Resilience and Efficiency Tradeoffs in Interconnected Systems

This presentation does not necessarily reflect the views of the United States Government, and is only the view of the author

Andrew Jin

Department of Defense SMART Fellow,

US Army Engineer R&D Center;

Dr. Igor Linkov

Senior Science and Technology Manager (SSTM),

US Army Engineer R&D Center;

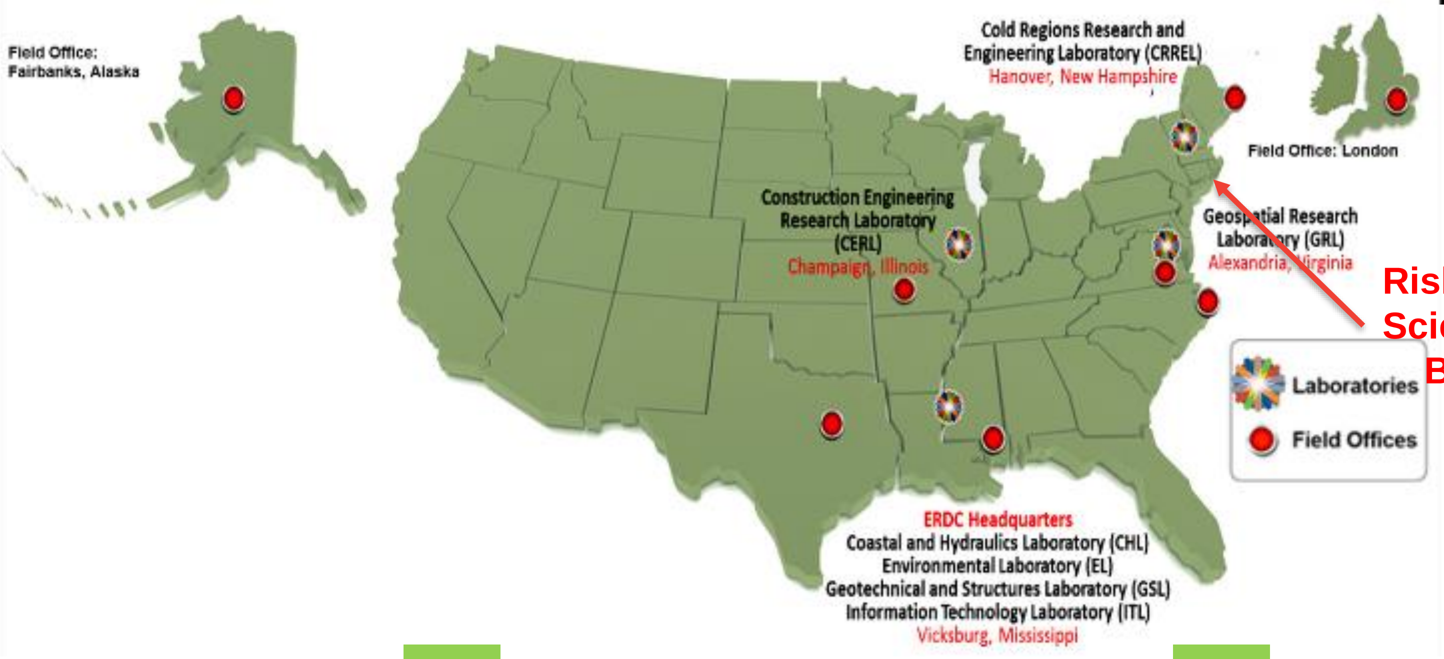
Adjunct Professor, Carnegie Mellon University

Igor.Linkov@usace.army.mil

17 May 2022

US Army Corps of Engineers®

About Army Engineer R&D Center



7 Laboratories

Coastal and Hydraulics Laboratory (CHL)
Cold Regions Research and Engineering Laboratory (CRREL)
Construction Engineering Research Laboratory (CERL)
Environmental Laboratory (EL)
Geospatial Research Laboratory (GRL
Geotechnical and Structures Laboratory (GSL)
Information Technology Laboratory (ITL)

Annual Research Program Exceeding
$1.3 Billion

People

2100 Strong
61% E&S
71% of E&S with Advanced Degrees
29% of E&S with PhD

Core Competencies

- Blast and Weapons Effects on Structures and Geo-Materials
- 3-D Mapping and Characterization
- Cold Regions Science and Engineering
- Civil and Military Engineering
- Computational Prototyping of Military Platforms
- Coastal, River, and Environmental Engineering
- Military Installations and Infrastructure

Partners

All DoD Services
Army, Navy, Air Force, NASA, DHS, FEMA, DIA, NGA
Academia
68 EPAs with top engineering schools
Industry
172 CRADAs
International
14 international agreements with 7 countries

US Army Corps of Engineers

U.S. ARMY

Engineered systems are becoming increasingly interconnected

US Army Corps of Engineers

U.S. ARMY

This increased interconnectivity can create major challenges to system operations

c&en CHEMICAL & ENGINEERING NEWS

TOPICS MAGAZINE COLLECTIONS VIDEOS JOBS

WATER

How a water treatment plant hack could have affected a Florida town's water

Hackers tried to increase the NaOH levels in a town's municipal drinking water. C&EN unpacks the chemistry implications

by *Leigh Krietsch Boerner*

February 12, 2021

US Army Corps of Engineers

U.S. ARMY

A number of terms are often conflated when discussing how to protect critical infrastructure systems.

Definitions by Oxford Dictionary

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

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

Reliability -- “the quality of performing consistently well.”

Resilience -- “the capacity to recover quickly from difficulties.”

US Army Corps of Engineers

U.S. ARMY

Calls for 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, th our national and economic security. America's critical infrastructure is complex and diverse, combini both cyberspace and the physical world -- from power plants, bridges, and interstates to Federal bui massive electrical grids that power our Nation. During Critical Infrastructure Security and Resilience resolve to remain vigilant against foreign and domestic threats, and work together to further secure systems, and networks.

(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**.

