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

Measuring Resilience: Science and Practice

Igor Linkov, PhD

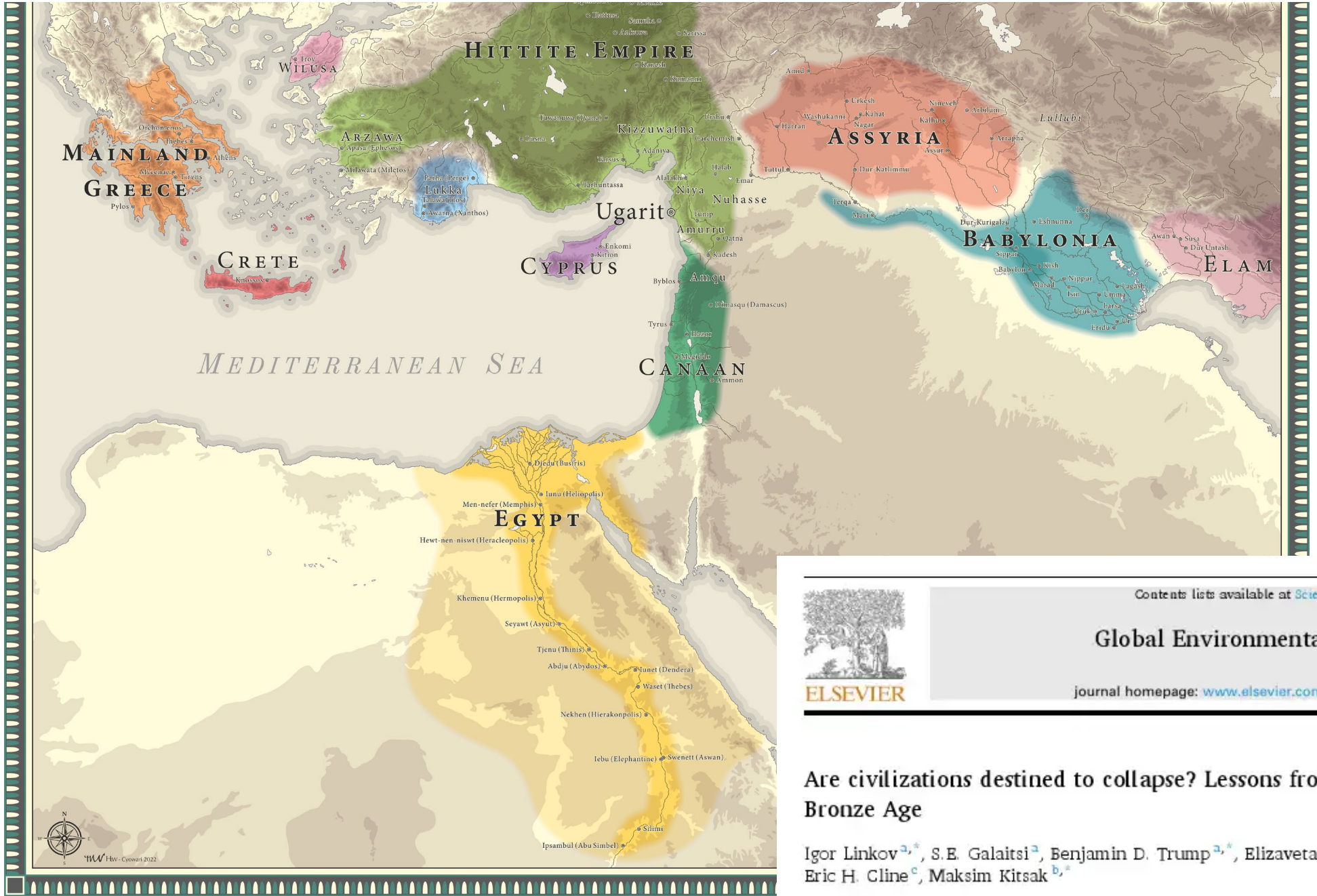
Senior Science and Technology Manager (SSTM), US Army Engineer R&D Center; US Army Corps of Engineers

Adjunct Professor, Carnegie Mellon University and University of Florida

Igor.linkov@usace.army.mil

11 October 2024

The Collapse of the Bronze Age 1200 to 1100 BCE



Contents lists available at ScienceDirect

Global Environmental Change

journal homepage: www.elsevier.com/locate/gloenvcha

Are civilizations destined to collapse? Lessons from the Mediterranean Bronze Age

Igor Linkov[a,*], S.E. Galaitsi[a], Benjamin D. Trump[a,*], Elizaveta Pinigina[a], Krista Rand[a], Eric H. Cline[c], Maksim Kitsak[b,*]

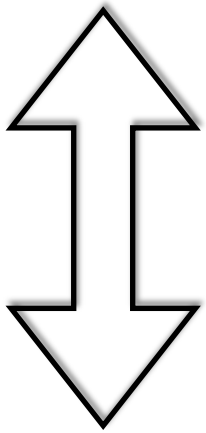
Stability Rule: Region must be stable in both layers simultaneously

