Indicators for Communities

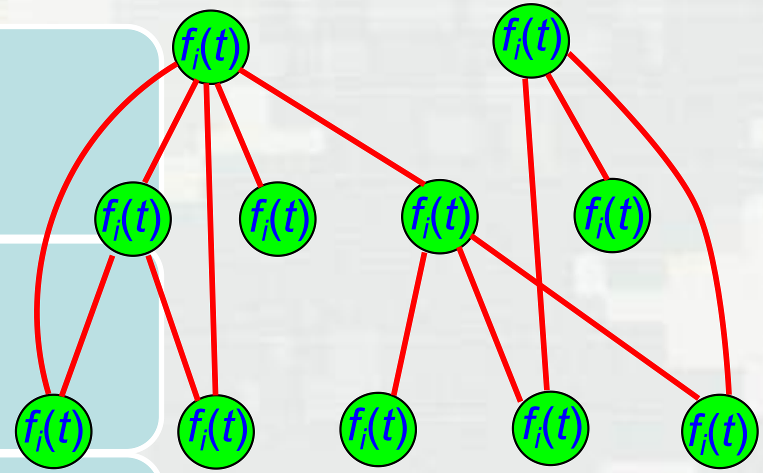
Network-based Resilience Theory?

System's *critical functionality* (K)

Network topology: *nodes* ($\mathcal{N}$) and *links* ($\mathcal{L}$)

Network *adaptive algorithms* ($\mathcal{C}$) defining how nodes' (links') properties and parameters change with time

A *set of possible damages* stakeholders want the network to be resilient against ($\boldsymbol{E}$)

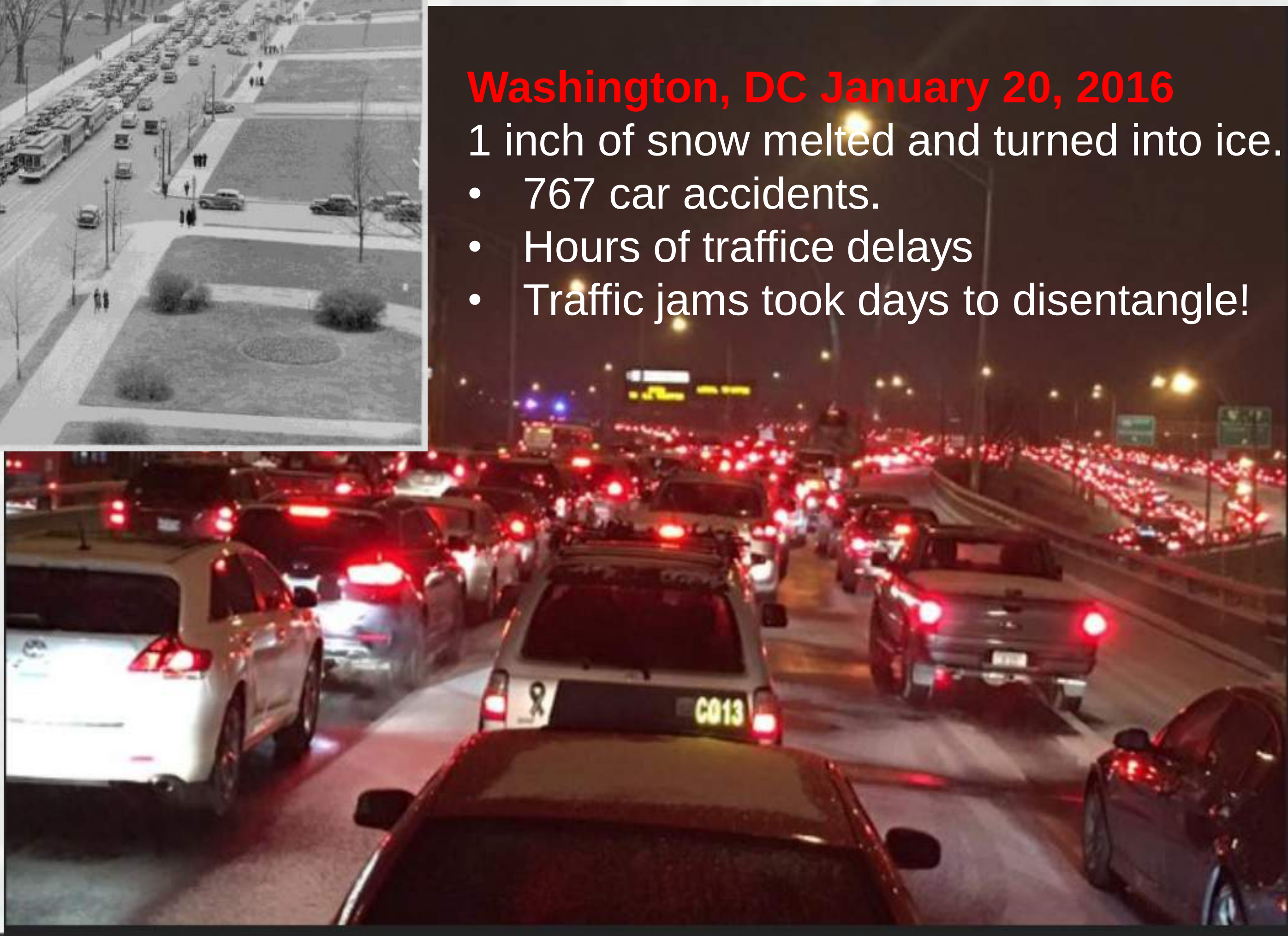


Ganin et al., 2016

$$R = f(\mathcal{N}, \mathcal{L}, \mathcal{C}, \boldsymbol{E})$$

Resilience: Transportation Network

Washington, DC 1937



Washington, DC January 20, 2016

1 inch of snow melted and turned into ice.

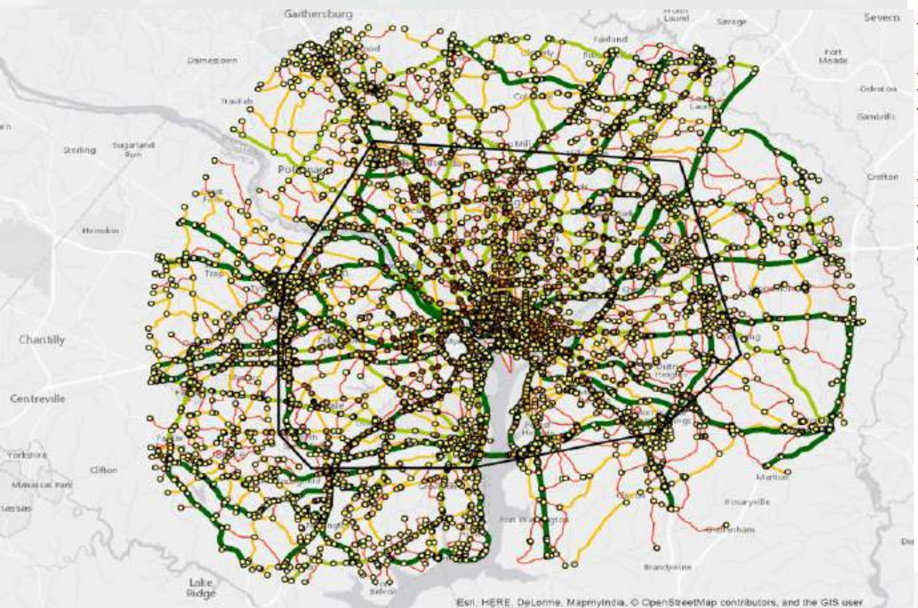
- 767 car accidents.
- Hours of traffice delays
- Traffic jams took days to disentangle!

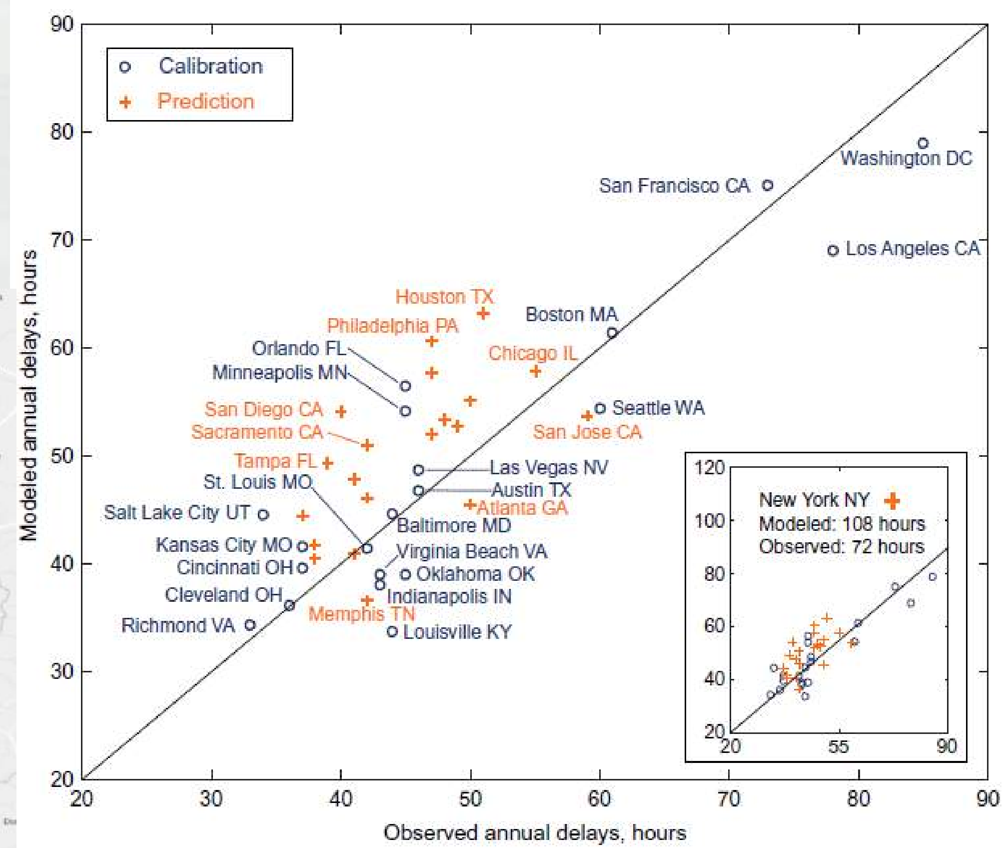
NETWORK SCIENCE

Resilience and efficiency in transportation networks

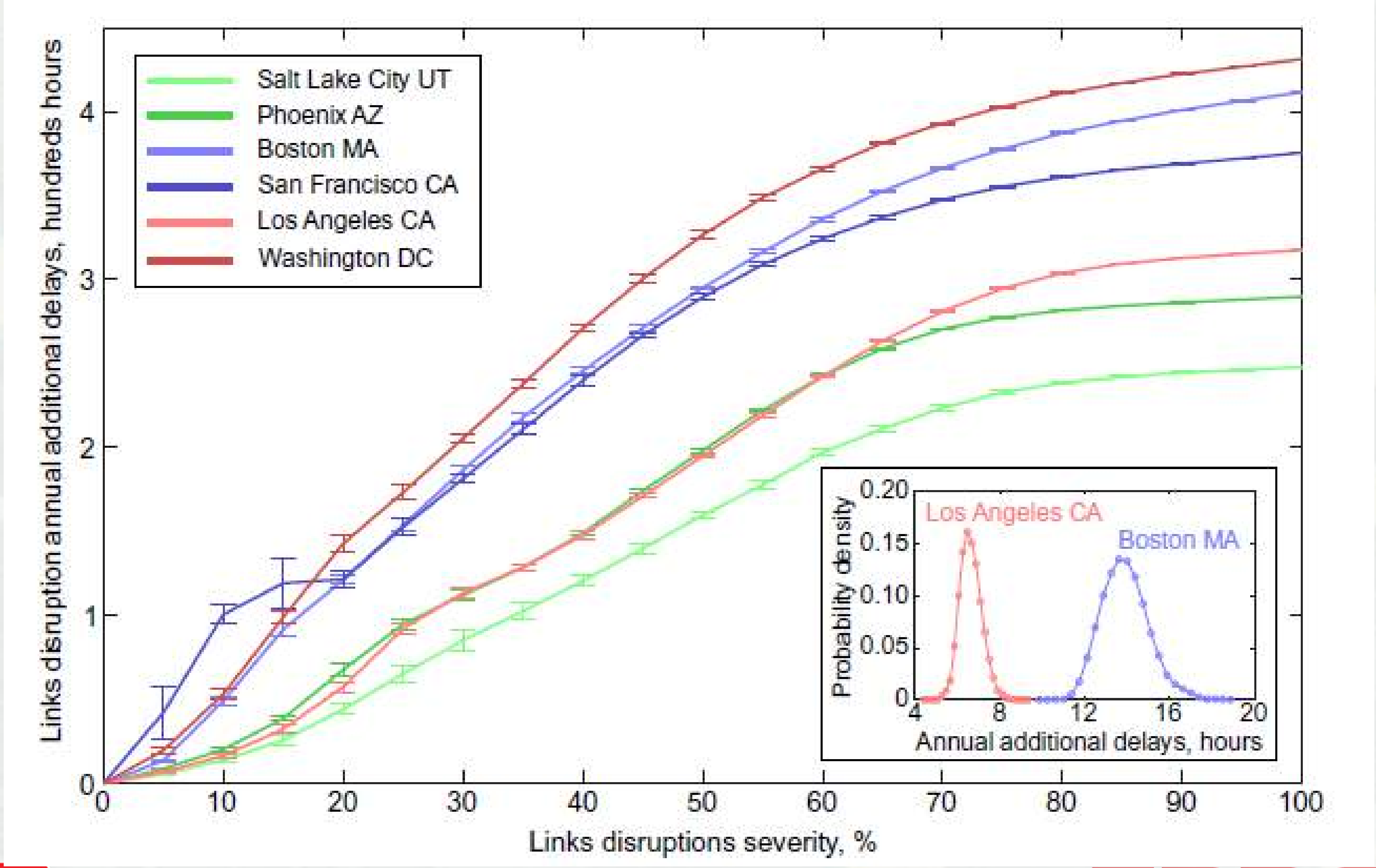
Alexander A. Ganin,[1,2] Maksim Kitsak,[3] Dayton Marchese,[2] Jeffrey M. Keisler,[4] Thomas Seager,[5] Igor Linkov[2]*