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

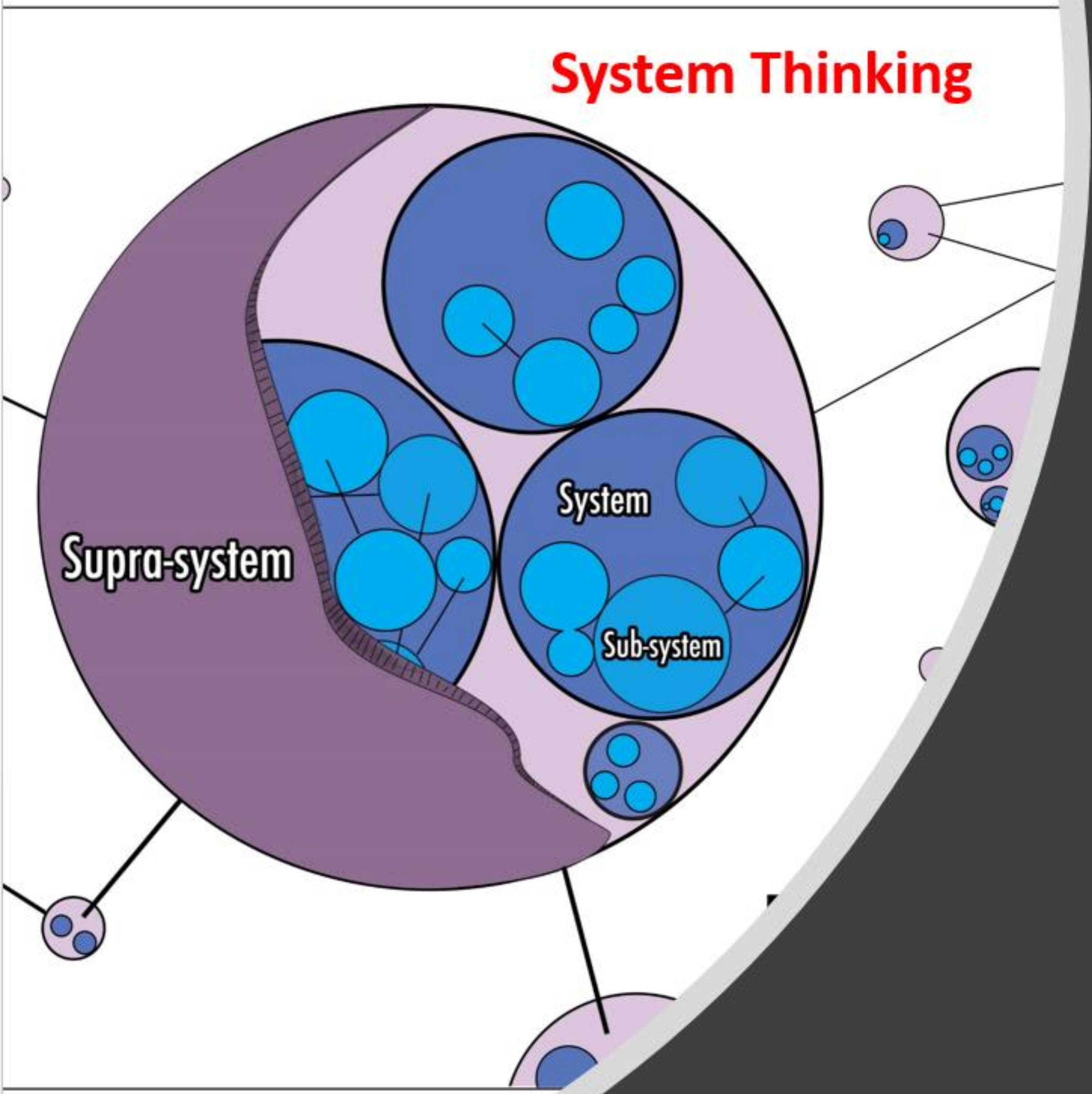
The White House

Office of the Press Secretary

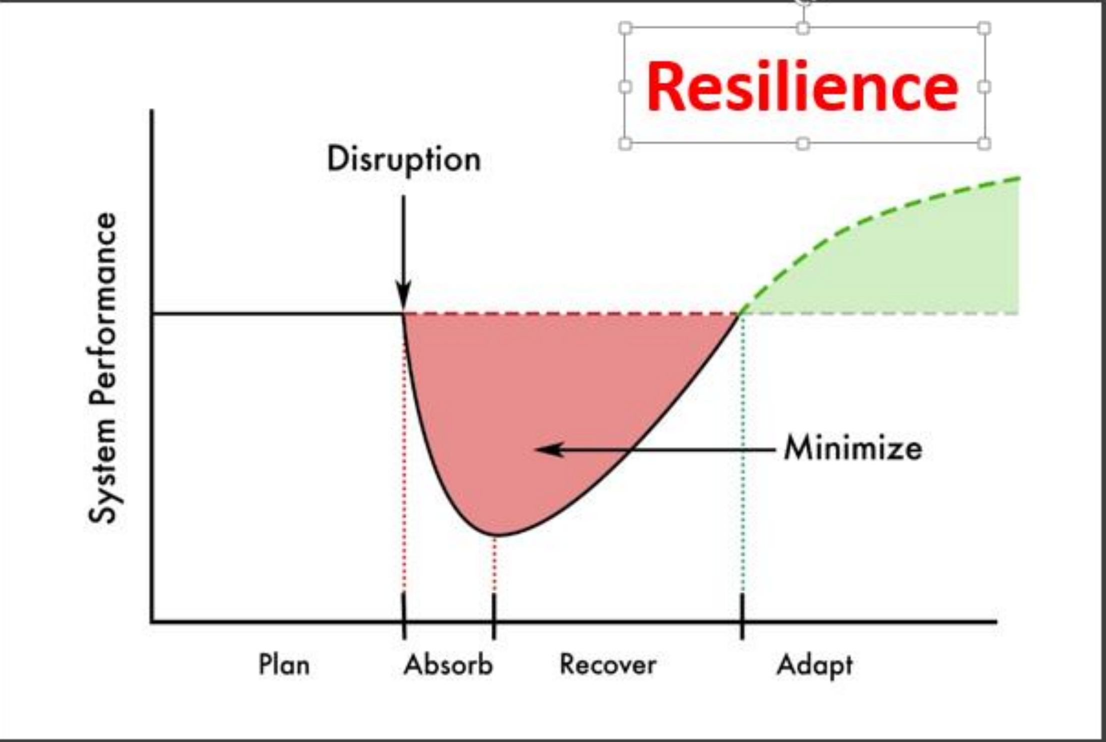
For Immediate Release May 11, 2017

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

EXECUTIVE ORDER



What Makes Complex Systems (Communities) Susceptible to Threat?



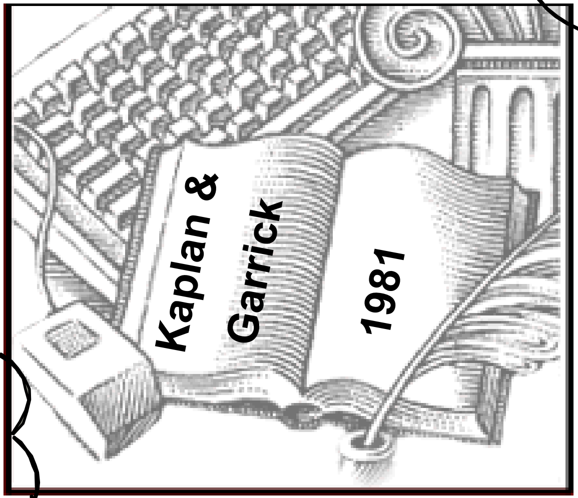
After Linkov and Trump, 2019

Science of Risk

Risk =Threat x Vulnerability x Consequence

What can happen (go wrong)?

How likely is it?



What are the consequences?