N = 10 regions

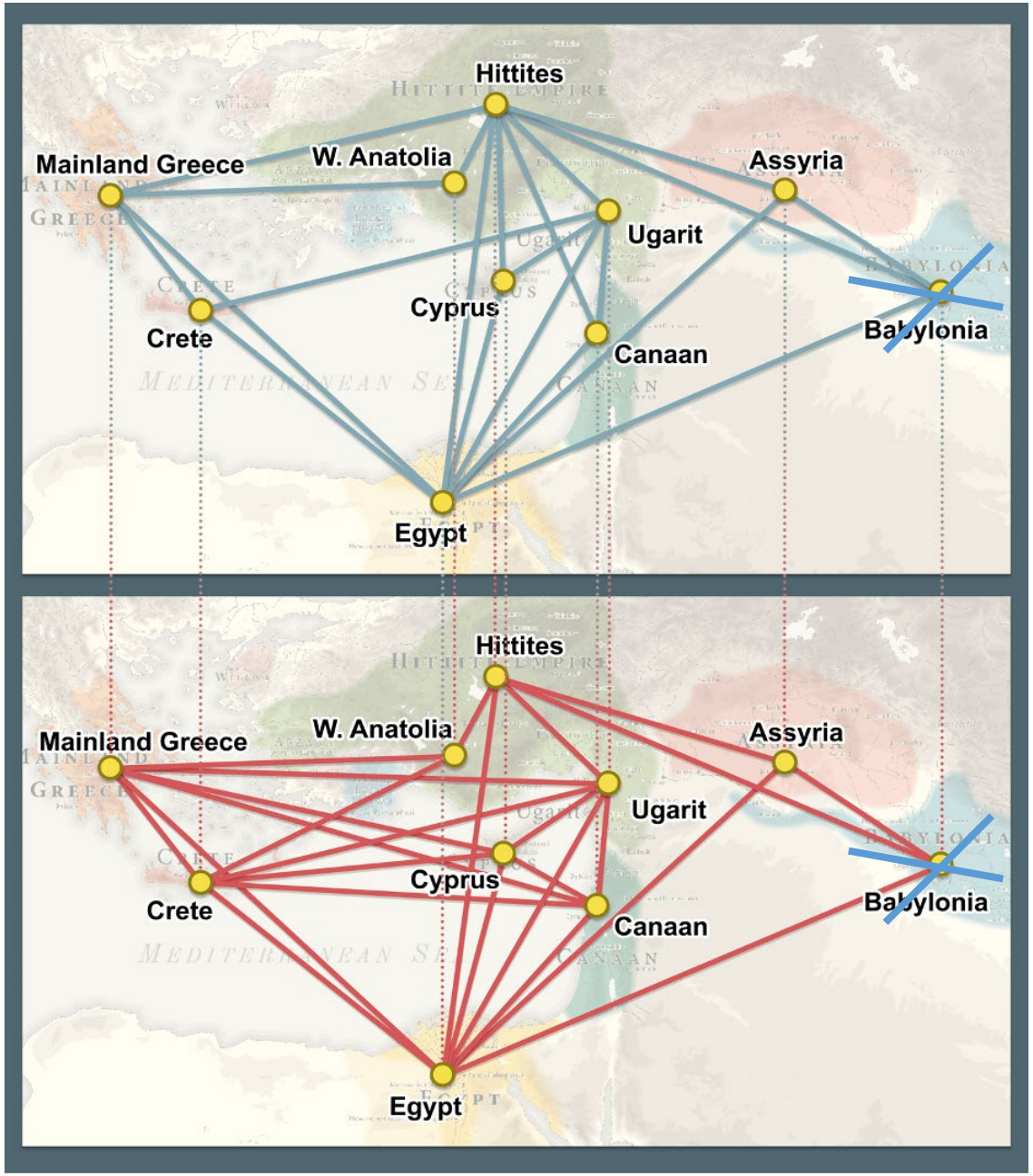
E_1 = 21 political ties

E_1 = 27 trade ties

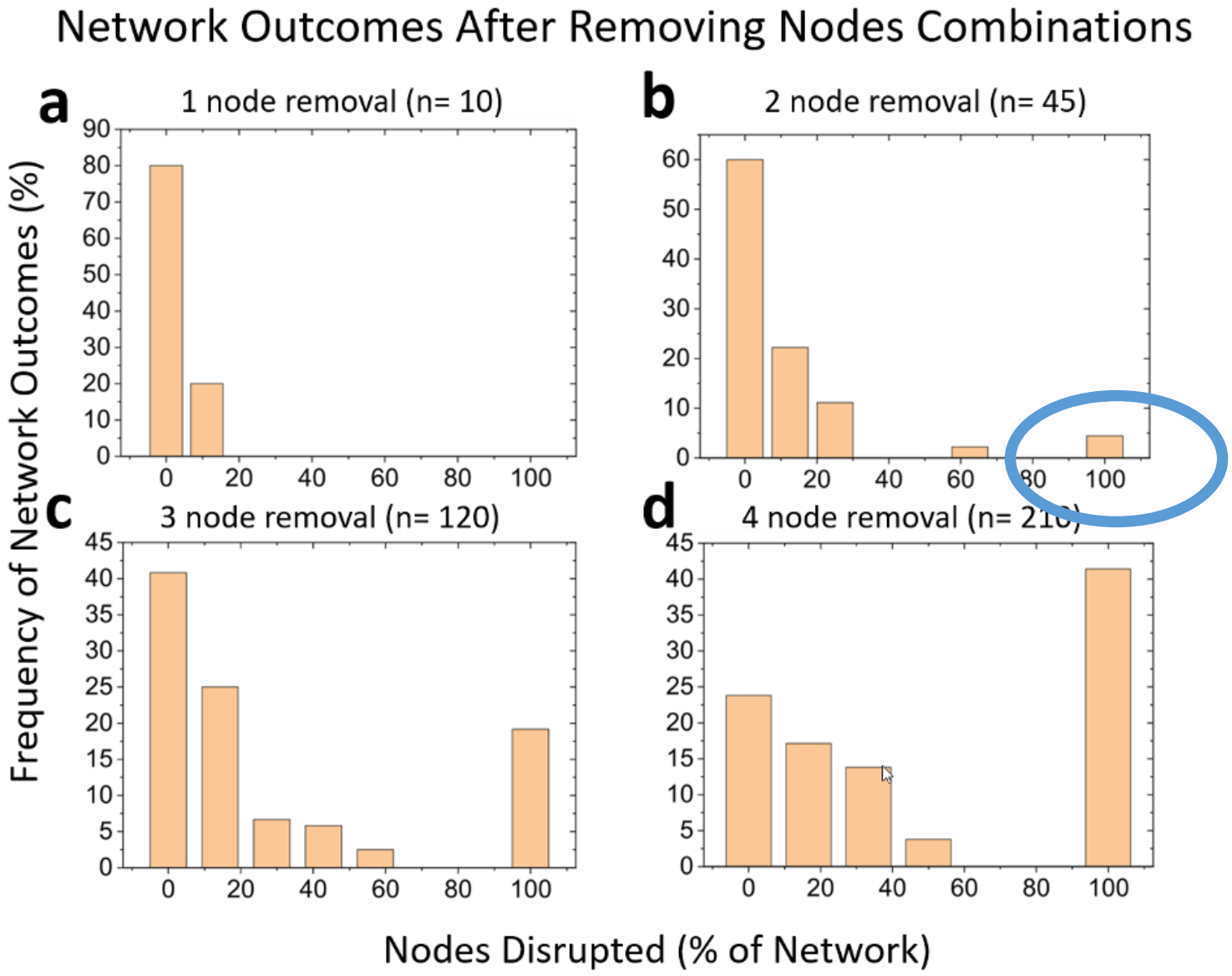
Politics Layer



Trade Layer



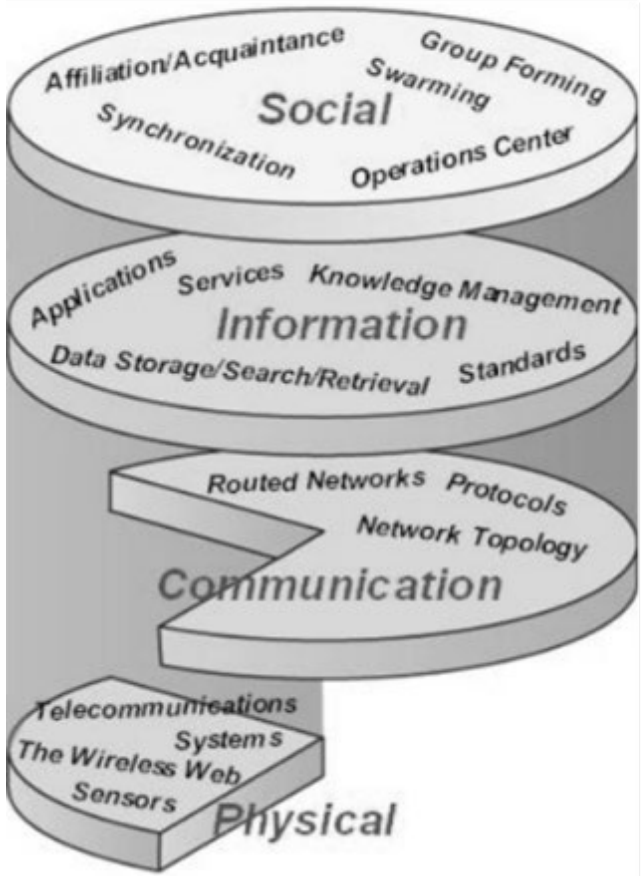
Stress-Test for the Bronze Age Network



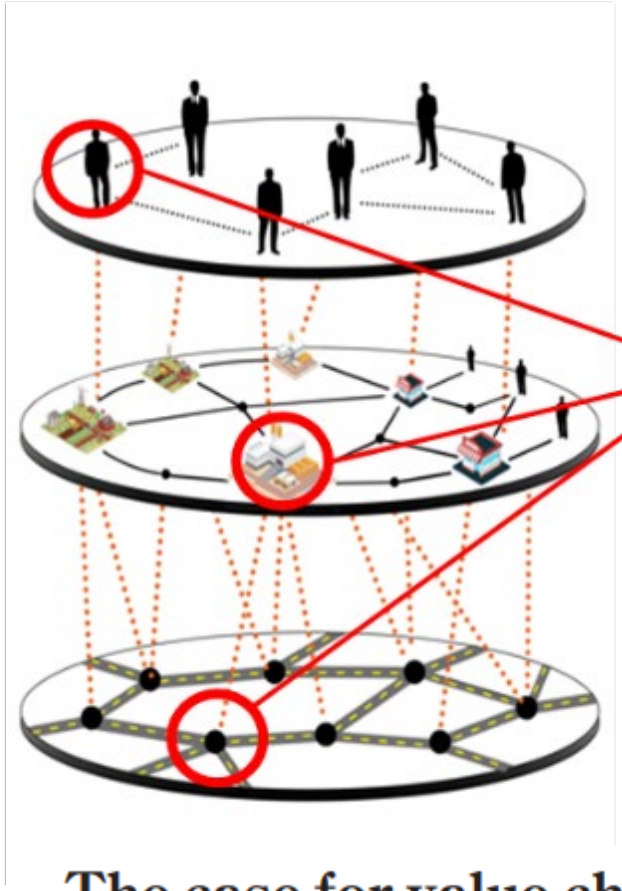
Simultaneous failure of 2 regions can be catastrophic!

Vision for System Resilience

Real World



Model



Operations

Management Alternatives

The case for value chain resilience