40 US Cities with Different Traffic Delays

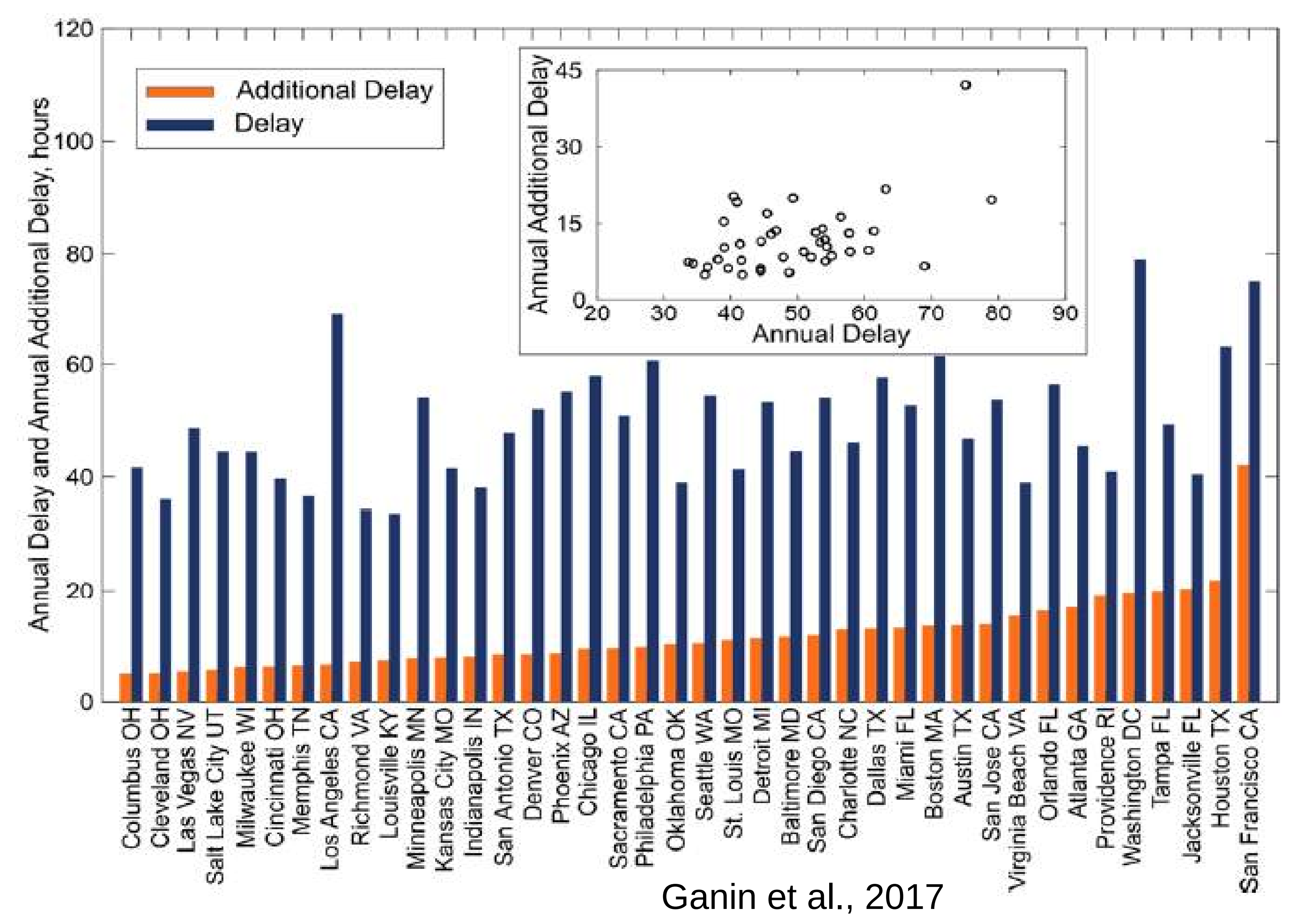




Transportation Networks in 40 Cities

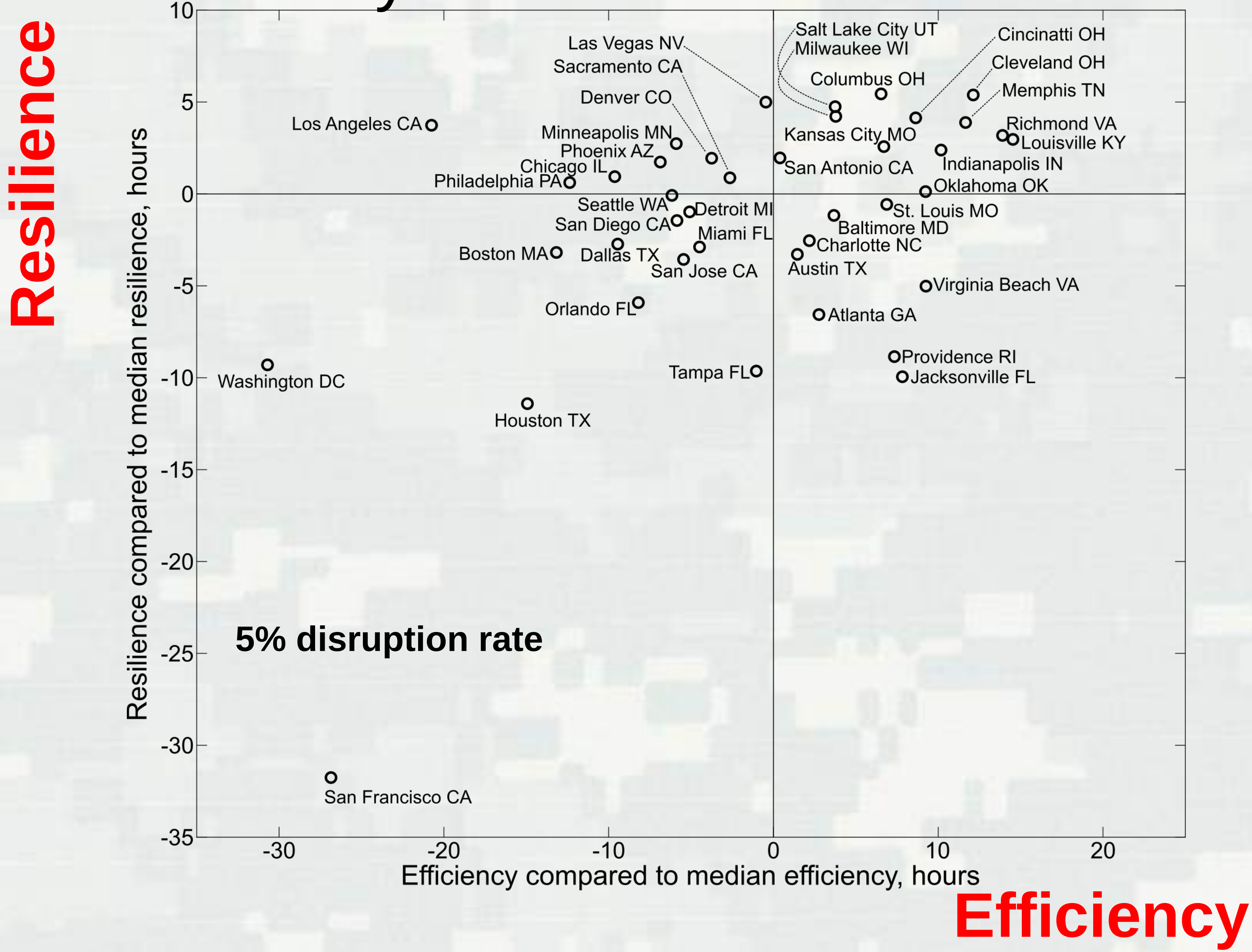


Efficiency vs. Resilience



Ganin et al., 2017

Efficiency and Resilience in 40 Cities



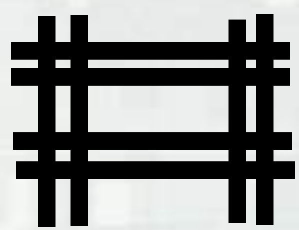
Resilience/Efficiency Costs and Management Strategies

$ Resilience

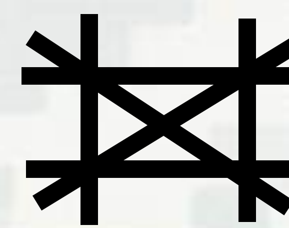
$ Efficiency

Current System

Design to Maximize Efficiency



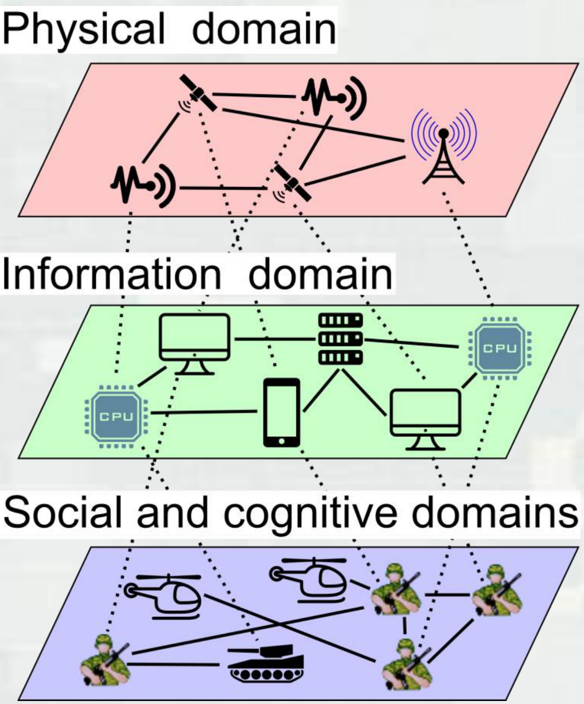
Design to Maximize Resilience



Real Networks are Interdependent

Military examples

A highly networked system is governed by *domains of warfare* that organize system components and establish a basis for measurement [1].



Civil examples

Modern infrastructure system are dependent on each other. Nodes pertaining to one infrastructure system affect nodes from the others and vice versa.

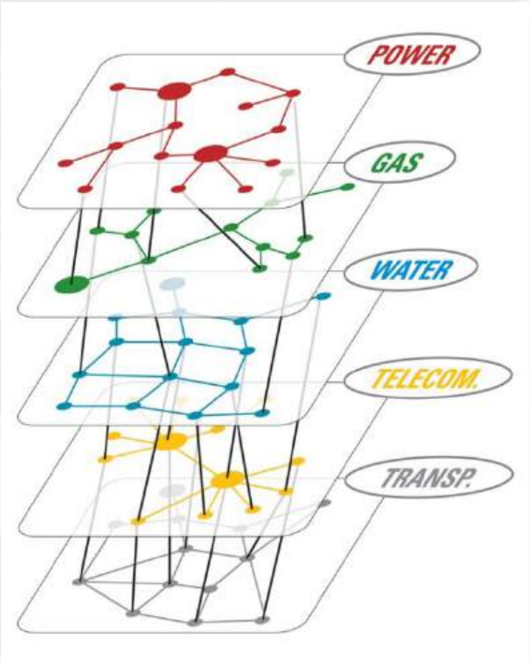


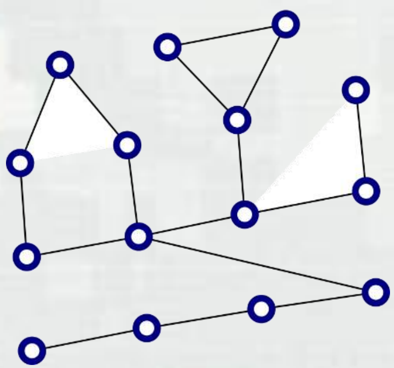
Illustration by L. Dueñas-Osorio et al [2].

1. D.S. Alberts and R.E. Hayes. *Power to the edge.* CCRP, 2005.
2. L. Dueñas-Osorio, A. Kwasinski. Quantification of lifeline system interdependencies after the 27 February 2010 Mw 8.8 Offshore Maule, Chile, Earthquake. *Earthquake Spectra*, 2012.