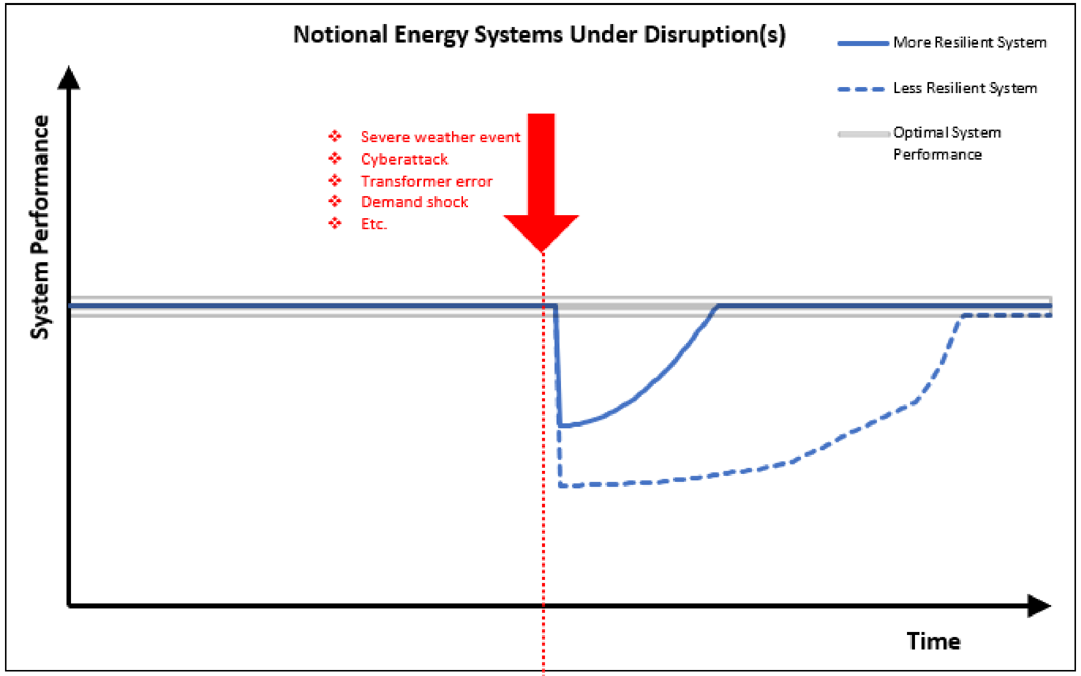
US Army Corps of Engineers

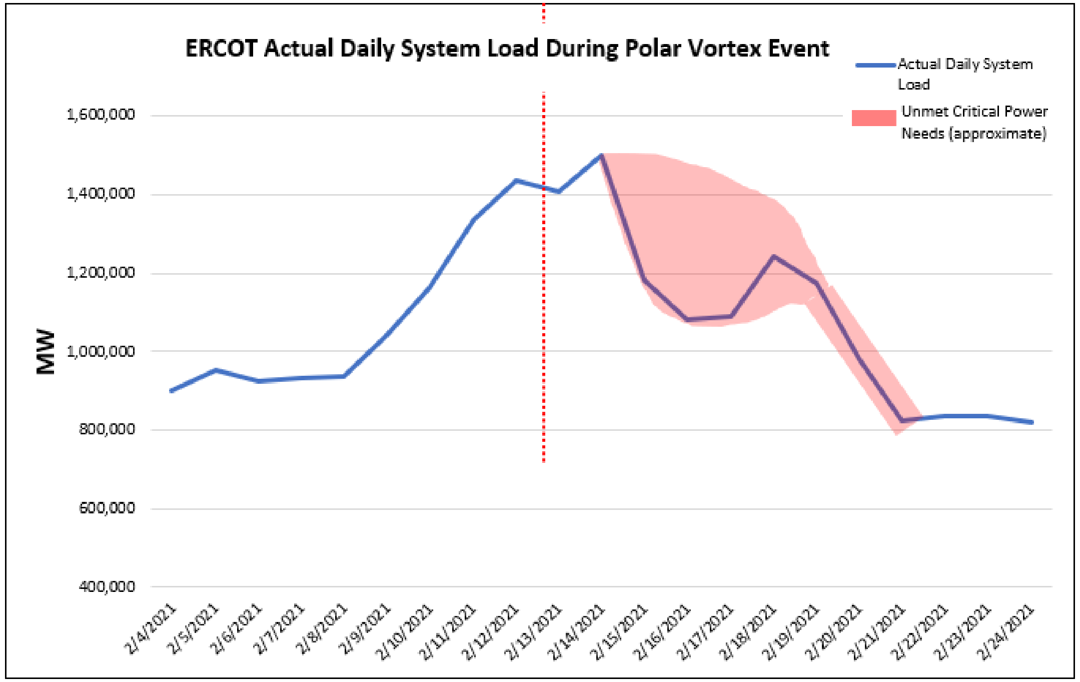
U.S.ARMY

CASCADING IMPACTS OF COMPLEX INTERCONNECTED SYSTEMS REQUIRE RESILIENCE-THINKING

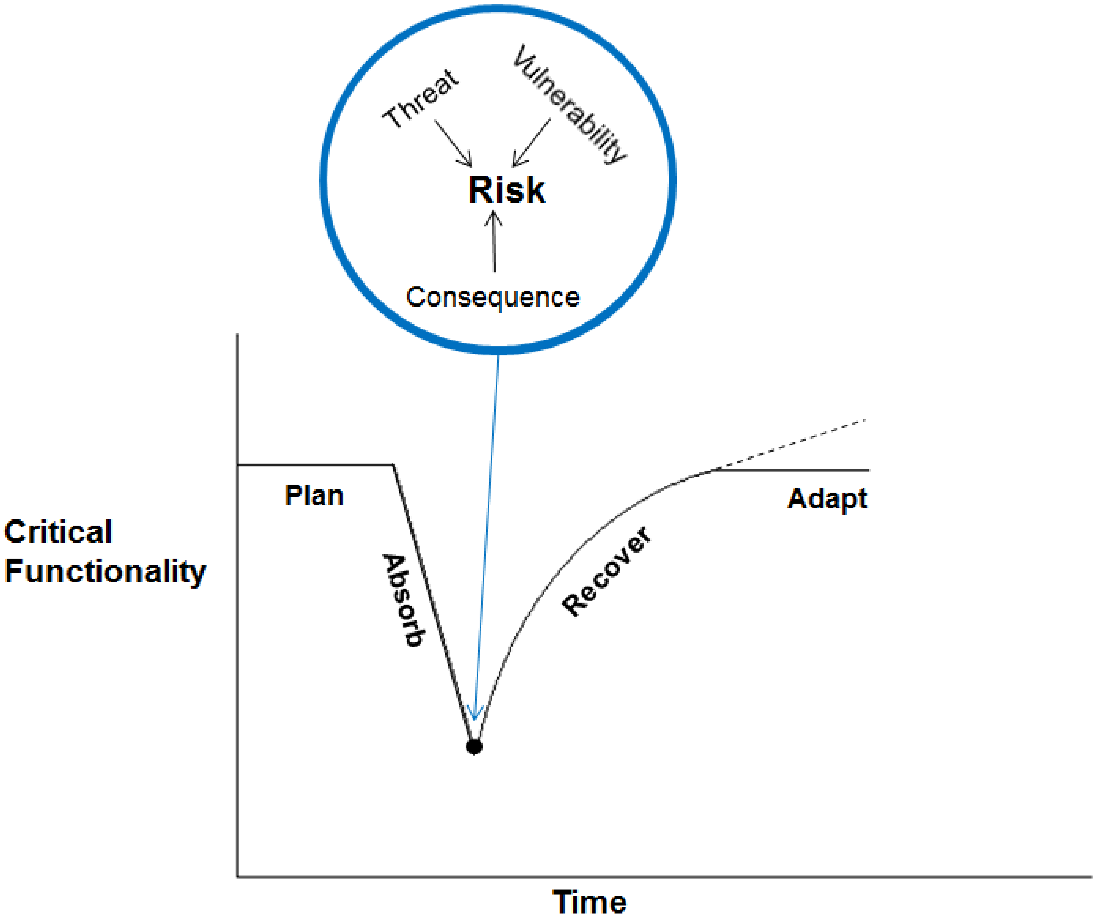
Example of Texas Polar Vortex:

- Electric demand shock
- Decreased capacity from lack of winterization and supply of natural gas
- ERCOT forced to operate under emergency conditions until Feb. 19th, at which point 34,000 MW remained on forced outage
- How should proactive resilience corrective actions and network design be implemented?
  - How should the cyber-physical energy system be accounted for in resilience implementation?





System Risk/Security and Resilience



Risk Analysis

System Resilience

After Linkov et al, Nature Climate Change 2014

US Army Corps of Engineers

U.S. ARMY

Cascading impacts of failures in other sectors, like energy, can cause other sectors to fail as well.

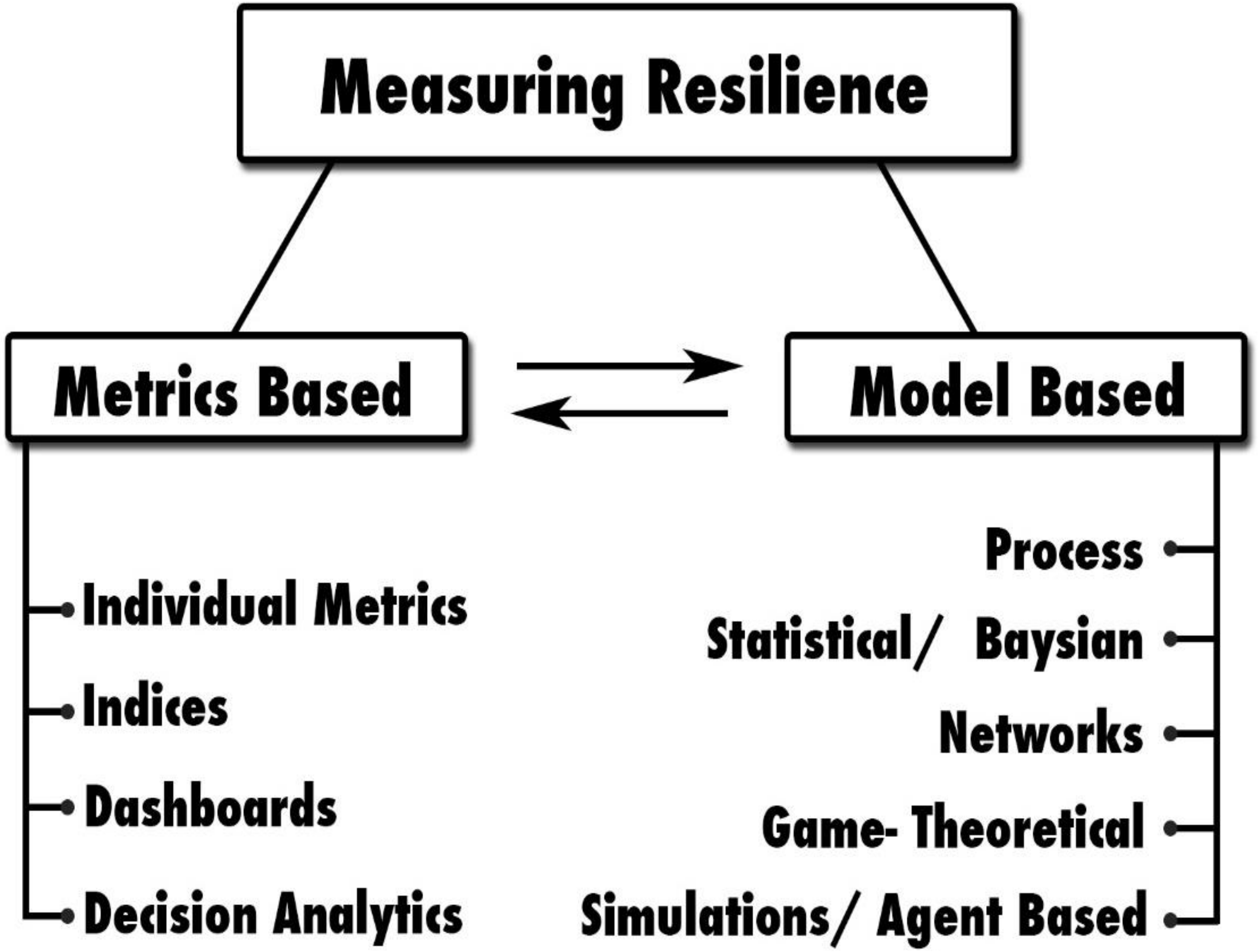
Millions of gallons have leaked from burst water pipes in just one Texas city: 'That is an incredible amount of water'