Igor Linkov, Savina Carluccio, Oliver Pritchard, Áine Ní Bhreasail, Stephanie Galaitsi, Joseph Sarkis and Jeffrey M. Keisler

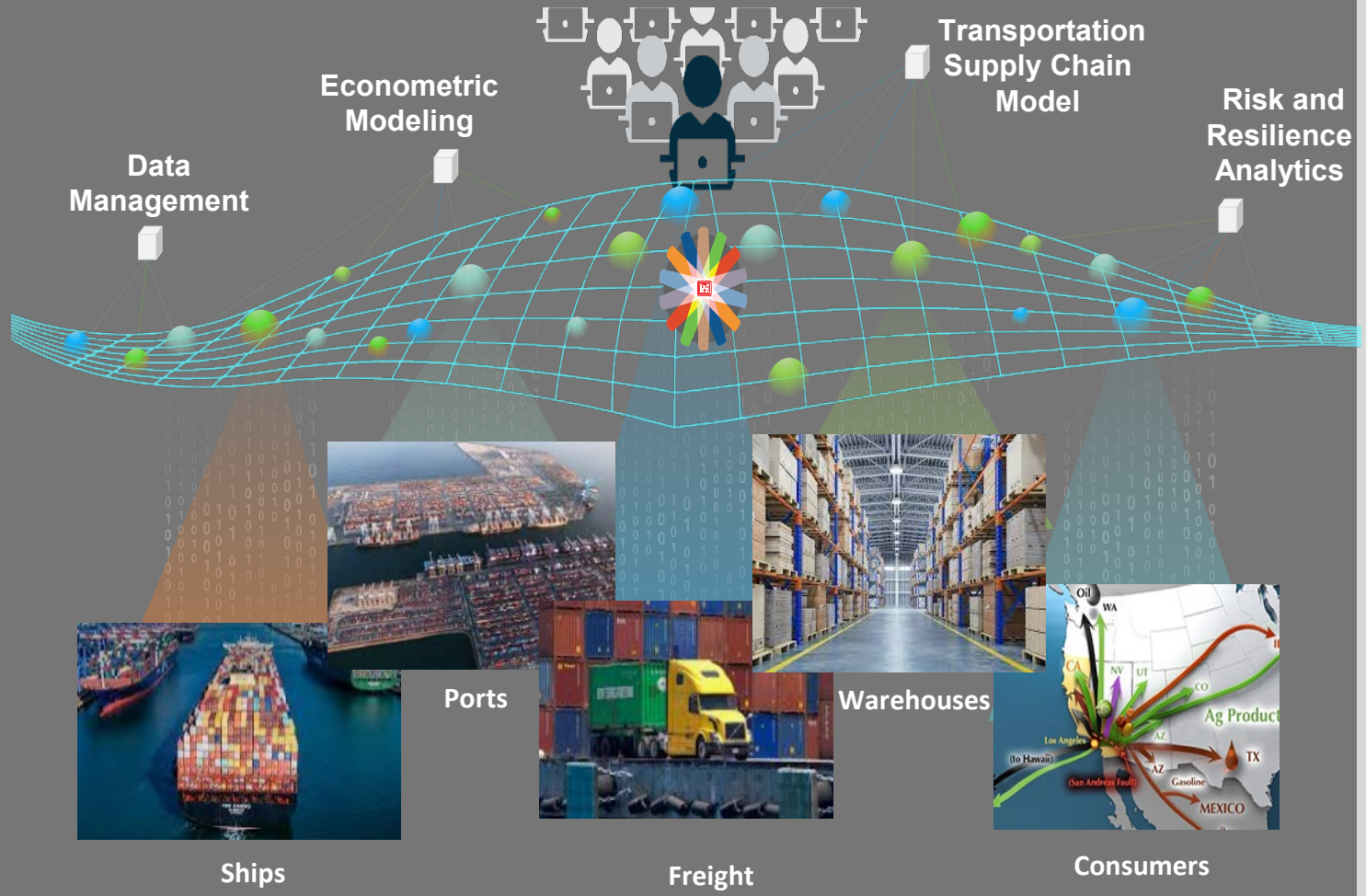
Management Research Review

2040-8269
DOI 10.1108/MRR-08-2019-0353

Approach:
Increase Resilience Through Networks + Analytics

- **Motivations of Approach:**
  - Supply chain transportation is a large, interconnected systems
  - Limiting factors are non-obvious
  - Traditional approaches to comparing projects may not account for these factors