Random and Scale-free Networks

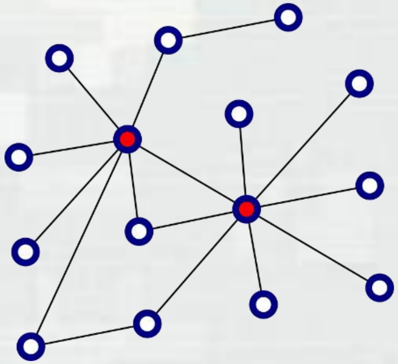
We consider two types of undirected networks: random and scale-free
The number of nodes in both networks is 200,000 and the number of links is 510,000
Average degree is 5.1

Random

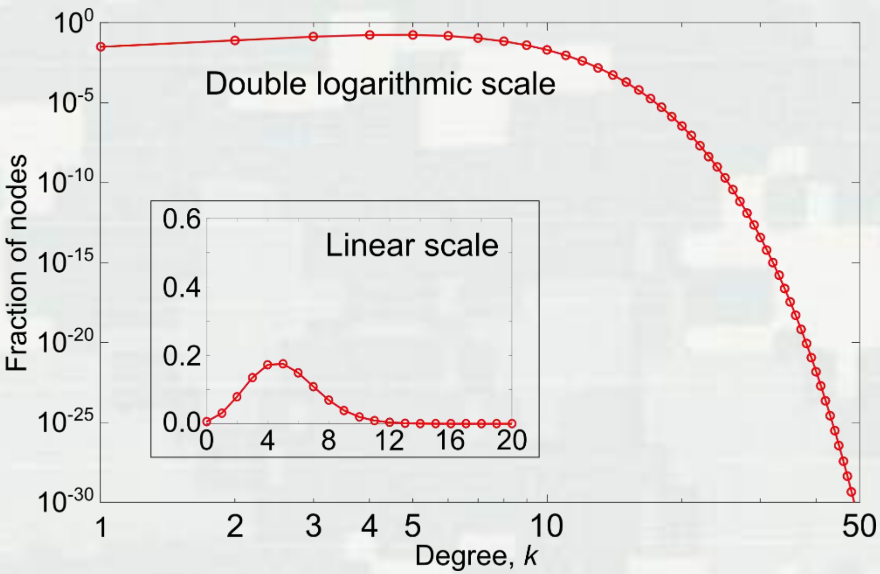


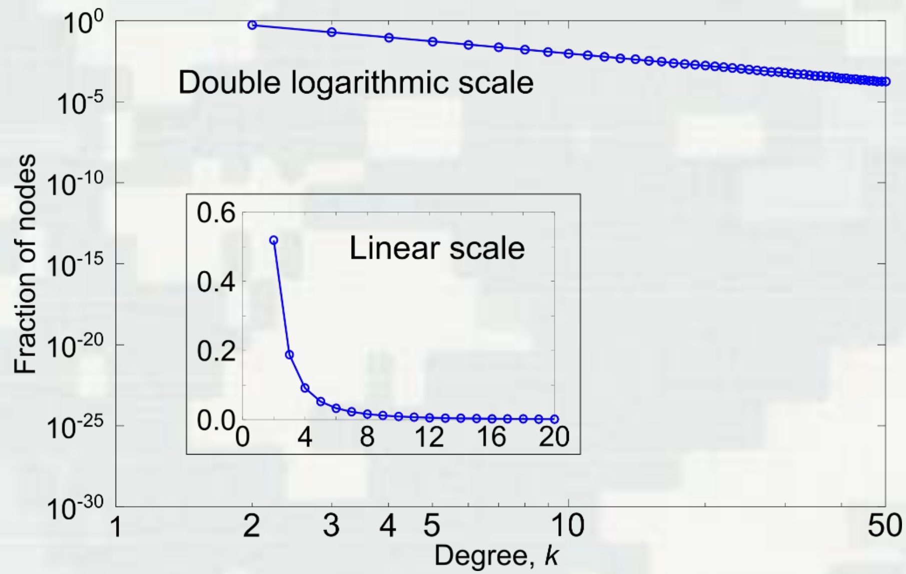
Links are distributed between nodes with equal probability

Scale-free



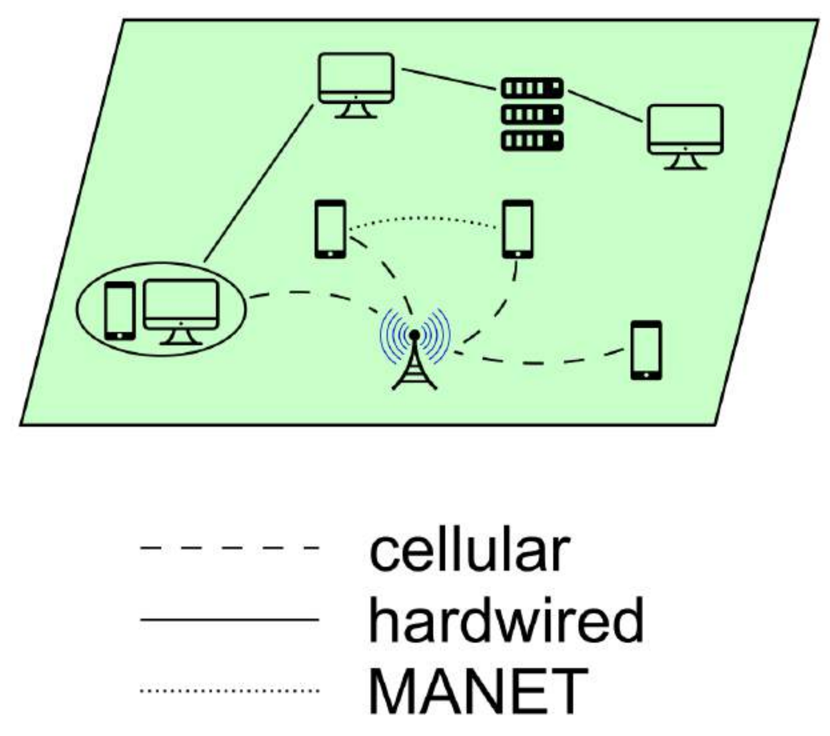
Links distribution favors highly connected nodes



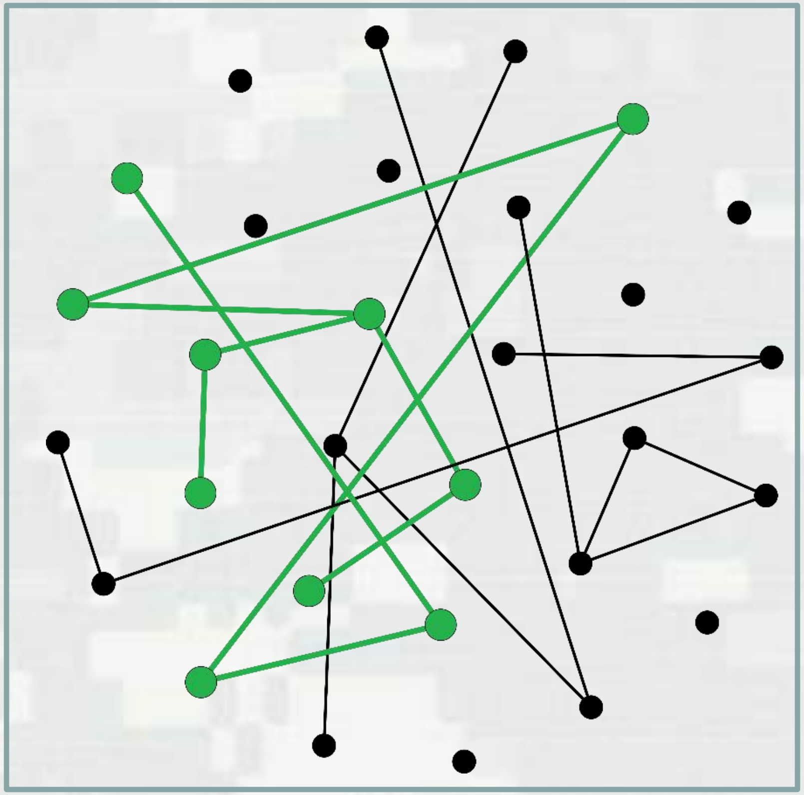


Importance of Connectedness

Conceptual Model

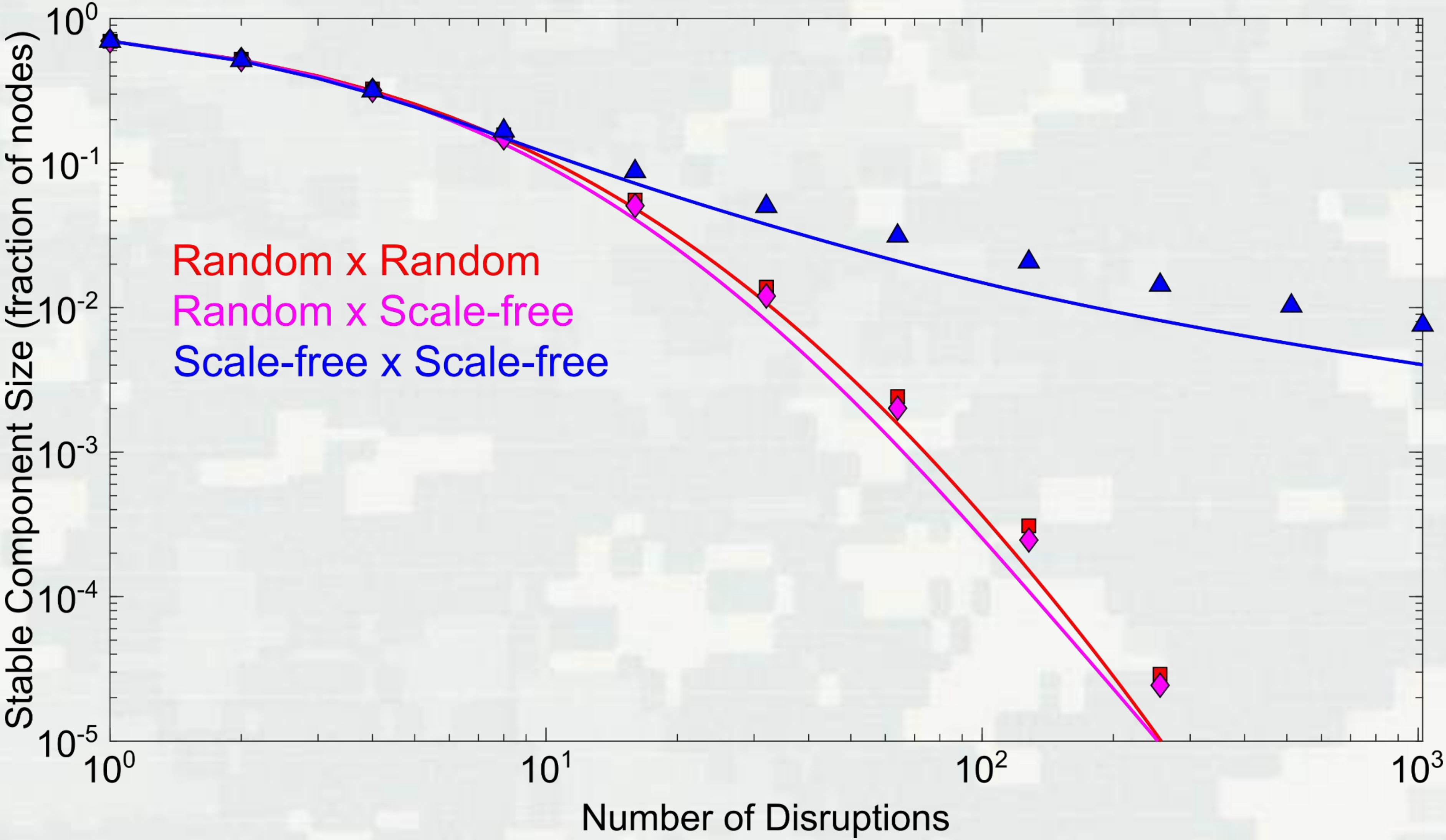


Graph representation



In undirected networks, typically there is a giant connected component (GCC) that fills most of the network – green nodes and links on the panel to the right. In certain infrastructure systems only nodes connected to the GCC can function normally.