Ryan W. Miller
USA TODAY

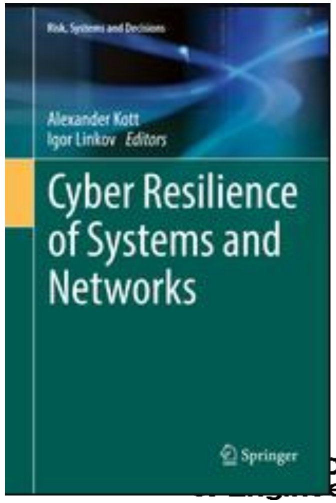
US Army Corps of Engineers

U.S.ARMY

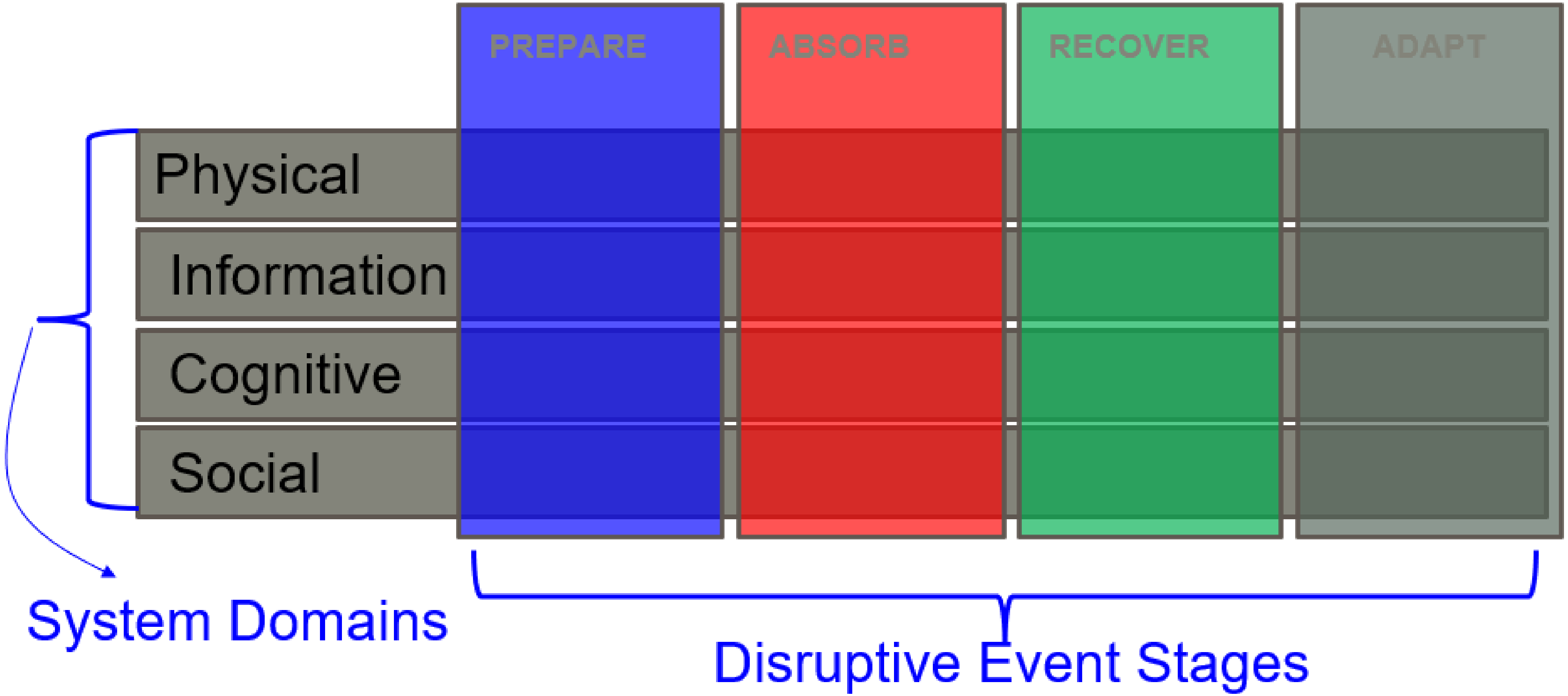
How to Quantify Resilience?



After
2019



Resilience Matrix



US Army Corps of Engineers
U.S.ARMY

Our group has applied this matrix to smart water systems in the pasts.

ASCE

Journal of Water Resources Planning and Management / Volume 146 Issue 1 - January 2020

Forum

Resilience for Smart Water Systems

Dayton Marchese, P.E., A.M.ASCE; Andrew Jin; Cate Fox-Lent; and Igor Linkov, Ph.D.

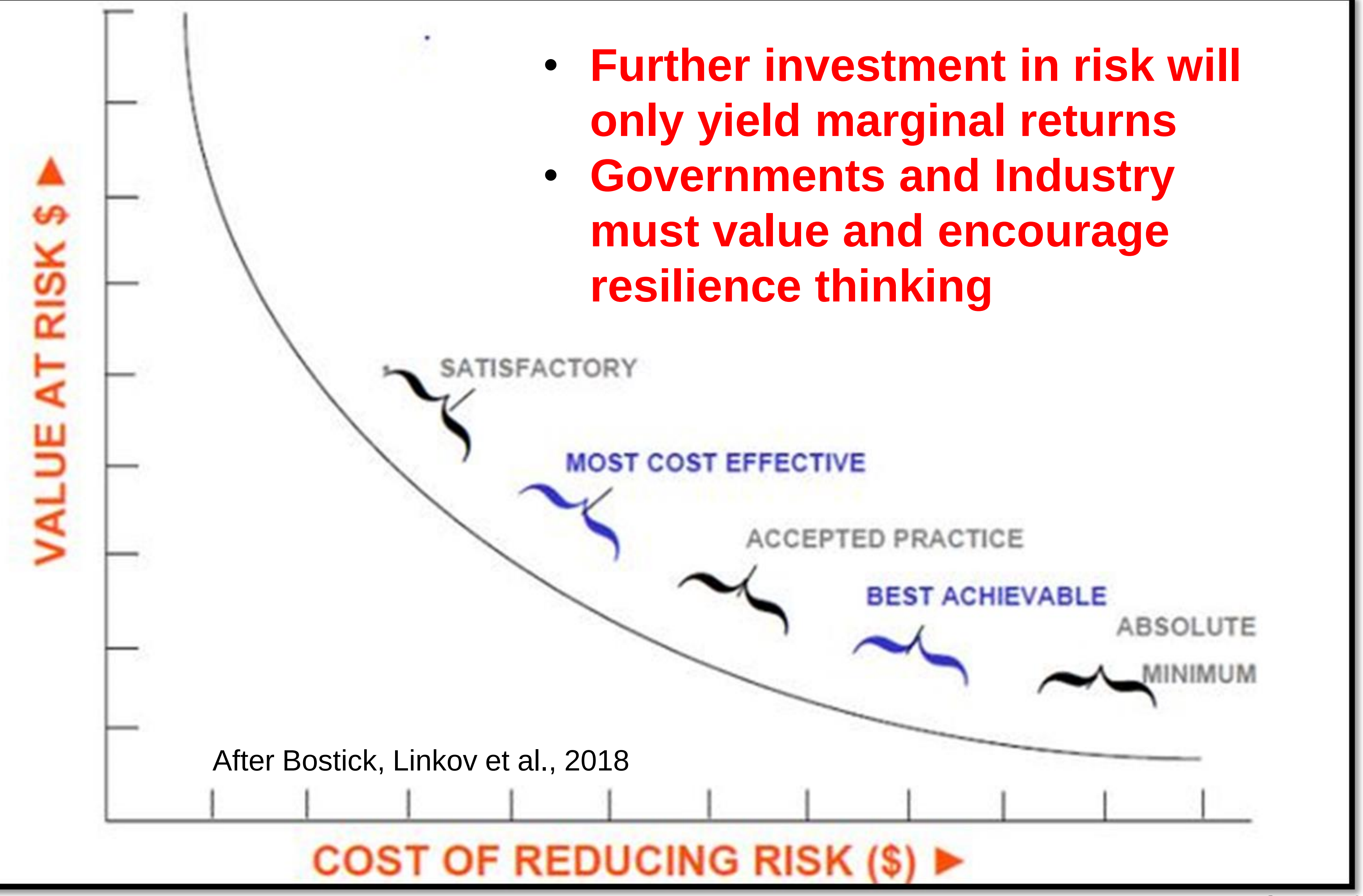
Table 1. Baseline resilience matrix for water systems