- **Technical Approach:**
  - Network-based, system-level approach
  - Combine with meaningful analytics
  - Relevant to government users



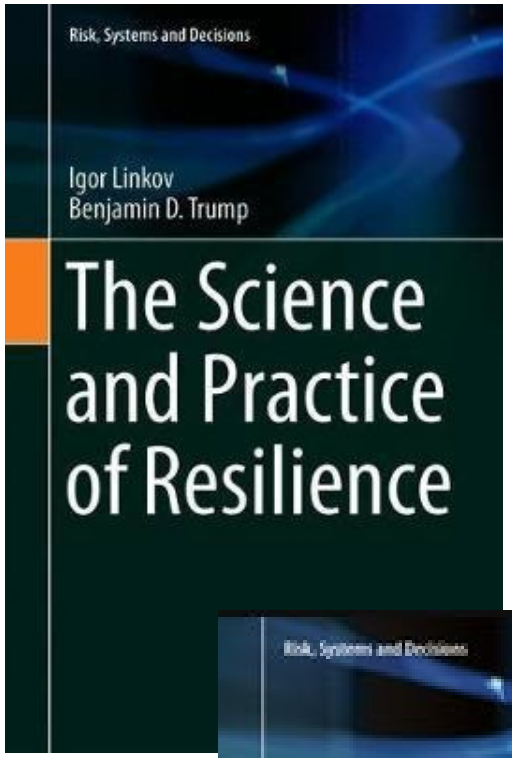
ENVIRONMENTAL LABORATORY

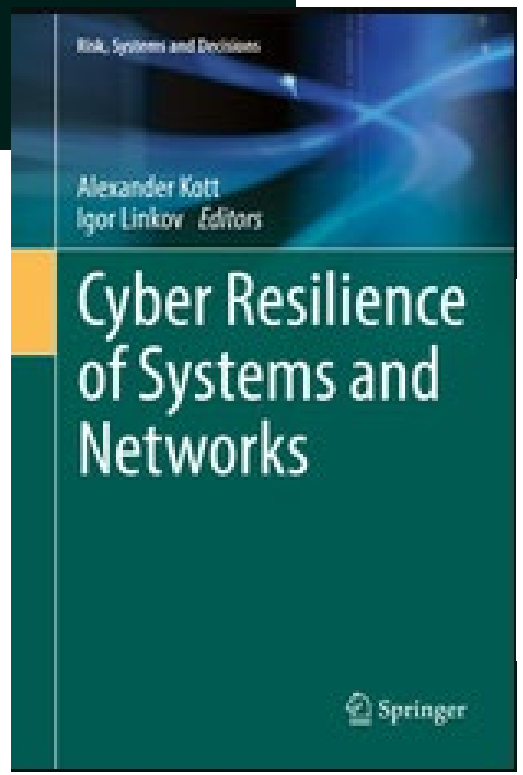
1

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 stakeholders need.

30 | NATURE | VOL 555 | 1 MARCH 2018





COMPUTER PUBLISHED BY THE IEEE COMPUTER SOCIETY

2

To Improve Cyber Resilience, Measure It

Alexander Kott, U.S. Army DEVCOM Army Research Laboratory
Igor Linkov, U.S. Army Engineer Research and Development Center

NATURE ENERGY

Check for updates

comment

Building resilience will require compromise on efficiency

3

nature
CORRESPONDENCE · 08 DECEMBER 2020

Combine resilience and efficiency in post-COVID societies

Benjamin D. Trump, Igor Linkov & William Hynes

4

ELSEVIER
International Journal of Disaster Risk Reduction
Volume 82, November 2022, 103323

Resilience stress testing for critical infrastructure

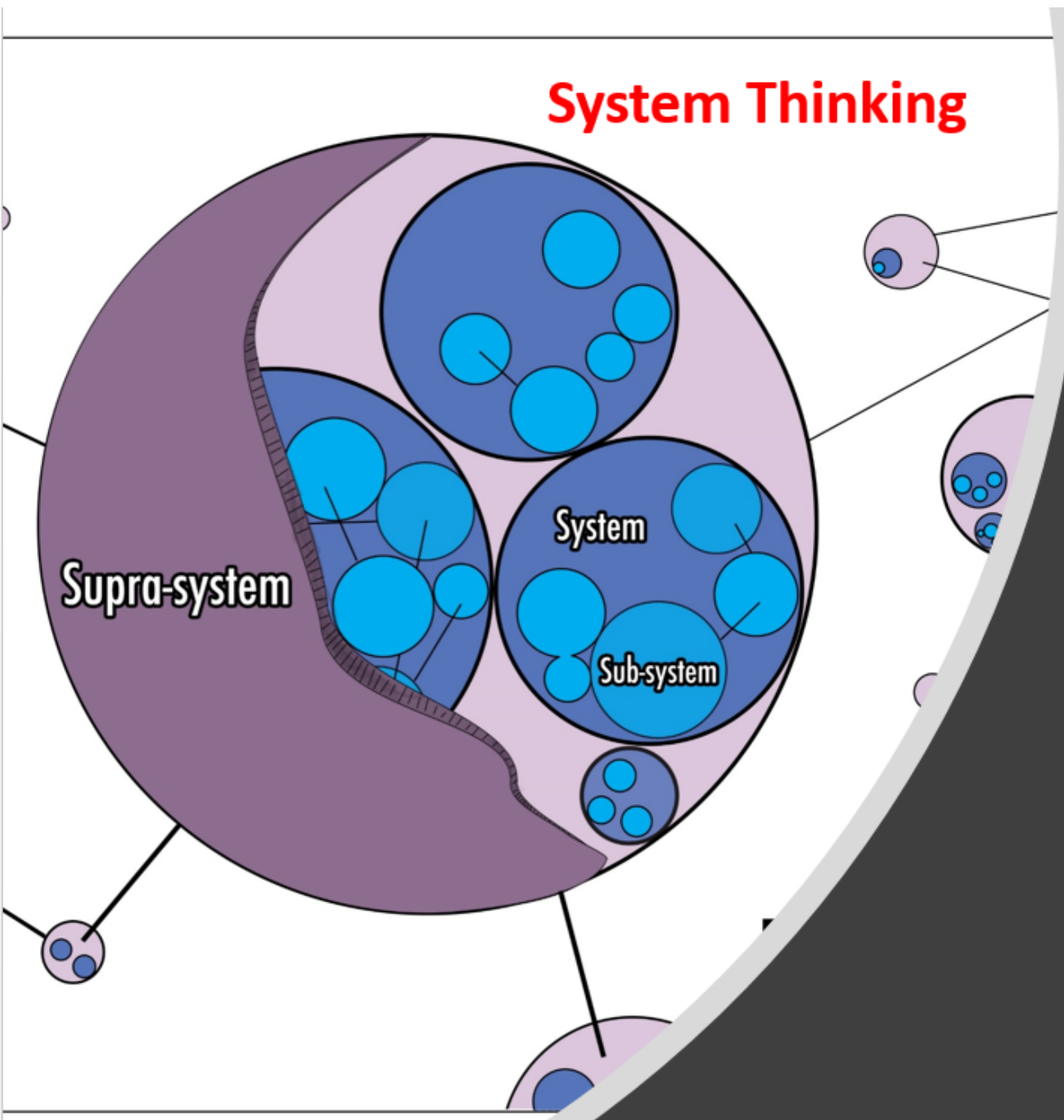
Igor Linkov [a b], Benjamin D. Trump [a c], Joshua Trump [d], Gianluca Pescaroli [e], William Hynes [f], Aleksandrina Mavrodieva [g h], Abhilash Panda [h i]