Number of Disruptions and Stability of Connectedness

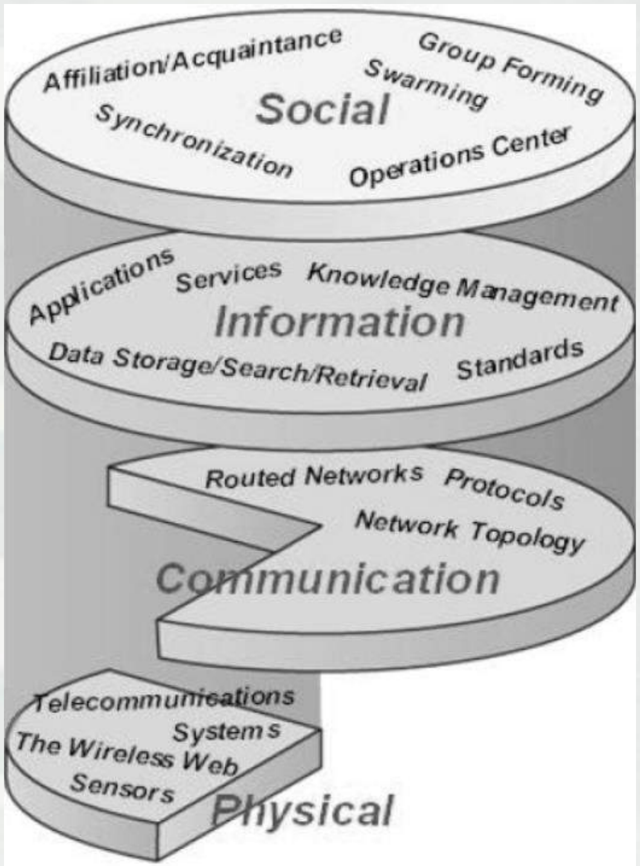


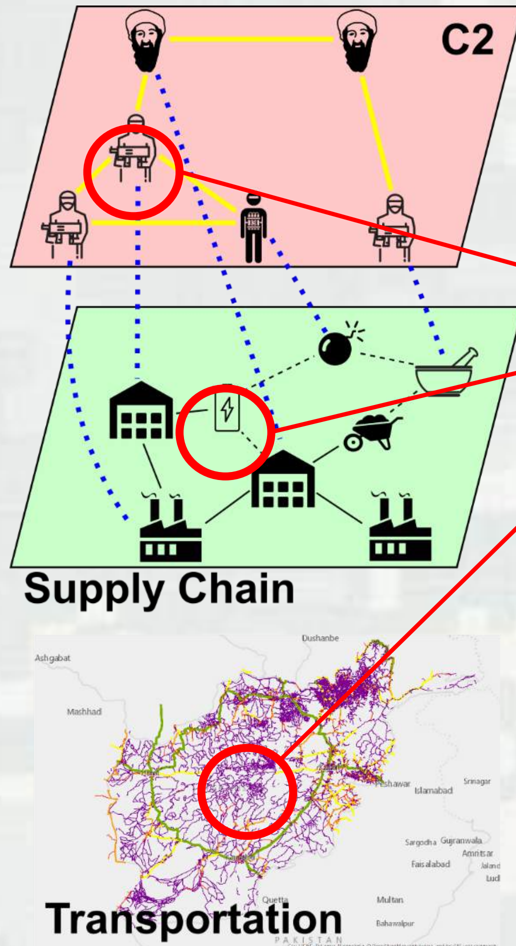
Vision for Resilience of Interconnected Networks

Real world

Model

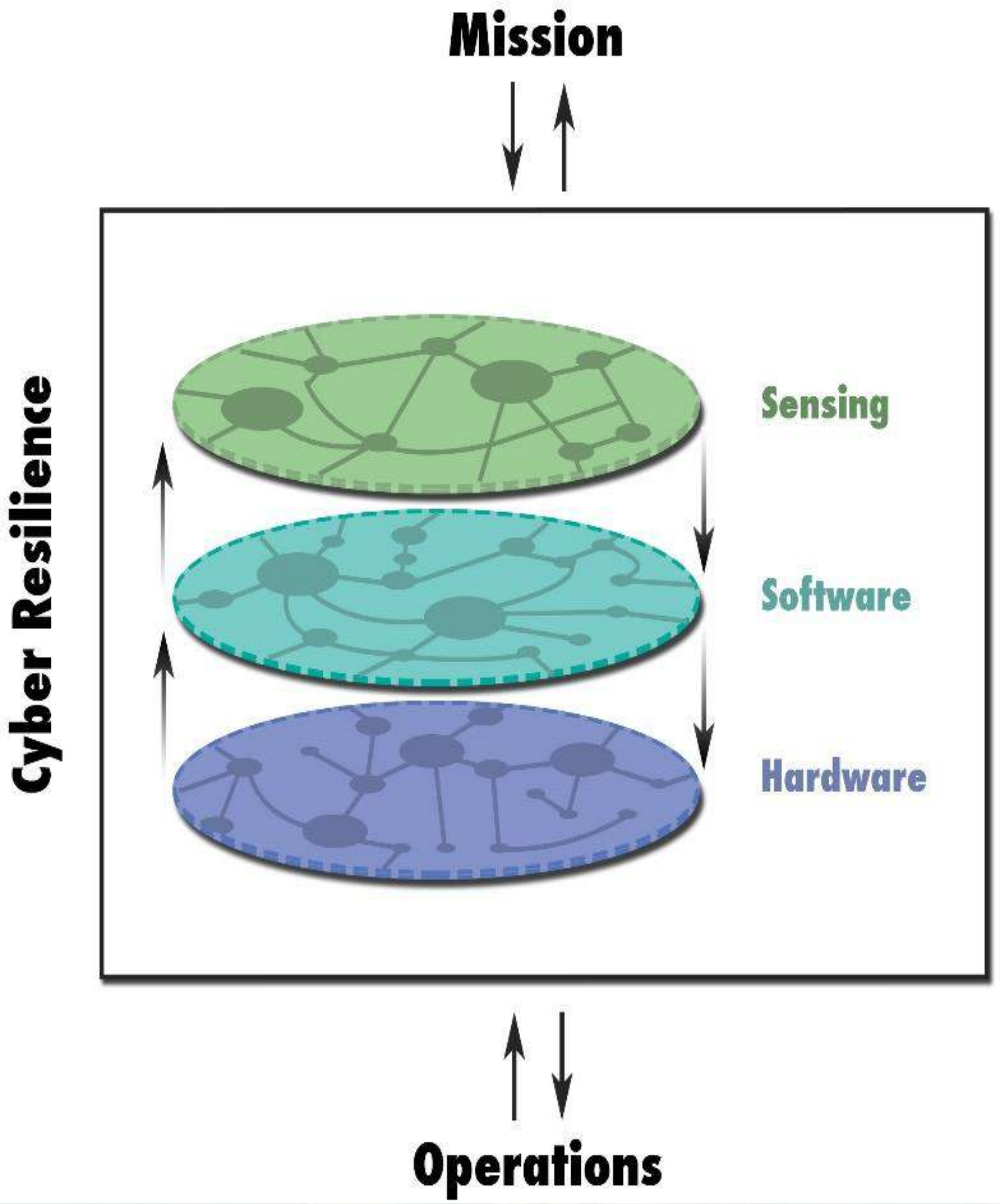
Operations





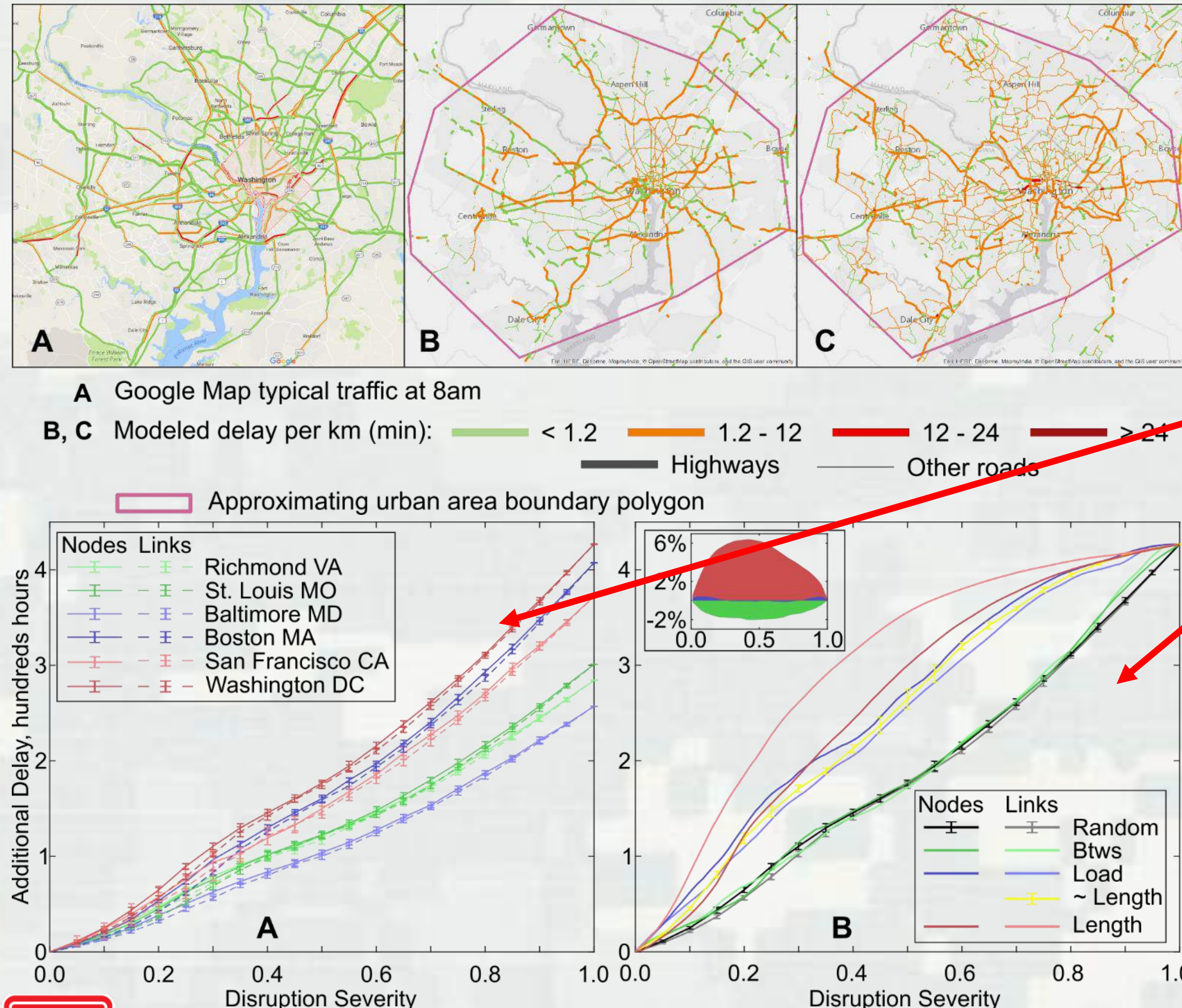
Management Alternatives

Cyber Resilience Domains



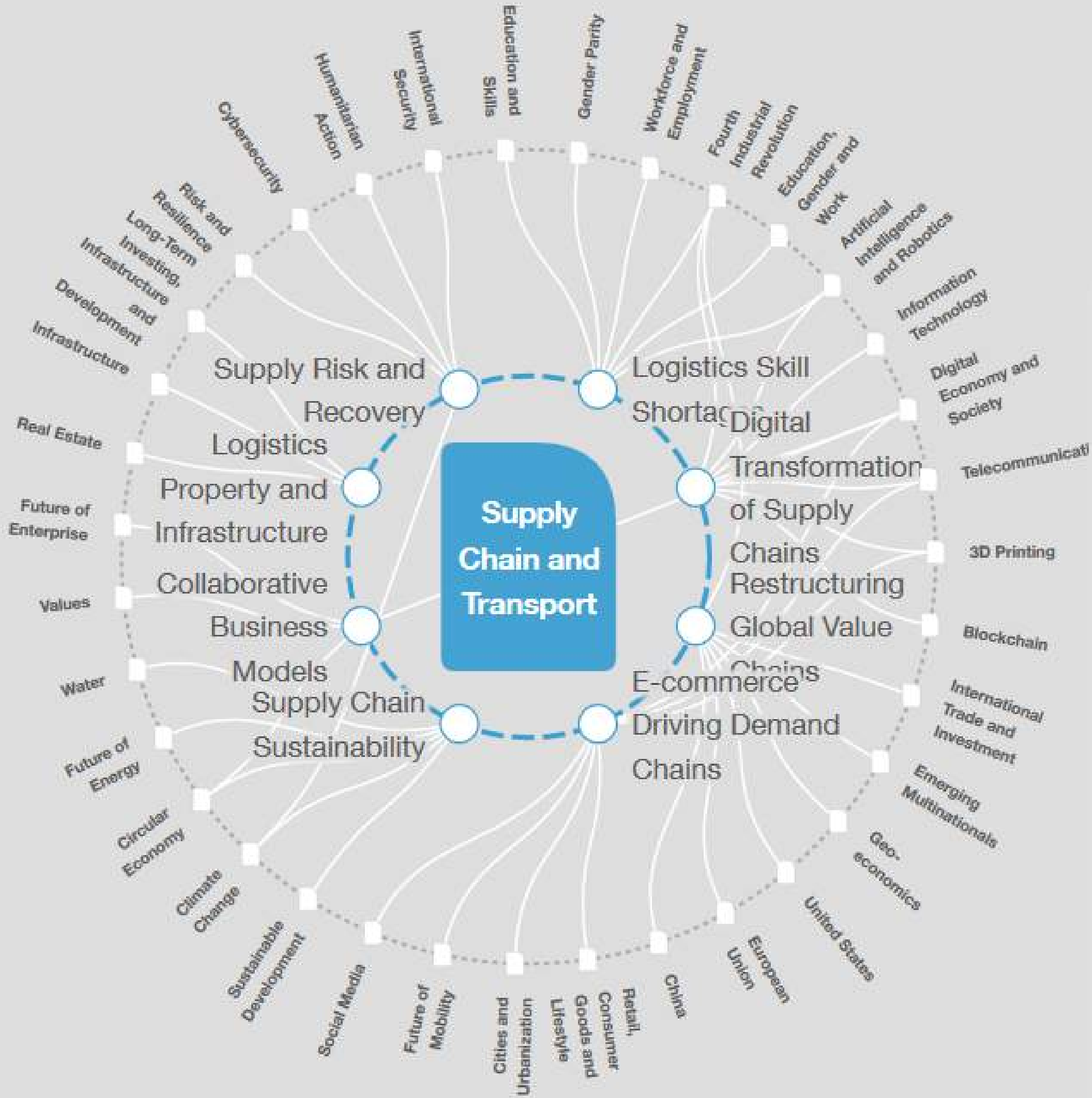
vative solutions for a safer, better world