Domain	Prepare	Absorb	Recover	Adapt
Physical	Reduce water demand	Utilize neighboring utilities for water resources	Implement flexible, temporary systems	Replace obsolete and damaged assets
	Build redundant piping structures[a]	Manually trigger safeguards to isolate and contain damage to specific components	Stockpile machinery, communications, and power systems	
	Perform preventative maintenance[b]			
Information	Evaluate resources with risk framework in American Water Works Association (AWWA) standards[c]	Restrict dissemination of critical facility information[d]	Make historical information regarding customer needs and status available to emergency crews	Evaluate incident point of entry, event process, vulnerabilities, and impacts
	Utilize information sharing frameworks (e.g., WaterISAC[c])			
	Implement cross-sector vulnerability assessment[b]			
	Determine water requirements using normal-state system capabilities and population information			
Cognitive	Identify gaps between projected needs and available resources	Adhere to the incident command system (ICS) model for clear lines of control and accountability[a]	Prioritize restoration of critical support services with cross-sector decision makers[3]	Utilize a compendium of lessons learned, best practices, expert knowledge, and tools in after-action analyses[d]
	Develop emergency response plans using tools, such as EPA Road to Resilience Toolkit[d]			
	Simulate catastrophic events across large geographic regions[d]			Assess performance after low probability, high impact events (e.g., Hurricane Sandy)
Social	Develop connections with other local utility personnel, information, and resources[b]	Ensure relevant personnel and resources are available, requesting support if needed[a]	Implement protocols for internal, external, and public/media communication of recovery procedures	Distribute after-action reports with lessons learned and input from various stakeholders and authorities to consumers
	Implement education campaigns for citizens on the community water demand relative to system capacity and environmental or economic thresholds	Enforce individual resilience efforts during disturbances[a]		Incentivize community members to implement more resilient systems

US Army Corps of Engineers

U.S. ARMY

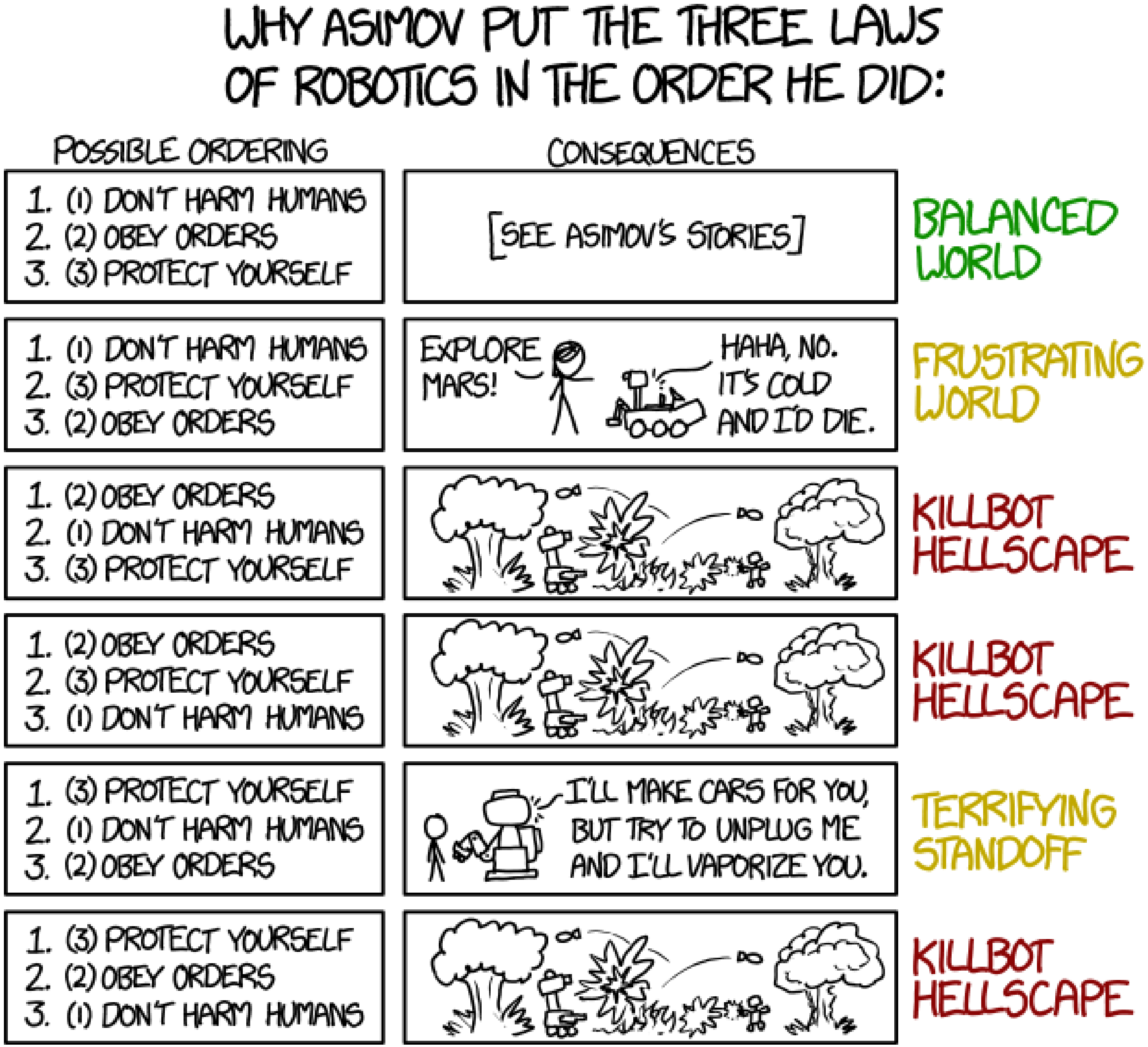
Cost of Buying Down Risk and Resilience



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

After Bostick, Linkov et al., 2018

US Army Corps of Engineers



Order of Execution Reflect Values and Mission and Ultimately Affects End Results

US Army Corps of Engineers

U.S. ARMY

Assessment using Stakeholder Values

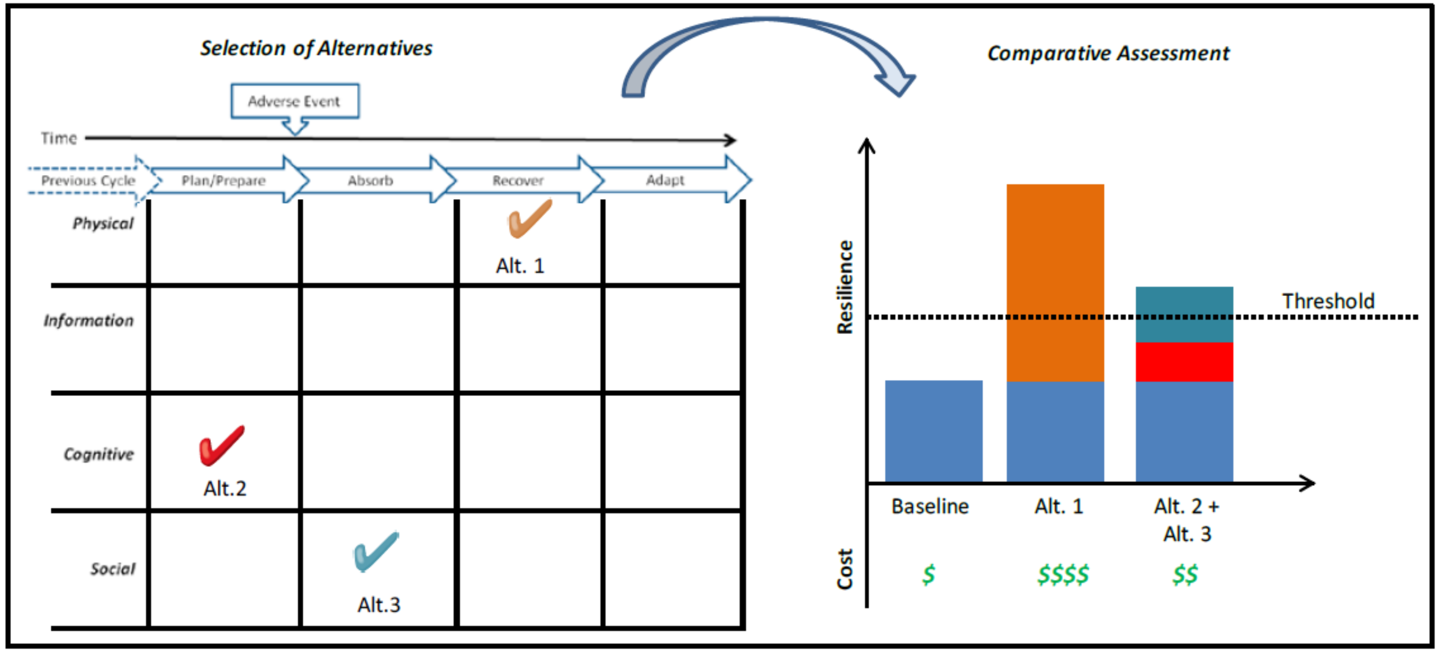


Figure 5: Comparative Assessment of Resilience-Enhancing Alternatives

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

After Fox-Lent et al., 2015

Efficiency and Resilience can be at odds with one another.