5

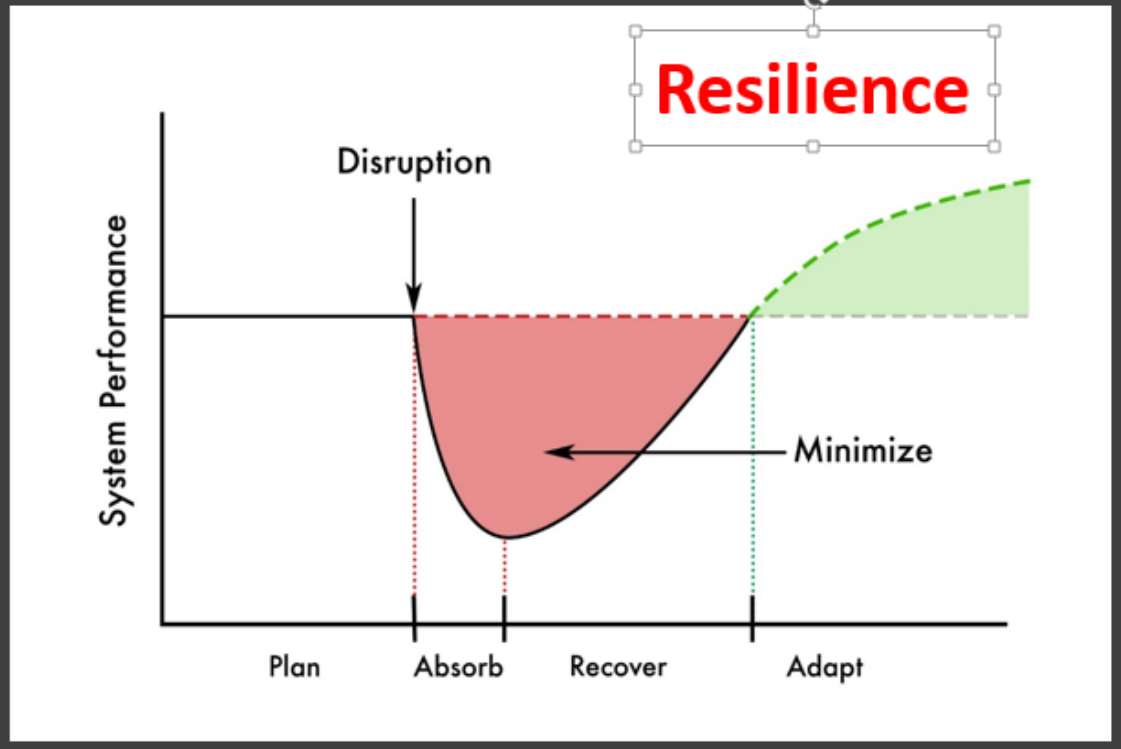
Toward Mission-Critical AI: Interpretable, Actionable, and Resilient AI

Igor Linkov

2023 15th International Conference on Cyber Conflict
Meeting Reality
T. Jančárková, D. Giovannelli, K. Podiņš, I. Winther
2023 © NATO CCDCOE Publications, Tallinn



What Makes Complex Systems (Communities) Susceptible to Threat?



After Linkov and Trump, 2019

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.”

Definitions by Oxford Dictionary

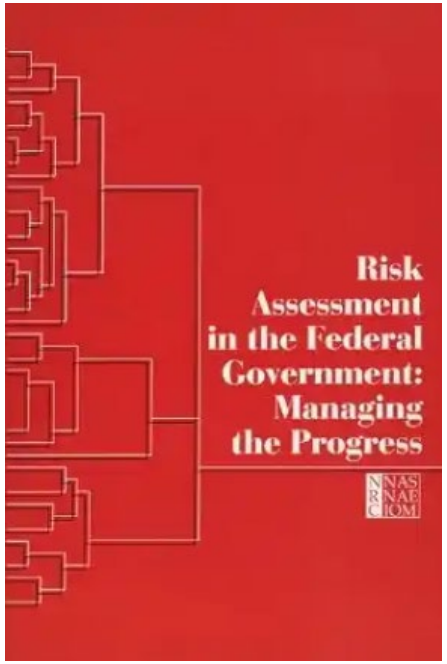
30 | NATURE | VOL 555 | 1 MARCH 2018

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

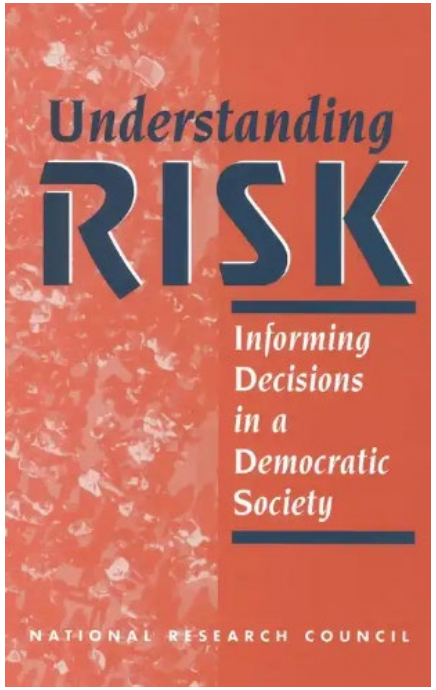
Igor Linkov, Benjamin D. Trump
US Army Corps of Engineers, Concord, Massachusetts, USA.
Jeffrey Keisler *University of Massachusetts Boston, USA.*
igor.linkov@usace.army.mil