Cyber Attacks on Transportation



Washington, DC

After Ganin et al., 2018 (under review)



From World Economic Forum

ns for a safer, better world

Environmental Science & Technology

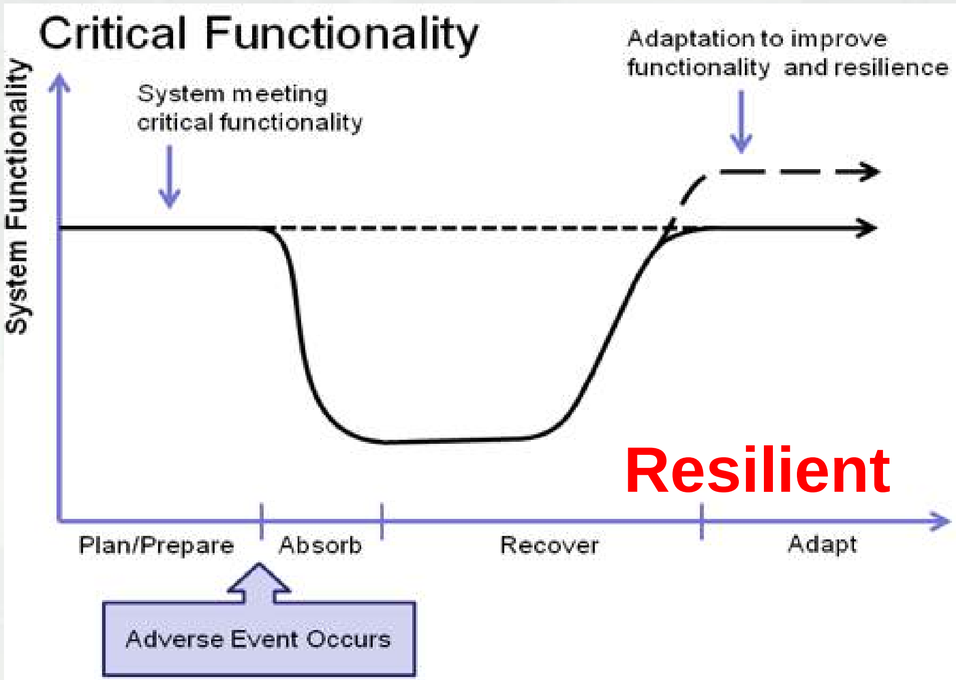
Viewpoint

pubs.acs.org/est

Can You Be Smart and Resilient at the Same Time?

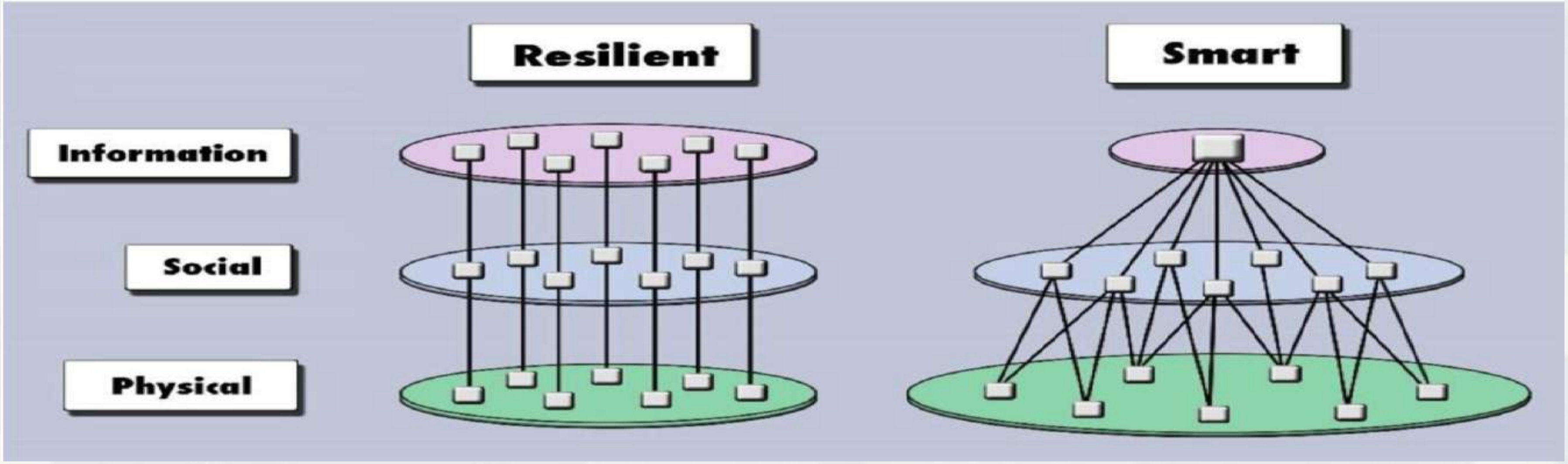
Dayton Marchese and Igor Linkov*

DOI: 10.1021/acs.est.7b01912
Environ. Sci. Technol. 2017, 51, 5867−5868



Smart

Resilient System and Smart Systems



- Fully Redundant
- Greater maintenance requirements
- Functional during disruption
- **Less efficient during random attacks**

- Observe emergent patterns
- Centralized decision making
- No redundancy
- **Prone to targeted attacks**

Resilience Needs to be Quantified

Risk-Resilience Integration

Top-Down
Decision Analysis/Social Science

Goal Identification and Problem Framing
-
What are the goals, alternatives, and constraints?

Decision Model
-
What are the criteria and metrics, How do we measure decision-maker values

Metrics Generation and Alternative Scoring
-
How does each alternative score along our identified criteria and metrics?

Management

Modeling

Data Collection

Bottom-Up
Risk Assessment/ Physical Sci

Risk Characterization
-
What are the risks relative to a threshold? How do they compare to other alternatives?

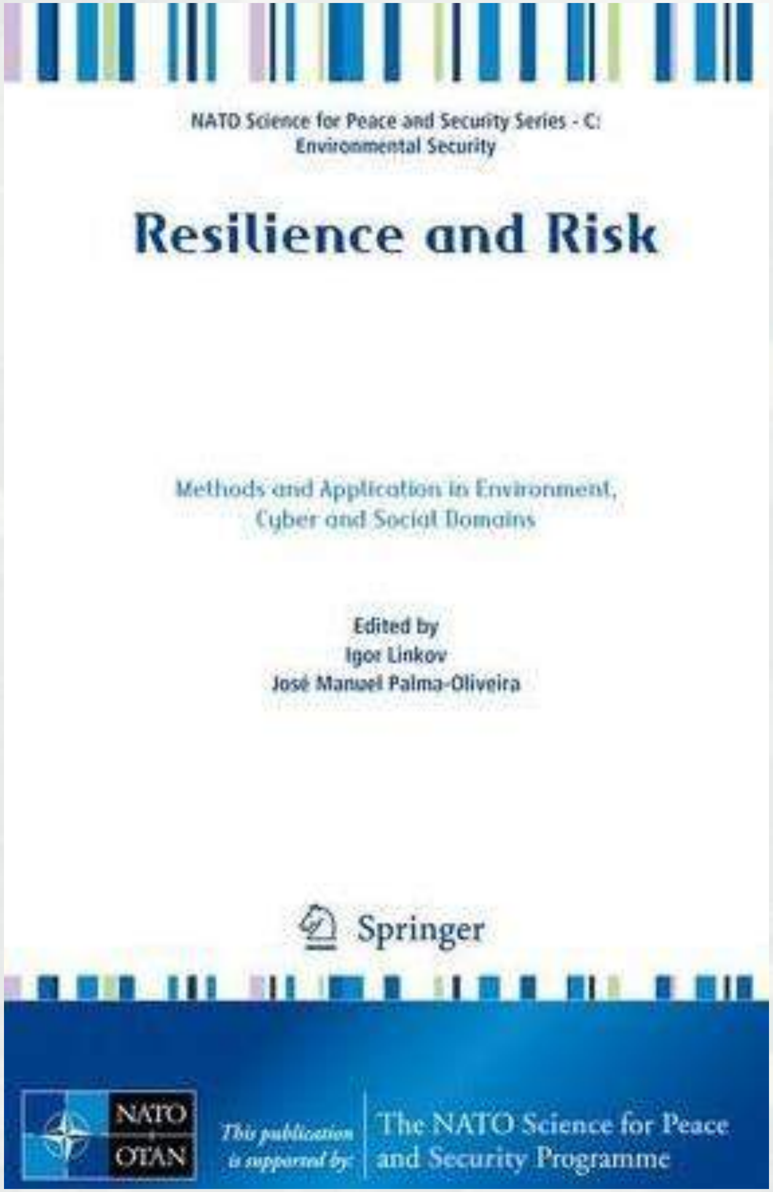
Physical/Statistical Model
-
What is the hazard?
What is exposure?

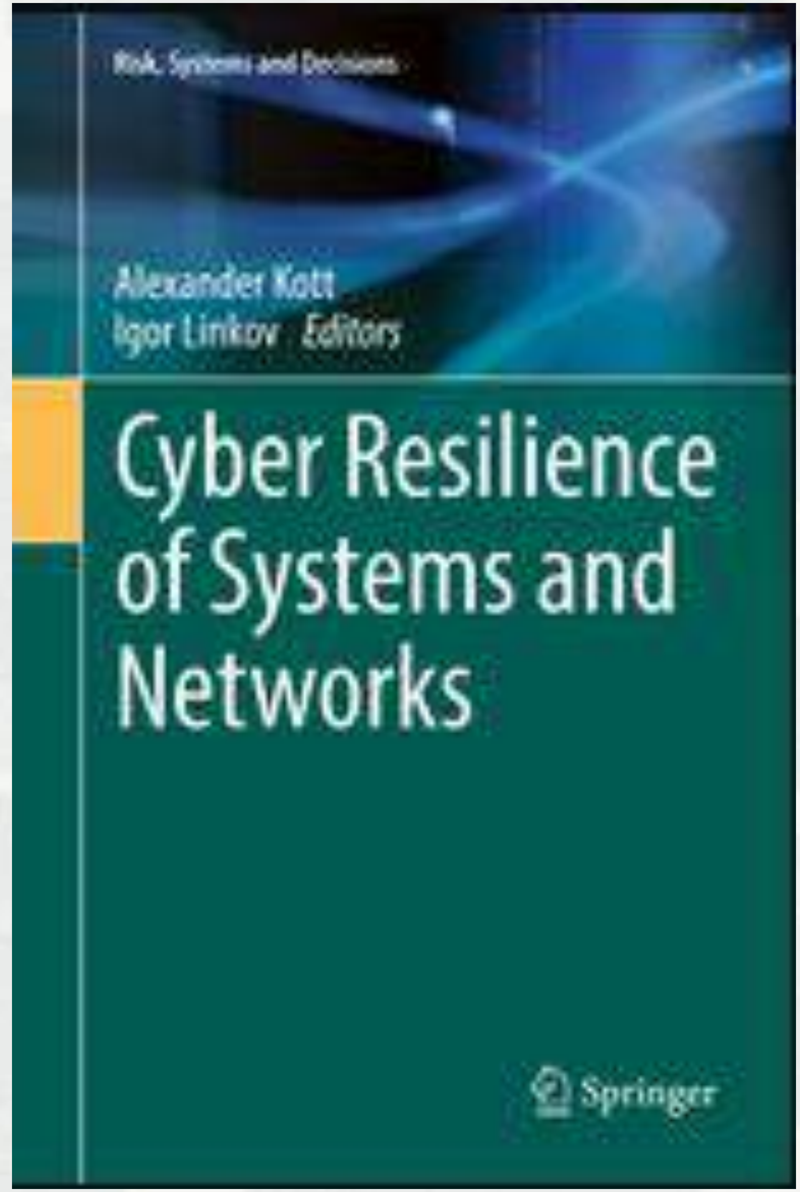
Data Collection
-
What are fundamental properties/mechanisms associated with each alternative?