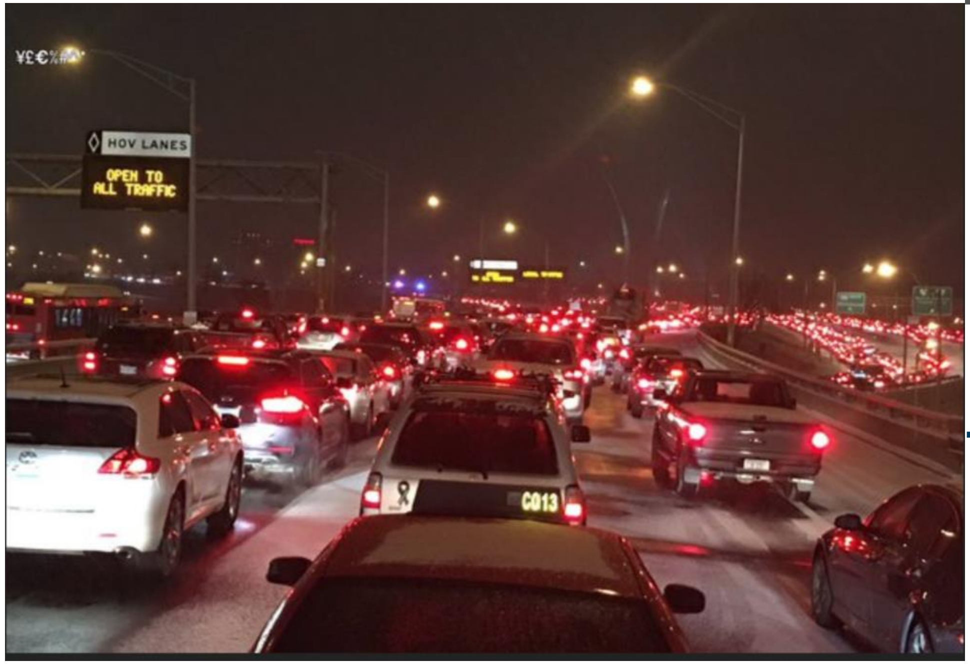
US Army Corps of Engineers

U.S. ARMY

Poor Efficiency:

System cannot not accommodate a large volume of commuters driving at the same time.

Traffic congestions are predictable and are typically of moderate level.



Lack of Resilience:

System cannot recover from adverse events
(car accidents, natural disasters)

Traffic disruptions are not predictable and of variable scale.

US Army Corps of Engineers

U.S. ARMY

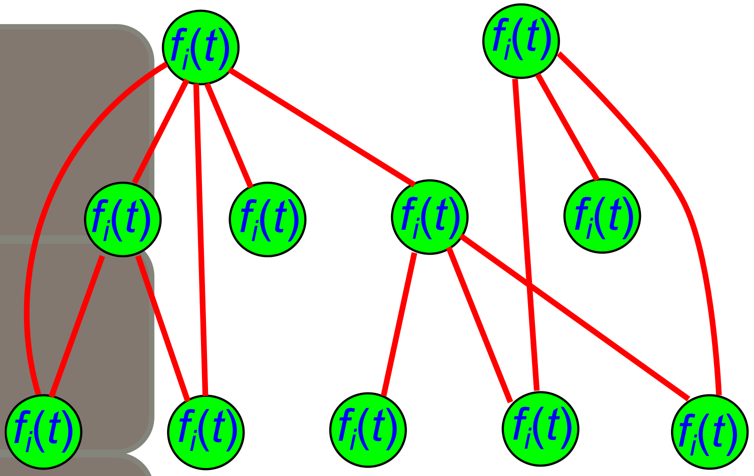
We can model systems through network-based resilience theory

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 ($\boldsymbol{E}$)