Evolution of Regulatory Risk Assessment

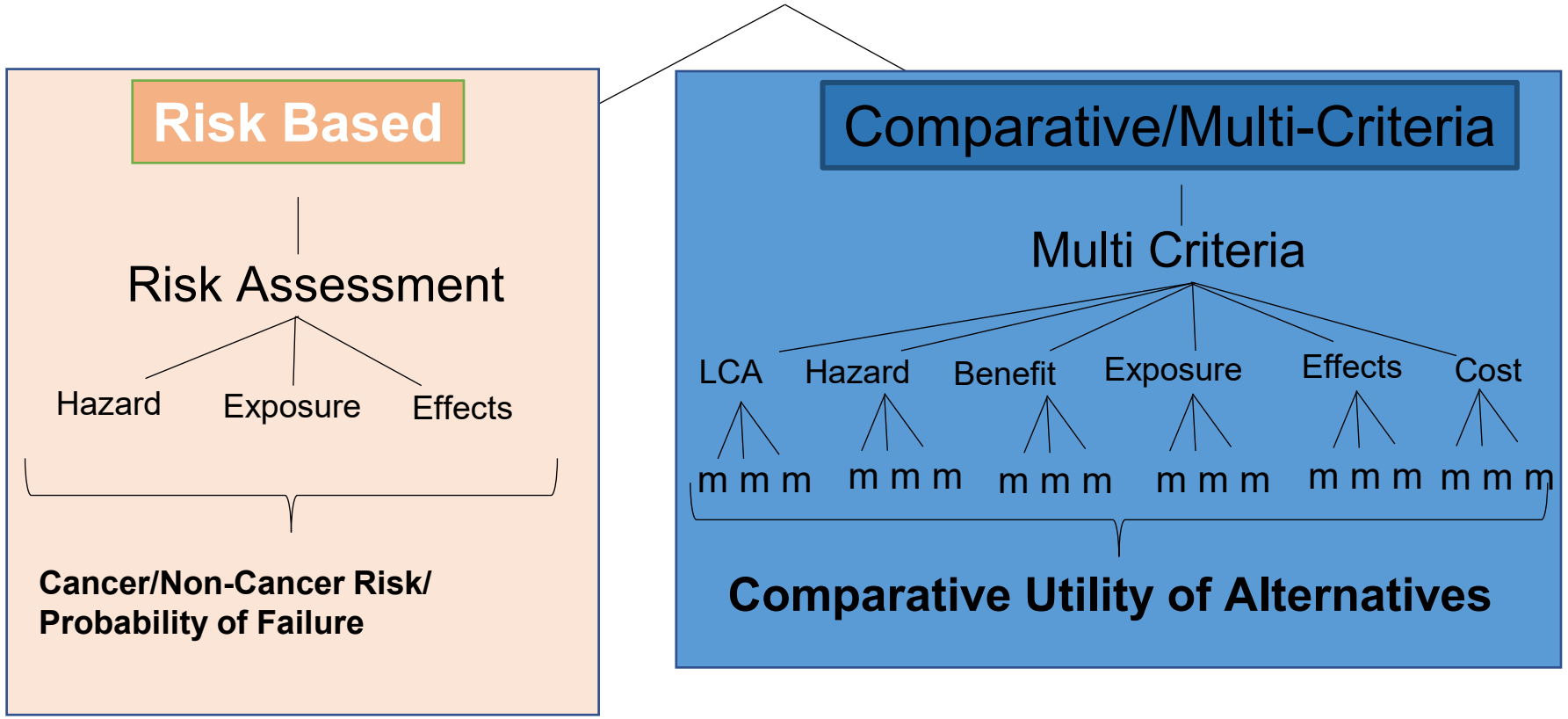


- 1970's- Risk=Probability x Consequence
- 1980's- Risk = Hazard x Exposure x Consequence
  =Threat x Vulnerability x Consequence
- 2000's- Risk $\sim f(H \times E \times E_{ff})$

$m_{H1} m_{H1} \ldots m_{Hn}$ $m_{E1} m_{E1} \ldots m_{En}$ $m_{Eff1} m_{Eff2} \ldots m_{Effn}$



Decision Analysis and Risk Governance



ENVIRONMENTAL Science & Technology

Viewpoint

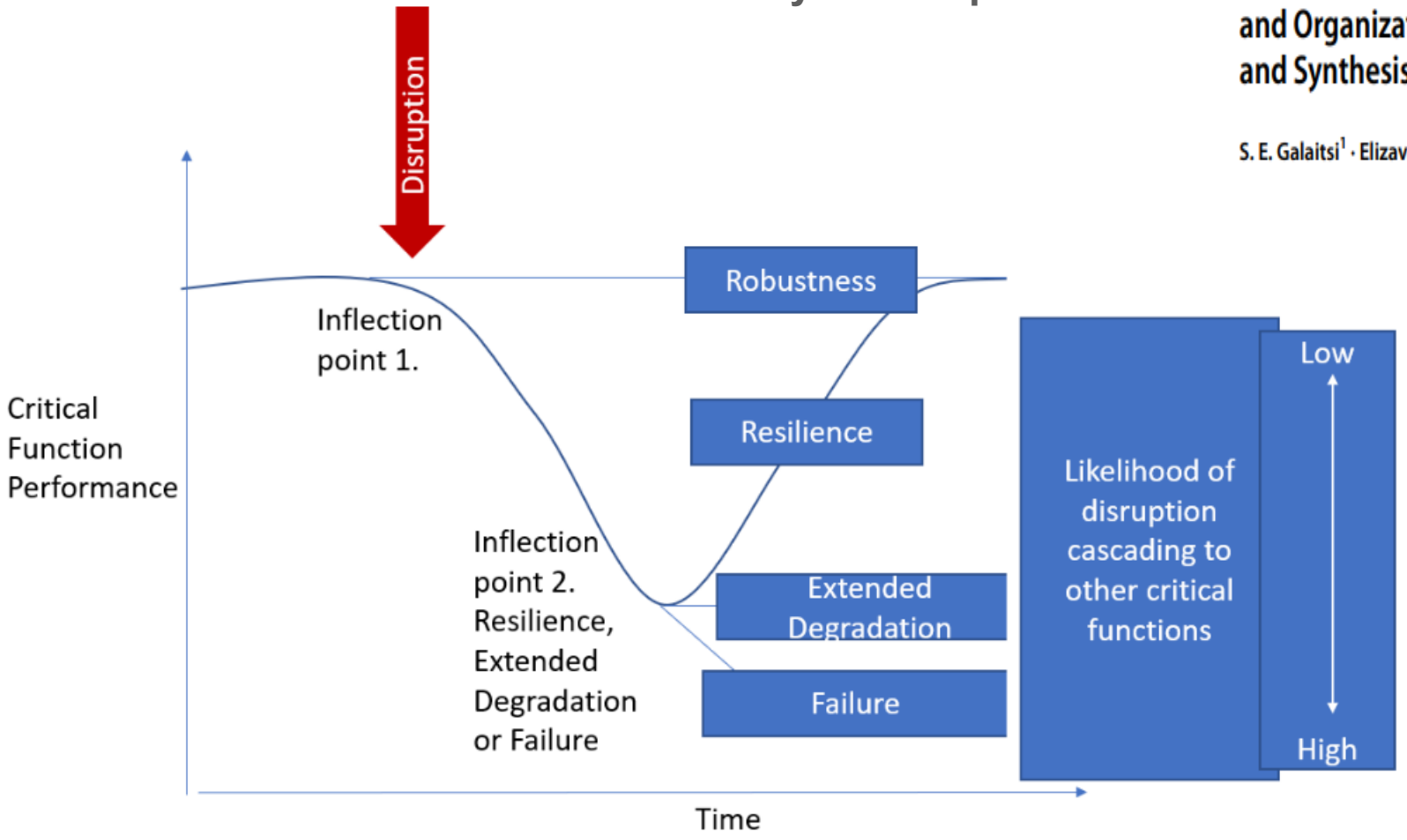
pubs.acs.org/est

Risk-Based and Prevention-Based Governance for Emerging Materials

Timothy Malloy,[†] Benjamin D. Trump,[‡,§] and Igor Linkov*[,§]