Linkov et al., 2014

References

1) Kott, A., Linkov, I. eds (2018). **Cyber Resilience in Systems and Networks.** Springer, Amsterdam.
2) Linkov, I., Palma-Oliveira, J.M., eds (2017). **Risk and Resilience.** Springer, Amsterdam.
3) Florin, M.V., Linkov, I., eds. (2017). **International Risk Governance Council (IRGC) Resource Guide on Resilience.** International Risk Governance Center, Switzerland
4) Bostick, T.P., Lambert, J.H., Linkov, I. (2018, on-line). **Resilience Science, Policy and Investment for Civil Infrastructure.** Reliability Engineering & System Safety.
5) Massaro, E., Ganin, A., Linkov, I., Vespignani, A. (2018). **Resilience management of networks during large-scale epidemic outbreaks.** Science Reports **8:**1859.
6) Ganin, A., Kitsak, M., Keisler, J., Seager, T., Linkov, I., (2017). **Resilience and efficiency in transportation networks.** Science Advances **3**:e1701079.
7) Marchese, D., Reynolds, E., Bates, M.E., Clark, S.S., Linkov, I. (2018). **Resilience and sustainability: similarities and differences.** Sci Total Environ. 613-614:1275-83.
8) Marchese, D., & Linkov, I. (2017). **Can You Be Smart and Resilient at the Same Time?** *Environ. Sci. Technol.* 2017, 51, 5867−5868
9) Connelly, E. B., Allen, C. R., Hatfield, K., Palma-Oliveira, J. M., Woods, D. D., & Linkov, I. (2017). **Features of resilience.** *Environ Systems and Decisions*, *37*(1), 46-50.
10) Allen, C.R., Bartlett-Hunt, S., Bevans, R.A., Linkov, I. (2016). **Avoiding decline: fostering resilience and sustainability in midsize cities.** Sustainability 8:844
11) DiMase D, Collier ZA, Linkov I (2016, on-line) **Traceability and Risk Analysis Strategies for Addressing Counterfeit Electronics in Supply Chains.** Risk Analysis.
12) Thorisson, H., Lambert, J.H., Cardenas, J.J., Linkov, I., (2017). **Resilience Analytics with Application to Power Grid of a Developing Region.** Risk Analysis 37:1268
13) Gisladottir, V., Ganin, A., Keisler, J.M., Kepner, J., Linkov, I., (2017). **Resilience of Cyber Systems with Over- and Under-regulation** Risk Analysis 37:1644
14) Bakkensen, L., Fox-Lent, C., Read, L., and Linkov, I. (2016). **Validating Resilience and Vulnerability Indices in the Context of Natural Disasters.** Risk Analysis 37:982
15) Linkov, I., Larkin, S., Lambert, J.H. (2015). **Concepts and approaches to resilience in governance.** Environment, Systems, and Decisions 35:219-228.
16) Ganin, A., Massaro, E., Keisler, J., Kott, A., Linkov, I. (2016). **Resilient Complex Systems and Networks.** Nature Scientific Reports 6,19540.
17) Fox-Lent, C., Bates, M. E., Linkov, I. (2015). **A Matrix Approach to Community Resilience Assessment.**. Environment, Systems, and Decisions 35(2):205-219.
18) Larkin, S., Fox-Lent C., Linkov, I. (2015). **Benchmarking Agency and Organizational Practices in Resilience Decision Making.** Environ., Syst., & Dec. 35(2):185-195.
19) DiMase D, Collier ZA, Linkov I (2015). **Systems Engineering Framework for Cyber Physical Security and Resilience.** Environment, Systems, and Decisions 35:291.
20) Sikula, N.R., Linkov, I., (2015). **Risk Management Isn't Enough: A Conceptual Model for Resilience.** Environ., Syst., & Dec. 35:219-228.
21) Linkov, I., Fox-Lent, C., Keisler, J., Della-Sala, S., Siweke, J. (2014). **Plagued by Problems: Resilience Lessons from Venice** .Environment, Systems, Decision 34:378
22) Collier, Z.A., Linkov, I., DiMase, D., Walters, S., Lambert, J.(2014). **Risk-Based Cybersecurity Standards: Policy Challenges and Opportunities.** *Computer* 47:70
23) Linkov, I, Kröger, W., Levermann, A., Renn, O. et al. (2014). **Changing the Resilience Paradigm**. *Nature Climate Change* 4:407
24) Roege, P., Collier, Z.A., Mancillas, J., McDonagh, J., Linkov, I. (2014). **Metrics for Energy Resilience.** *Energy Policy* Energy Policy 72:249
25) Eisenberg, D.A., Linkov, I., Park, J., Chang, D., Bates, M.E., Seager, T., (2014). **Resilience Metrics: Lessons from Military Doctrines.** *Solutions* 5:76
26) Linkov, I., Eisenberg, D. A., Plourde, K., Seager, T. P., Allen, J., Kott, A (2014). **Resilience Metrics for Cyber Systems.** *Environment, Systems and Decisions* 33:471
27) Park, J., Seager, T, Linkov, I., (2013). "**Integrating risk and resilience approaches to catastrophe management in engineering systems**," *Risk Analy.*, 33(3), pp. 356.


NATO Science for Peace and Security Series - C:
Environmental Security
Resilience and Risk
Methods and Application in Environment,
Cyber and Social Domains
Edited by
Igor Linkov
José Manuel Palma-Oliveira
Springer
NATO
OTAN
This publication
is supported by:
The NATO Science for Peace
and Security Programme


Risk, Systems and Decisions
Alexander Kott
Igor Linkov Editors
Cyber Resilience
of Systems and
Networks
Springer

Governance for Cyber Security and Resilience in the Arctic

NATO Workshop

Rovaniemi, Finland, 27-30 January 2019

NATO OTAN

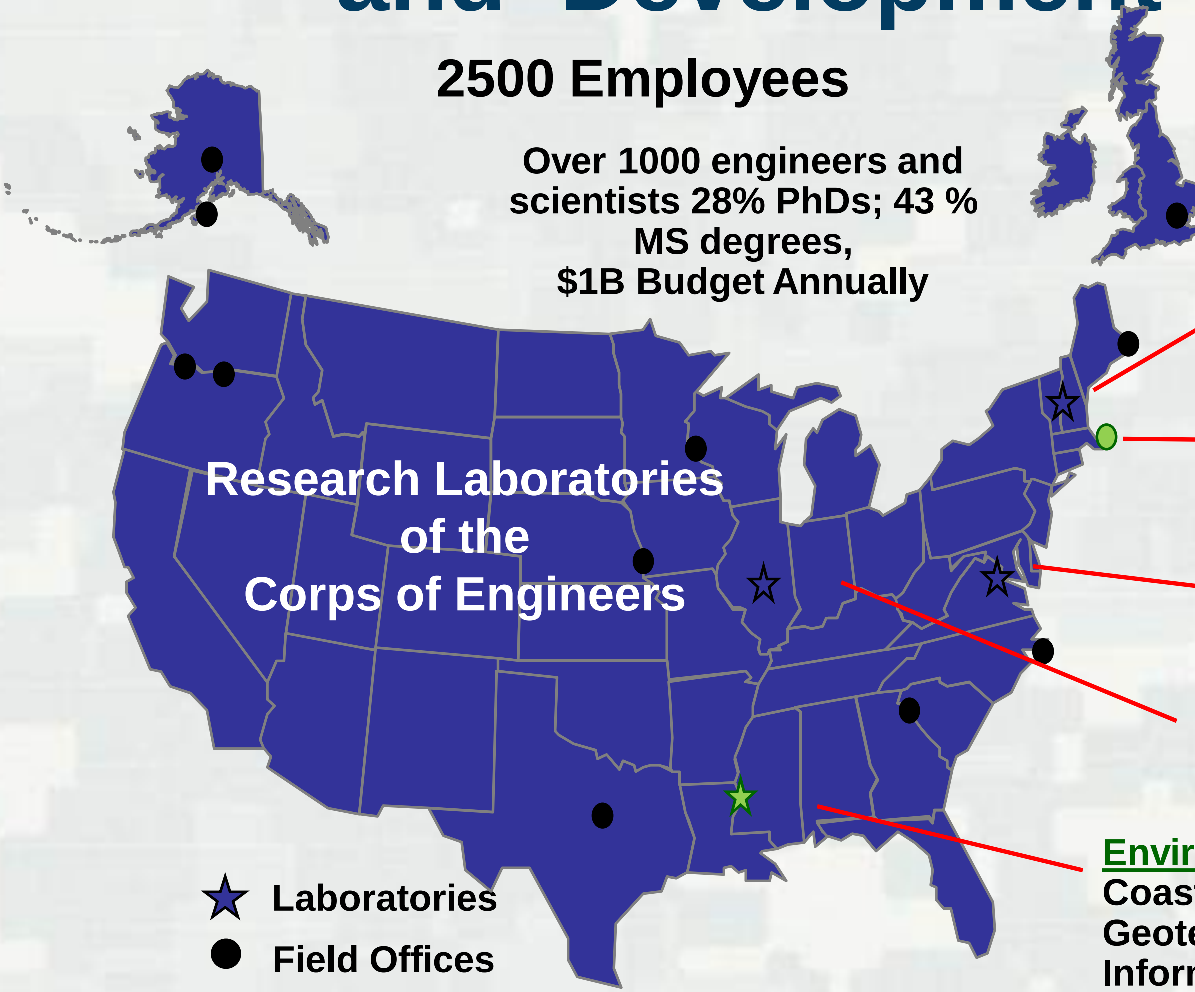
This workshop is supported by: The NATO Science for Peace and Security Programme

ADDITIONAL SLIDES

US Army Engineer Research and Development Center

2500 Employees

Over 1000 engineers and scientists 28% PhDs; 43 % MS degrees, $1B Budget Annually



Cold Regions Research Engineering Laboratory (Hanover, NH)

Risk and Decision Science Team Boston, MA)

Topographic Engineering Center (Alexandria, VA)

Construction Engineering Research Laboratory (Champaign, IL)

Environmental Laboratory
Coastal & Hydraulics Laboratory
Geotechnical & Structures Laboratory
Information Technology Laboratory
Headquarters (Vicksburg, MS)

ERDC

international risk governance center

Environ Syst Decis (2017) 37:46–50
DOI 10.1007/s10669-017-9634-9

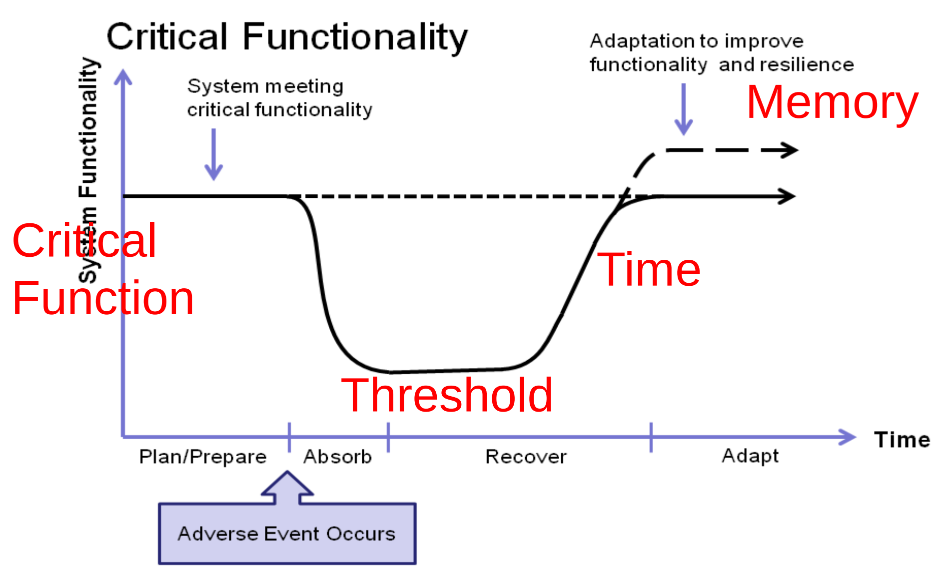
Features of resilience

Elizabeth B. Connelly[1] · Craig R. Allen[2] ·
David D. Woods[5] · Igor Linkov[6]

RESOURCE GUIDE

Resilience

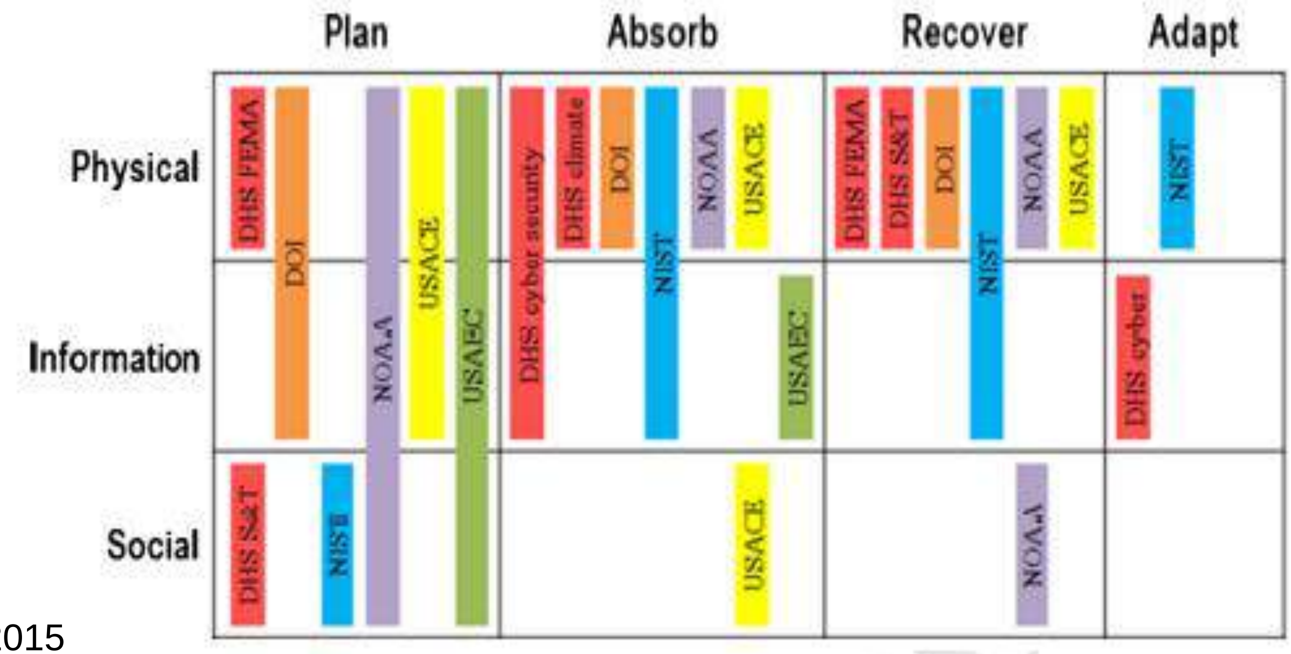
An edited collection of authored pieces comparing, contrasting, and integrating risk and resilience with an emphasis on ways to measure resilience



US Government Agencies

Environ Syst Decis

Fig. 1 Agency resilience actions addressed (relative to NAS definition) in physical, information, and social domains



Larkin, Fox-Lent, Linkov et al., 2015

US Army

READY RESILIENT

Achieving Personal Readiness. Optimizing Performance.