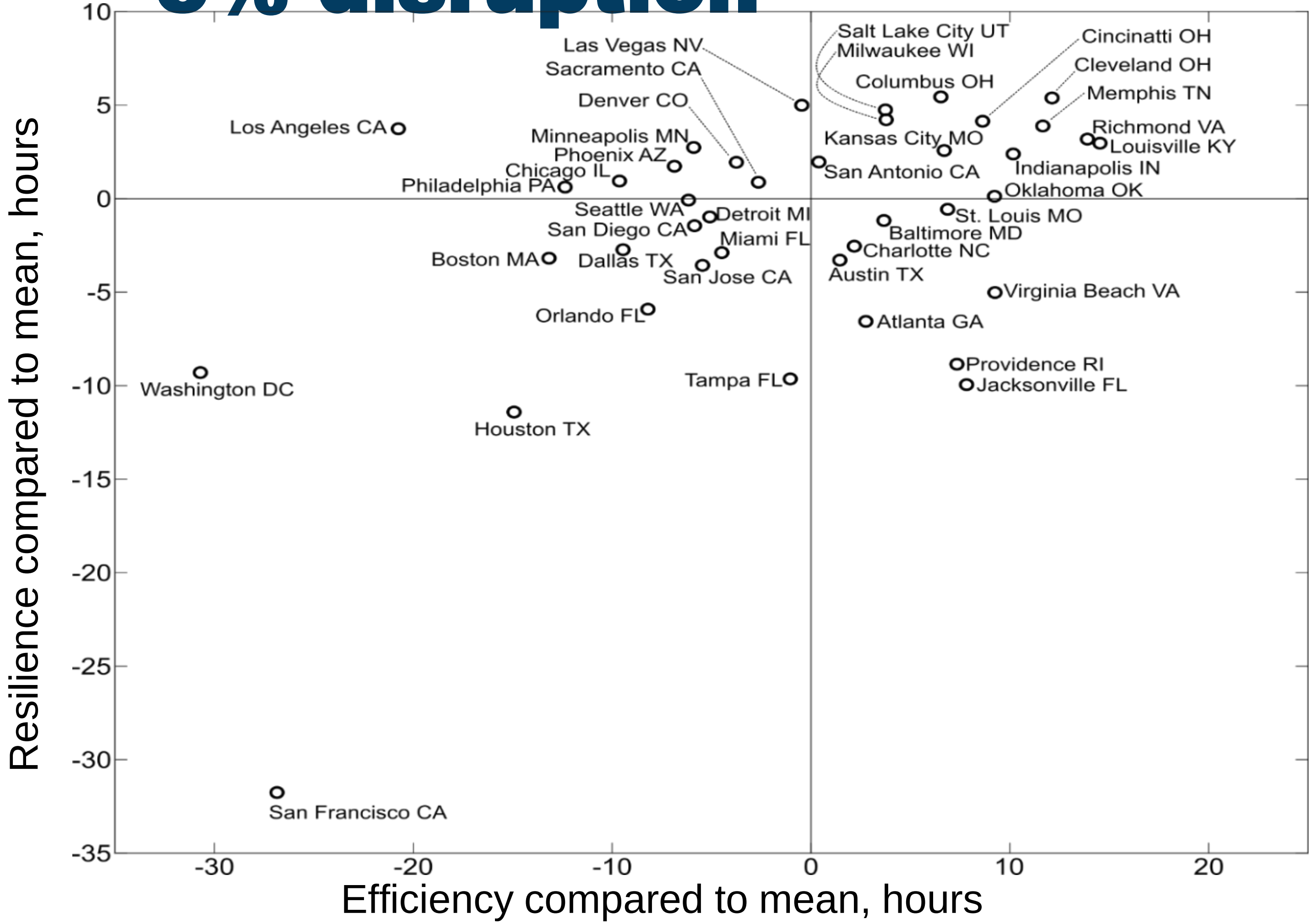


$$R = f(\mathcal{N}, \mathcal{L}, \mathcal{C}, \boldsymbol{E})$$

US Army Corps of Engineers

U.S. ARMY

Resilience vs Efficiency at 5% disruption



SCIENCE ADVANCES | RESEARCH ARTICLE 2017

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]*

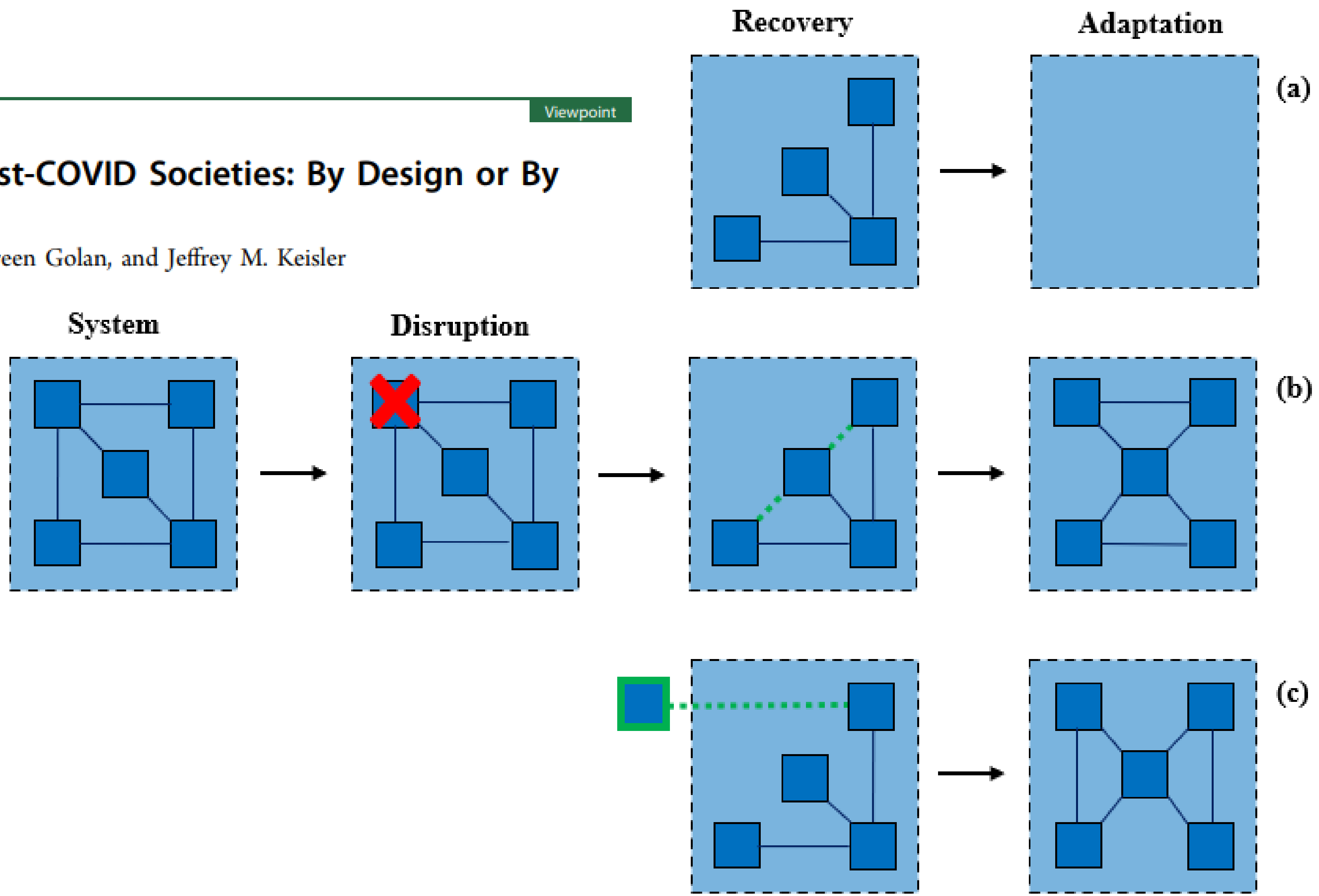
US Army Corps of Engineers

U.S. ARMY

Environmental Science & Technology
pubs.acs.org/est
Viewpoint

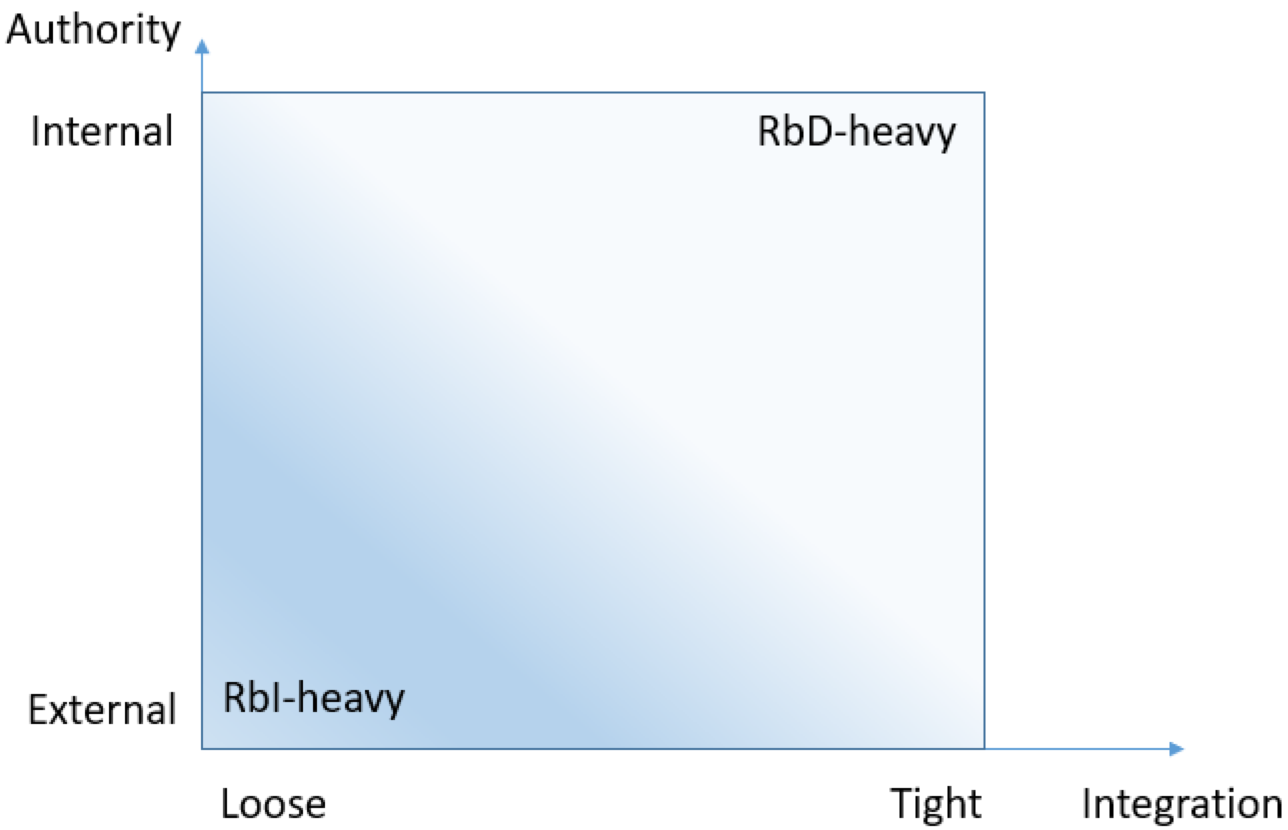
Enhancing Resilience in Post-COVID Societies: By Design or By Intervention?