Crisis Management, Risk and Resilience

Risk~ Threat*Vulnerability*Consequence

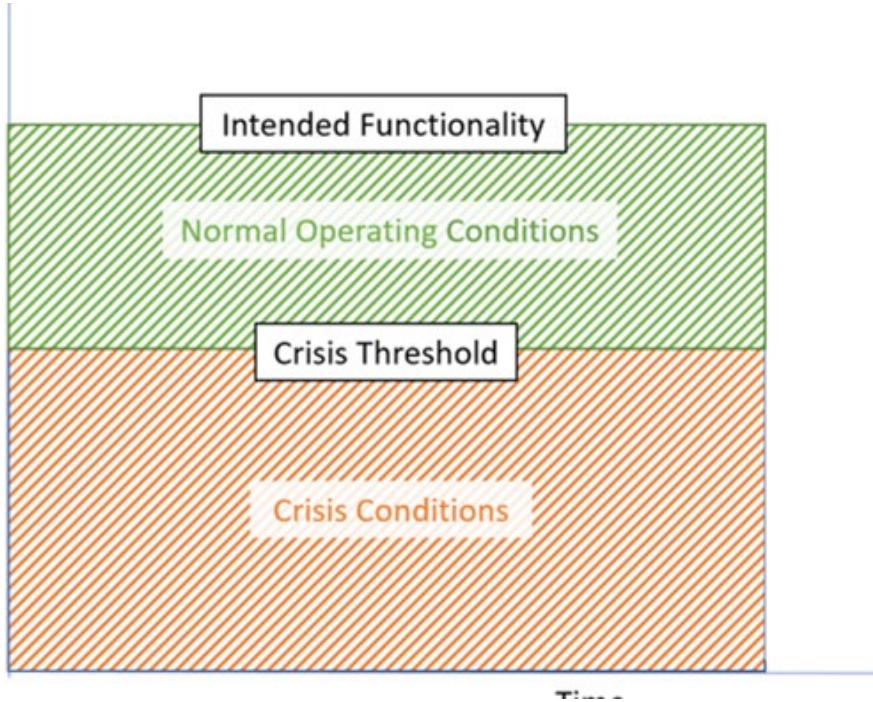


International Journal of Disaster Risk Science
https://doi.org/10.1007/s13753-023-00494-x
www.ijdrs.com
www.springer.com/13753

ARTICLE

Business Continuity Management, Operational Resilience, and Organizational Resilience: Commonalities, Distinctions, and Synthesis

S. E. Galaitsi[1] · Elizaveta Pinigina[1] · Jeffrey M. Keisler[2] · Gianluca Pescaroli[3] · Jesse M. Keenan[1,4] · Igor Linkov[1]



Galaitsi, Linkov et al, 2023

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, tl
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

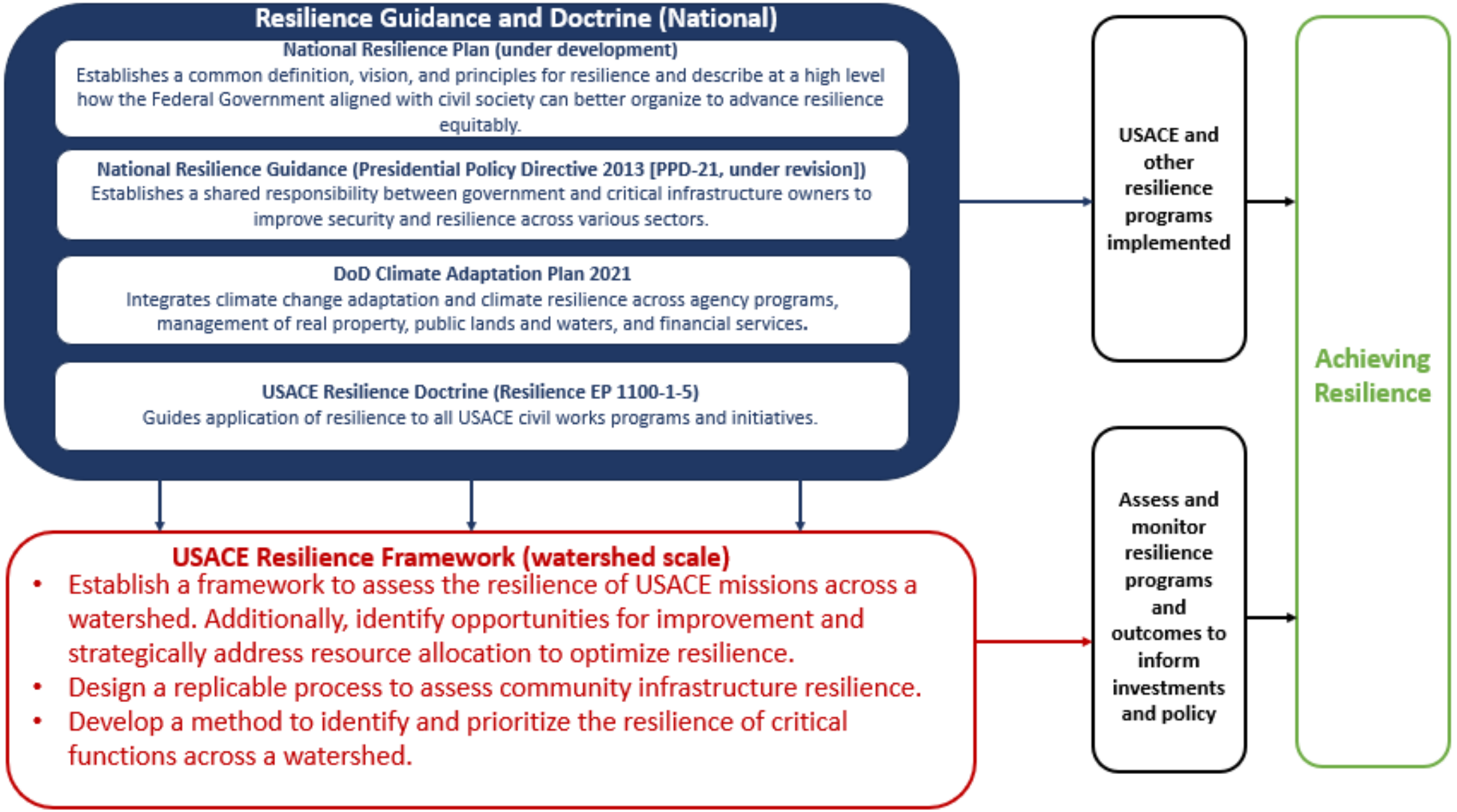
Office of the Press Secretary

For Immediate Release May 11, 2017

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

EXECUTIVE ORDER

Resilience at the National Scale (USACE example)