R2 OVERVIEW

MISSION

The Army provides Ready and Resilient (R2) capabilities to Commanders and Leaders to enable them to achieve and sustain personal readiness and optimize human performance in environments of uncertainty and persistent danger.

VISION

The Army of 2020 is comprised of adaptive leaders of character who develop cohesive teams of resilient individuals committed to the Army Profession and capable of accomplishing a range of missions in environments of uncertainty and persistent danger.

ased Organization of Trusted Army
als

ed Organization of Trusted Army
ls Promote a Culture of Trust and
ccountability

ofessionalism
ulture of Trust

Hotlines

Military Crisis Line (U.S.)
(800) 273-8255 or DSN 111 PRESS 1
Text: 838255
On-line Chat
Military Crisis Line (Europe)
00800-1273-8255 or DSN 118
Military Crisis Line (Korea)
0808-555-118 or DSN 118
Military Crisis Line (Afghanistan)
Use U.S. number
BeThere Peer Support Call and Outreach:
https://www.betherepeersupport.org
Safe Helpline - Sexual Assault Support for the DoD Community
877-995-5247
Text: 55-247 (inside the U.S.)
Text: 001-202-470-5546 (outside the U.S.)
Defense Centers of Excellence for Psychological Health and Traumatic Brain Injury (DCoE)
866-966-1020 - 24/7 Outreach
Military OneSource 24/7 Support
800-342-9647

R2 Leadership

Ms. Sharyn Saunders
Director
Army Resiliency Directorate

Sgt. Maj. John McNeirney
Sergeant Major
Army Resiliency Directorate

Tiered Approach to Resilience Assessment

Resilience Tiered Approach

Increase resources, capital expenditures ↑

Tier 3
Complex modeling of interactions between sub-systems and using robust scenario analysis.

Tier 2
Detailed models using formal decision analysis to prioritize system performance and investments

Tier 1
Screening models or indexes to identify easy improvements and guide focus of further analysis

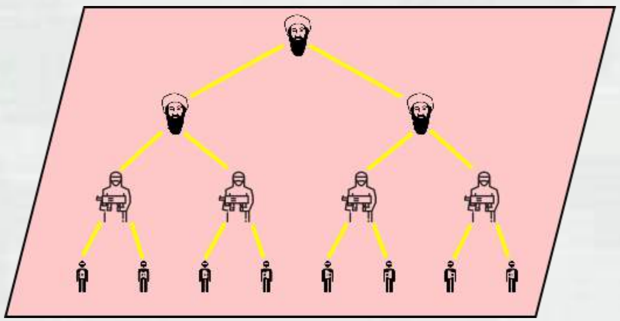
Decrease model complexity, data needs ↓

After Linkov et al., 2017

Command and Control Networks

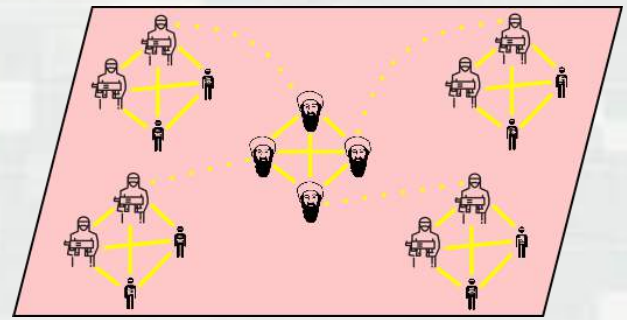
- Paramilitary

Hierarchical structure with defined roles (e.g. Provisional Irish Republican Army).



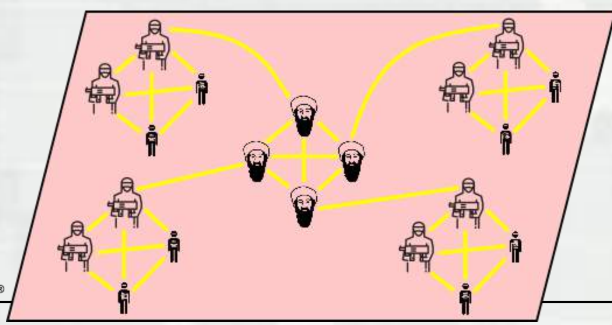
- Decentralized Cells

Leadership provides suggestion and guidance and may work within legal boundaries.



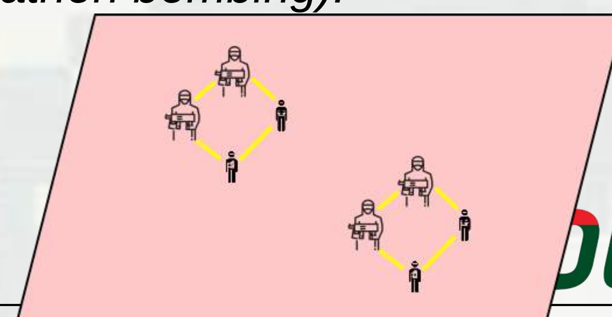
- Centralized Cells

C2 HQ cell linked to specialized support and operations cells.



- Ad-hoc Cells

Lowest density of interactions, formed for particular attacks (e.g. Boston Marathon bombing).



Macys A.J. (editor). Networks and Network Analysis for Defense and Security. Springer, 2014.

US Army Corps of Engineers:
Evolution of Approaches for Flood Risk Management

Live with floods
- Individuals and small communities adapt to nature's rhythm.

Use the floodplain
- Fertile land in floodplain is drained for food production.
- Permanent communities develop on the floodplain.

Control floods
- Large scale structural approaches are implemented through organized governance

Reduce flood damages
- A recognition that engineering alone has limitations.
- Effort to increase the resilience of communities should a flood occur.

Manage risk
- Not all problems are equal.
- Risk management is an effective and efficient means to maximize the benefit of limited investment.

Manage resilience?
- Not all problems need to be solved
- Systems approach & integration of communities is the key





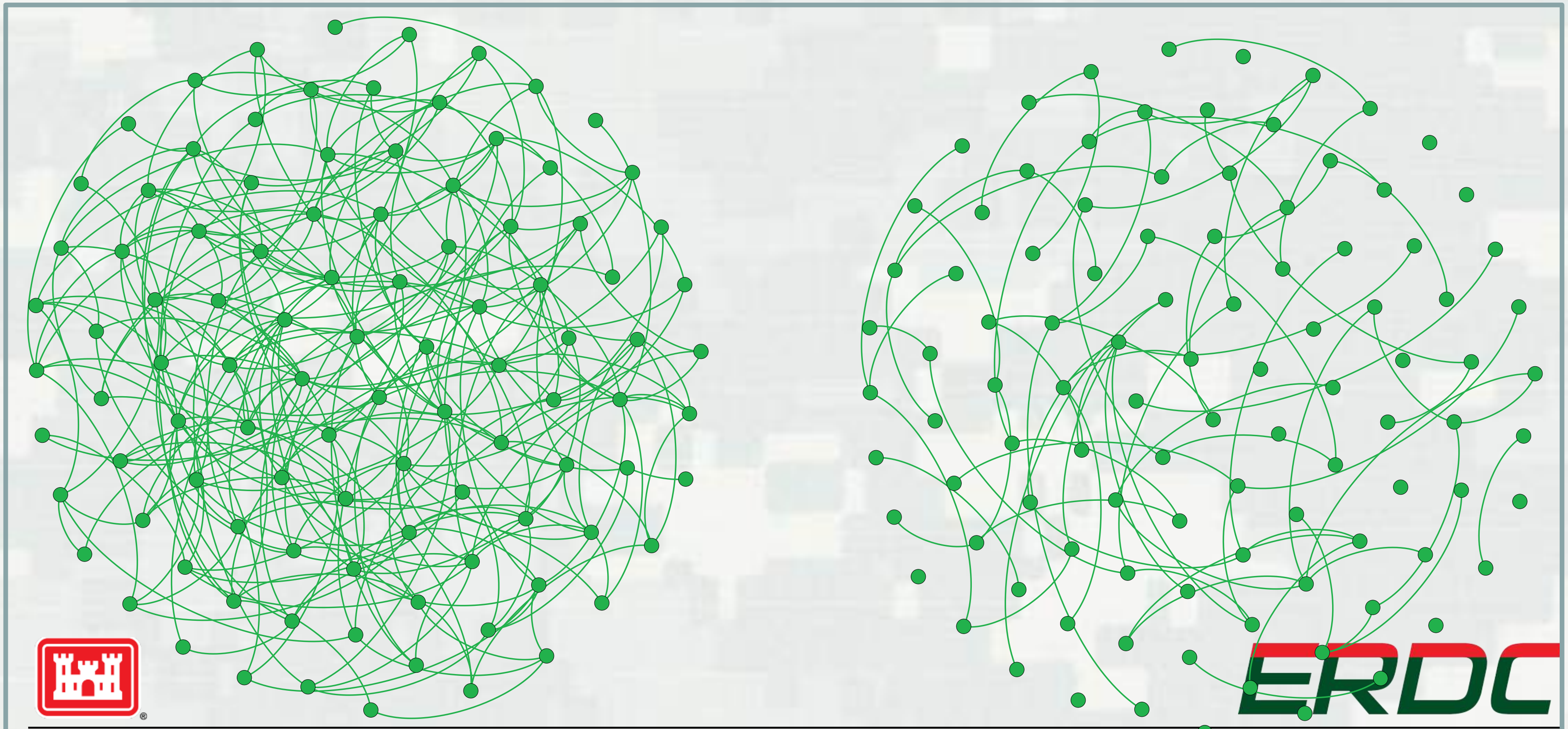
From Sayers et al , 2012

Network Disruption Model

How to allocate links between nodes to improve the system's response to links disruption and ensure the optimal connectedness of nodes.