Igor Linkov,* Benjamin D. Trump, Maureen Golan, and Jeffrey M. Keisler



US Army Corps of Engineers
U.S. ARMY

Resilience by Design and by Intervention for Cyber Systems

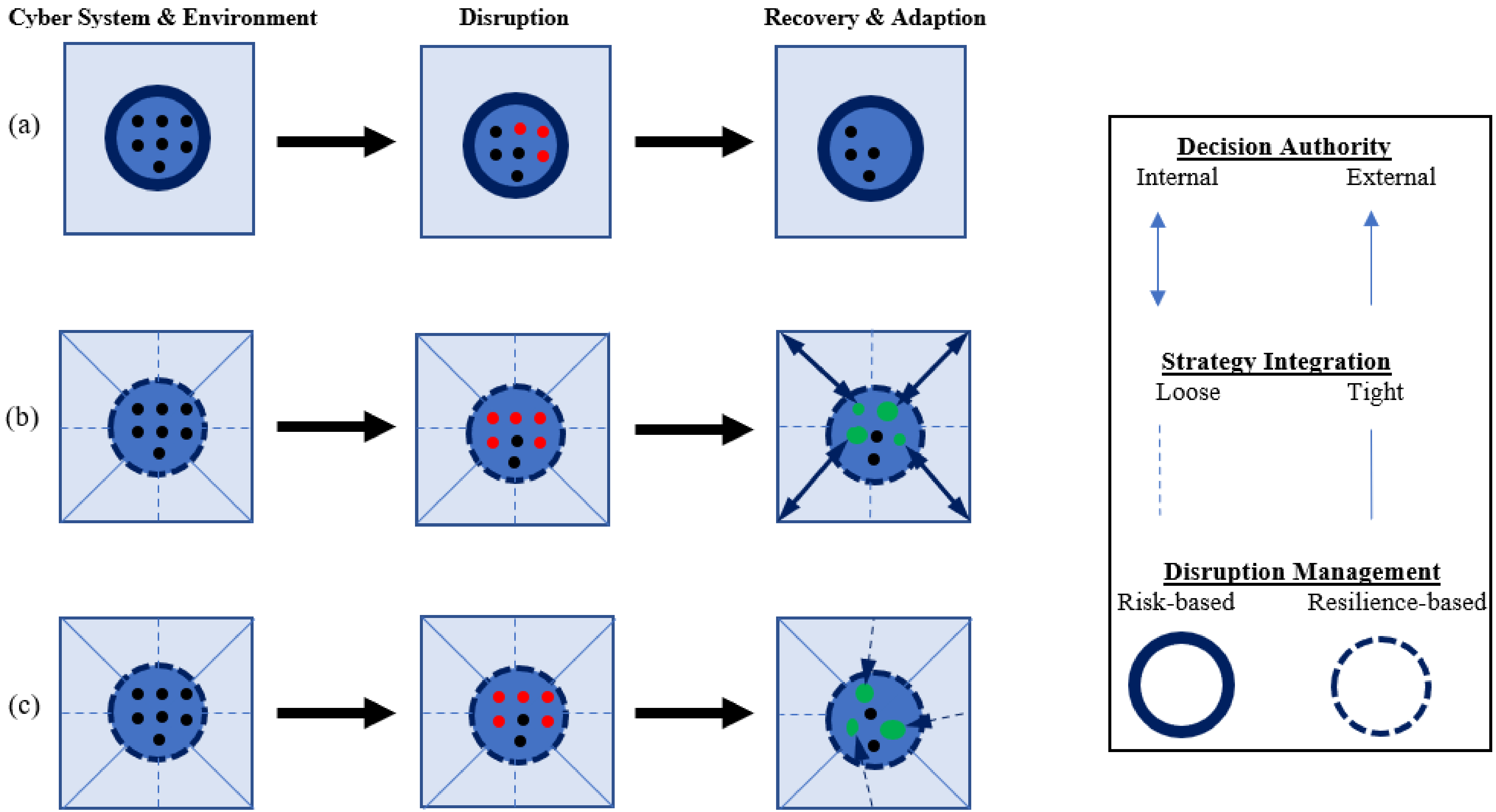


A cybersystem’s reaction to a disruption favors resilience-by-design (RbD) if the corrective actions are tightly integrated and internally governed; whereas a cyber system’s reaction to a disruption favors resilience-by-intervention (RbI) if the corrective actions are loosely integrated and externally governed. Resilience analytics drives the implementation degrees of RbI and RbD.

After Kott, Linkov et al (2021, in press)

US Army Corps of Engineers

U.S. ARMY



Notional cyber systems undergoing threat scenarios illustrating (a) cybersecurity approach that hardens certain system features to reduce anticipated disruption impacts, (b) resilience-by-design (RbD) system recovering and adapting post-disruption through internal authority and tight integration with the corrective actions, and (c) resilience-by-intervention (RbI) system recovering and adapting through external authority and loose integration with the corrective actions. Note that provisions for both RbD and RbI are found in the systems implementing resilience-based disruption management, but is not a requirement.

US Army Corps of Engineers

U.S. ARMY

Three Implementation Strategy Examples of RBI and RBD for Cyber-Dependent Water Systems

1. Resilience-by-intervention (RbI):
The water systems operators have contracts with third-party cybersecurity and recovery plans

2. Hybrid: Resilience-by-design (RbD) and Resilience-by-intervention (RbI)
The water system operators have built-in monitoring and response capabilities, but maintain a third-party provider for black swan events

3. Resilience-by-design:
Water system operators and end-users share onus for maintaining and implementing continuous monitoring, response, recovery and adaptation

US Army Corps of Engineers

U.S. ARMY

Comparison of risk management approaches RbD and RbI for complex systems

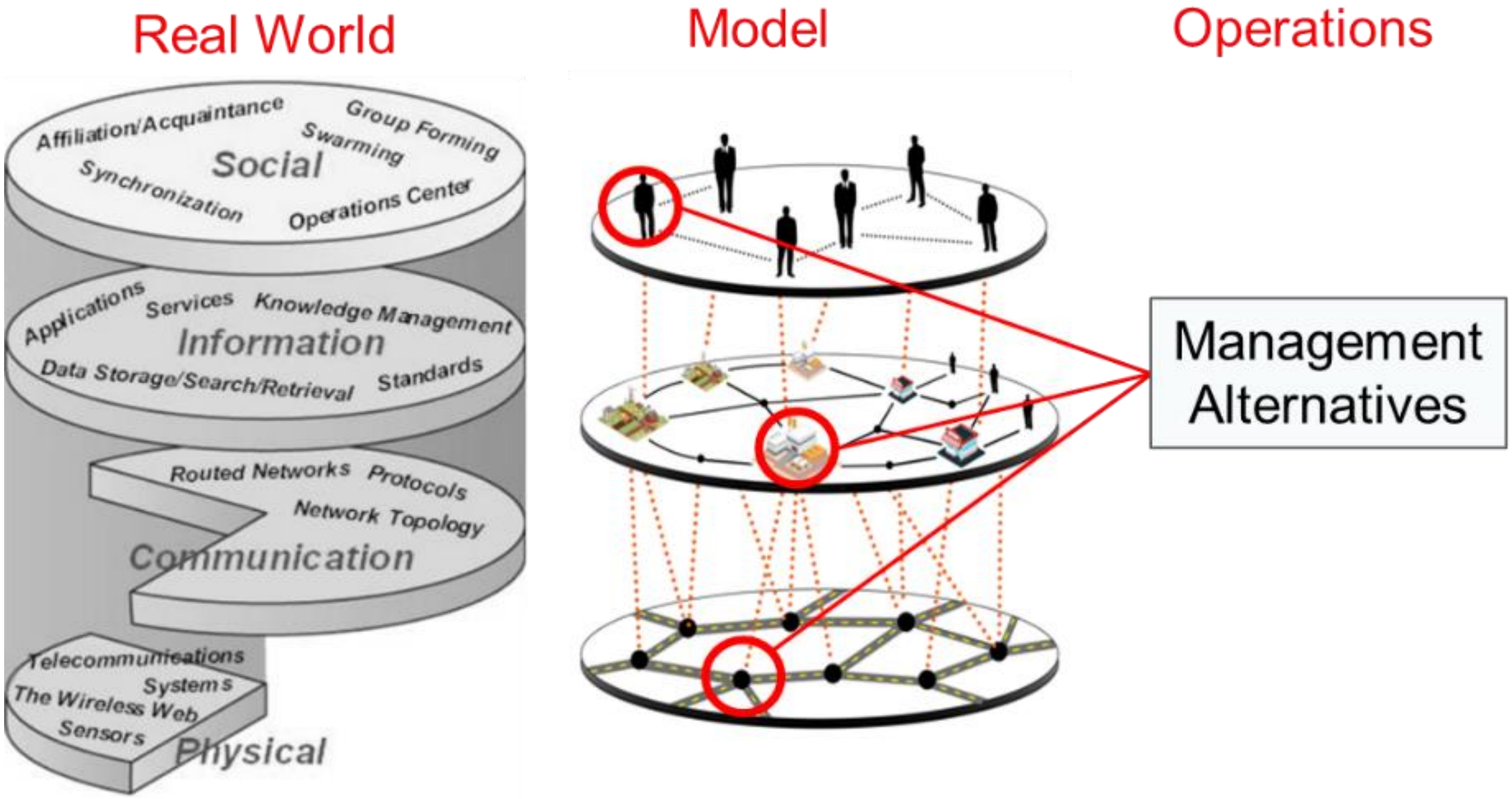
	Risk management	Resilience-by-design	Resilience-by-intervention
Objective	Harden individual components	Design components to be self-reorganizable	Rectify disruption to components and stimulate recovery by external actors
Capability	Predictable disruptions, acting primarily from outside the system components	Either known/predictable or unknown disruptions, acting at a component or system level	Failure in context of societal needs, may be constellation of networks across systems
Consequence	Vulnerable nodes and/or links fail as result of threat	Degradation of critical functions in time and capacity to achieve system's function	Degradation of critical societal function due to cascading failure in interconnected networks.
Actor	Either internal or external to the system	Internal to the system	External to the system
Corrective Action	Either loosely or tightly integrated with the system	Tightly integrated with the system	Loosely integrated with the system
Stages/Analytics	Prepare and absorb (risk is product of threat, vulnerability and consequences and is time independent)	Recover, and adapt (explicitly modeled as time to recover system function and the ability to change system configuration in response to threats)	Prepare, absorb, recover, and adapt (explicitly modeled as ability to recover and secure critical societal function and needs through constellation of relevant systems)

After Kott, A. et al. 2021

US Army Corps of Engineers

U.S. ARMY

Vision for System Resilience



Thank you!

Contact Us:

Dr. Igor Linkov

Igor.Linkov@usace.army.mil

Engineer Research & Development Center

Risk and Decision Science Team

Andrew Jin

asjin@usc.edu

Engineer Research & Development Center

Risk and Decision Science Team

US Army Corps of Engineers®