Example: Random network with 100 nodes and 257 links

Normal state | Random disruption of 70% of the links

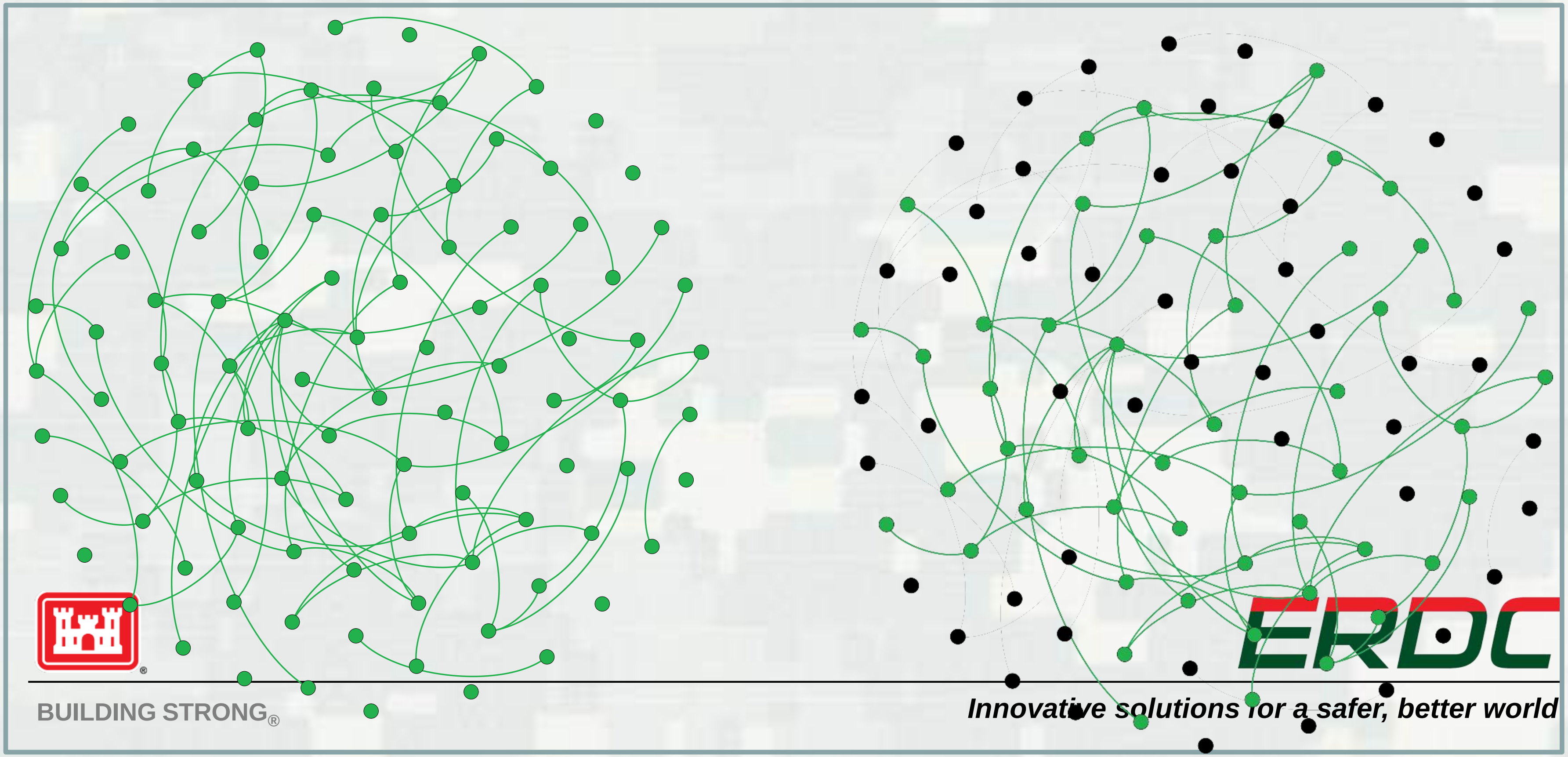


Disruption and Connectedness

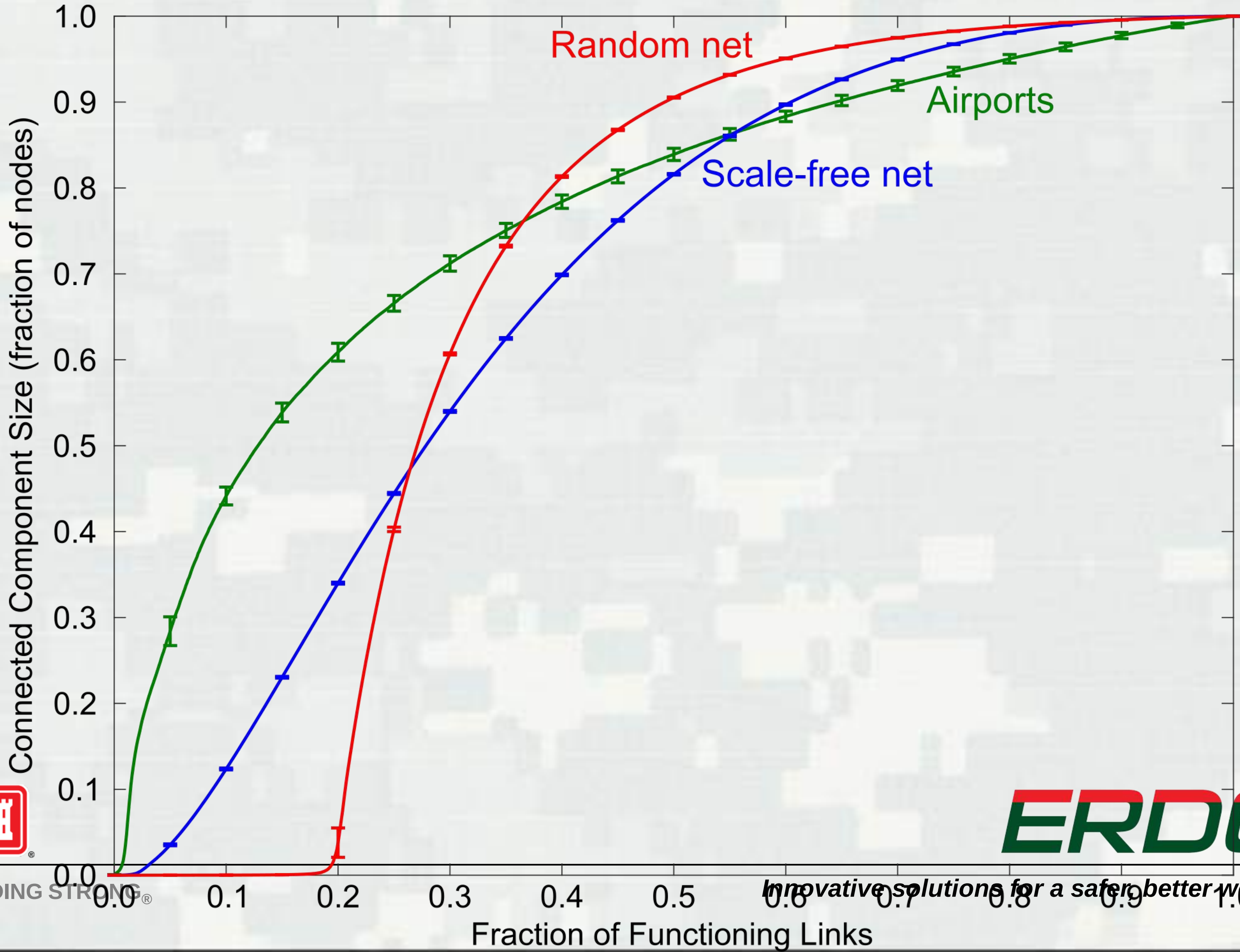
Disruption of links (left panel) results in a formation of a new giant connected component (right panel)

Disruption of 70% of the links

Giant connected component after the disruption (green nodes)



Classical Results on the Connected Component Size

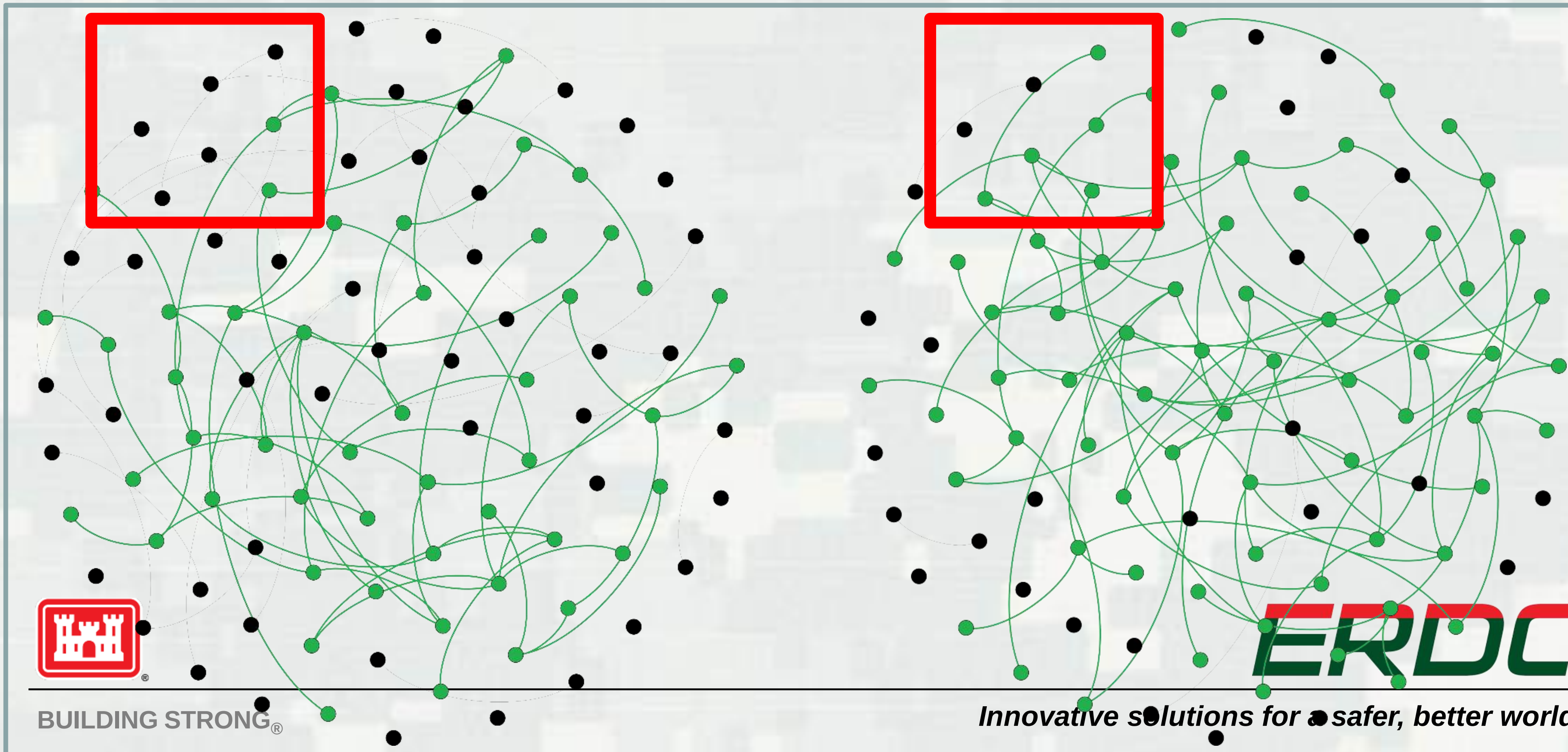


Is the Connected Component Stable?

As the links disruption is random, in another realization of link disruption different links will be taken out. This stochasticity means that the GCC will be different, even though the size of disruption (70% of links) stays the same.

Giant connected component after the disruption (1st example)

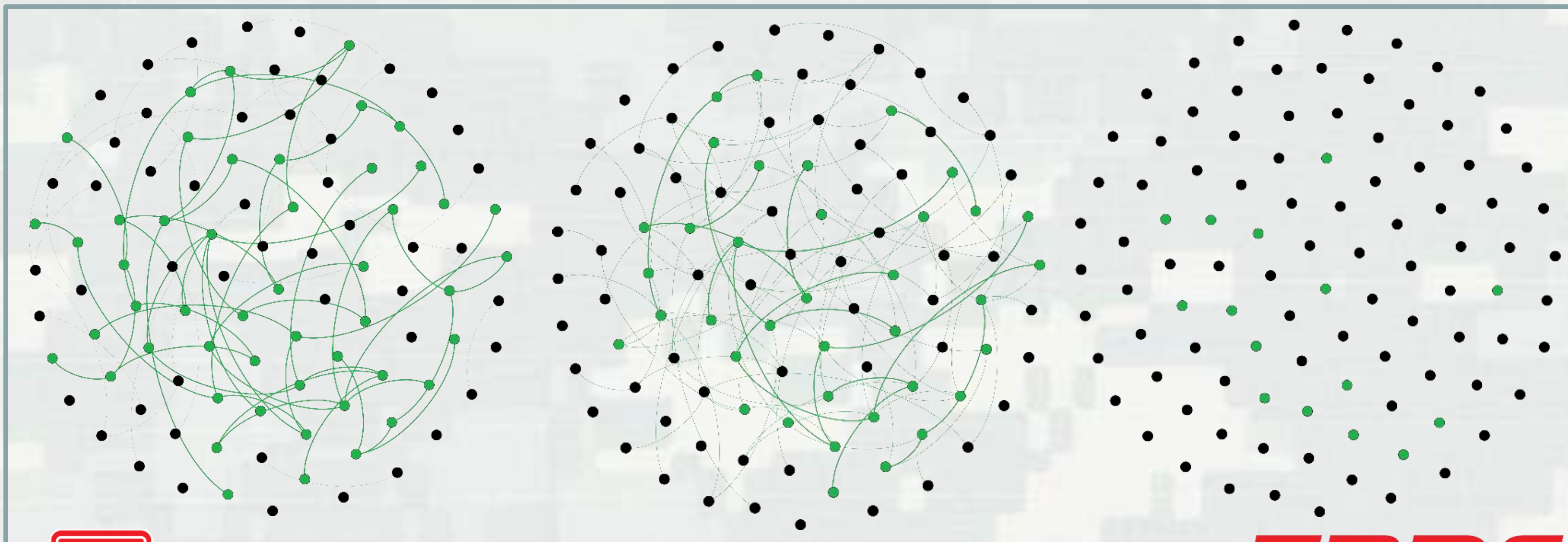
Giant connected component after the disruption (2nd example)



Research Question: Stability of the Connected Component

We are looking at the nodes, which stay connected in multiple disruptions, and define these nodes as persistently connected. Below we show the persistently connected nodes for 1, 2, and 5 disruptions of 70% of links.

1 disruption | 2 disruptions | 5 disruptions (links are not shown)



50 nodes out of 100 are in GCC (green) | 37 nodes out of 100 are in GCC (green) | 15 nodes out of 100 are in GCC (green)