DEFENCE STUDIES
https://doi.org/10.1080/14702436.2024.2365218

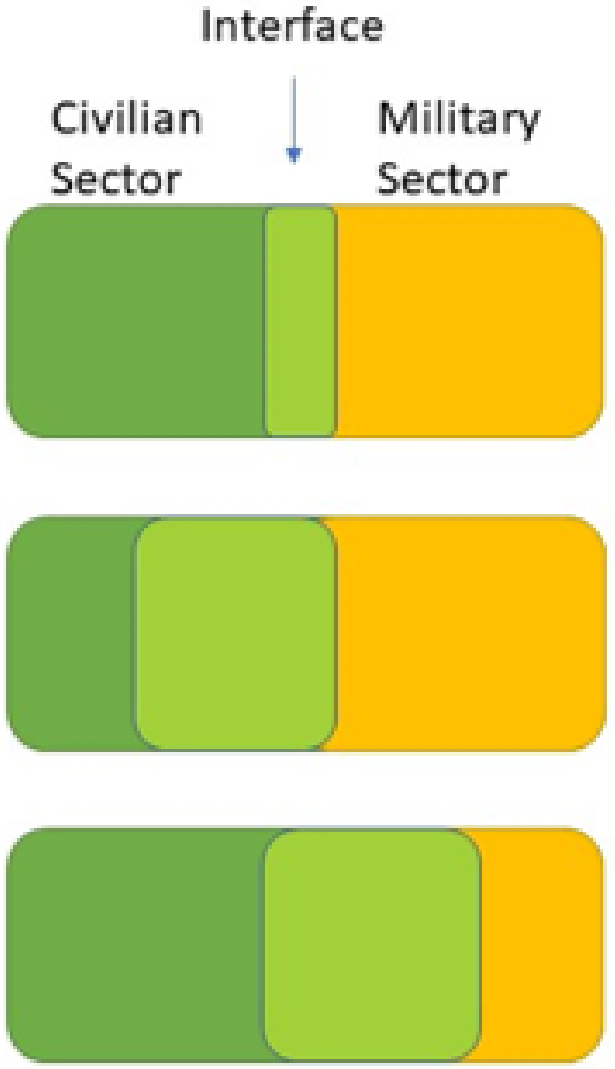
Routledge
Taylor & Francis Group

OPEN ACCESS Check for updates

The role of science in resilience planning for military-civilian domains in the U.S. and NATO

Jesse M. Keenan[a,b], Benjamin Trump[a], Eero Kytömaa[c], Gitanjali Adlakha-Hutcheon[d] and Igor Linkov[a]

NATO-Layered Resilience and USA National Resilience Plan



Scenario 1: No disruption

Military and civilian sectors are operation with small interface

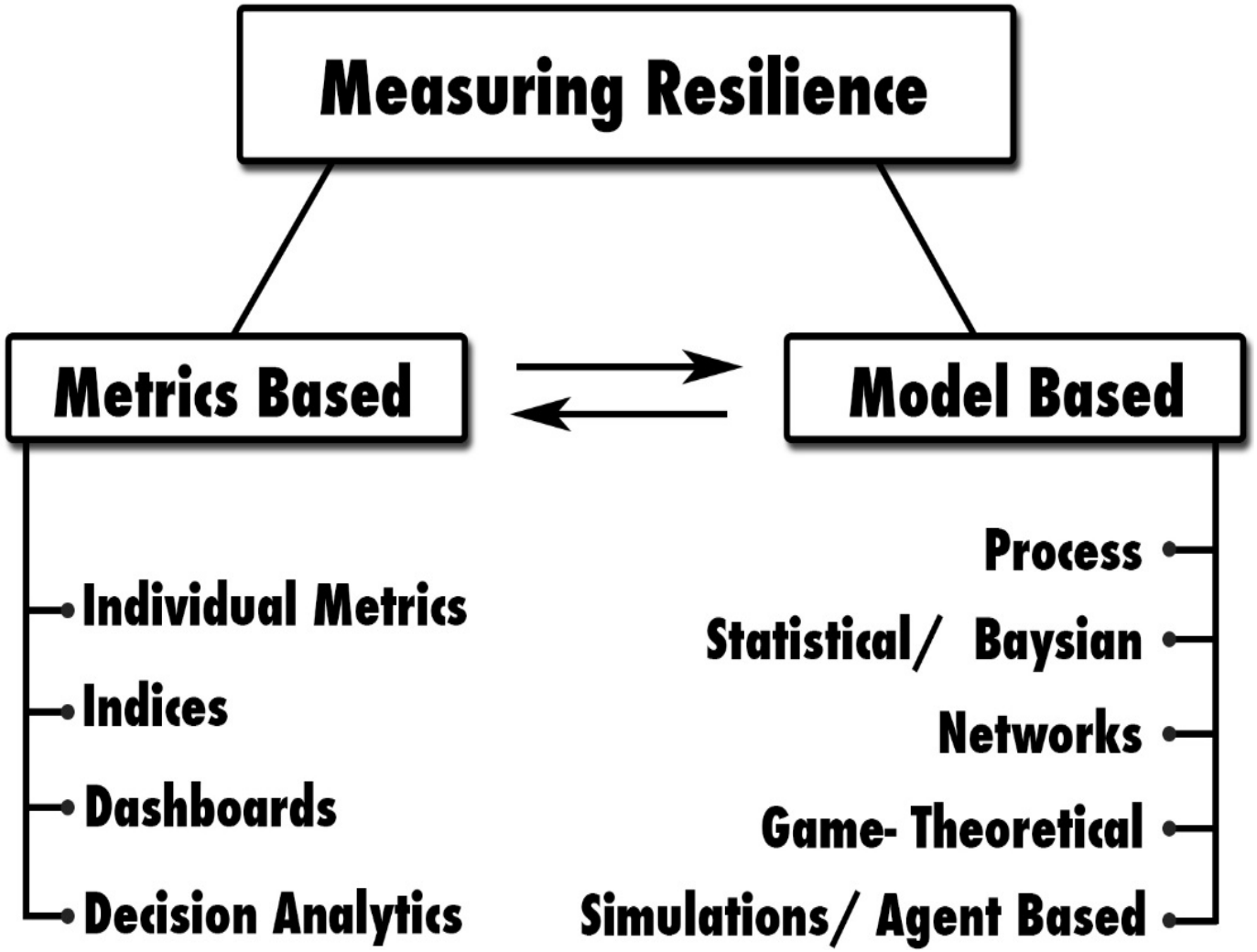
Scenario 2: Attack on military

Interface expands to more civilian resources to support the military

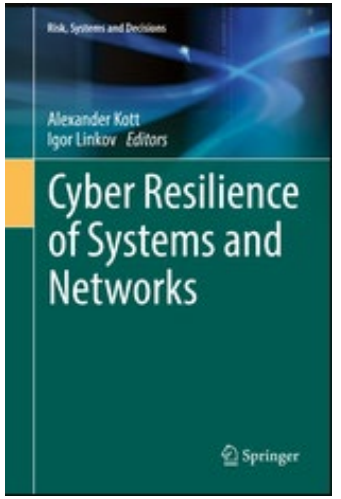
Scenario 3: Jeopardy in Civilian sector

Interface expands to more military resources to support more civilian institutions

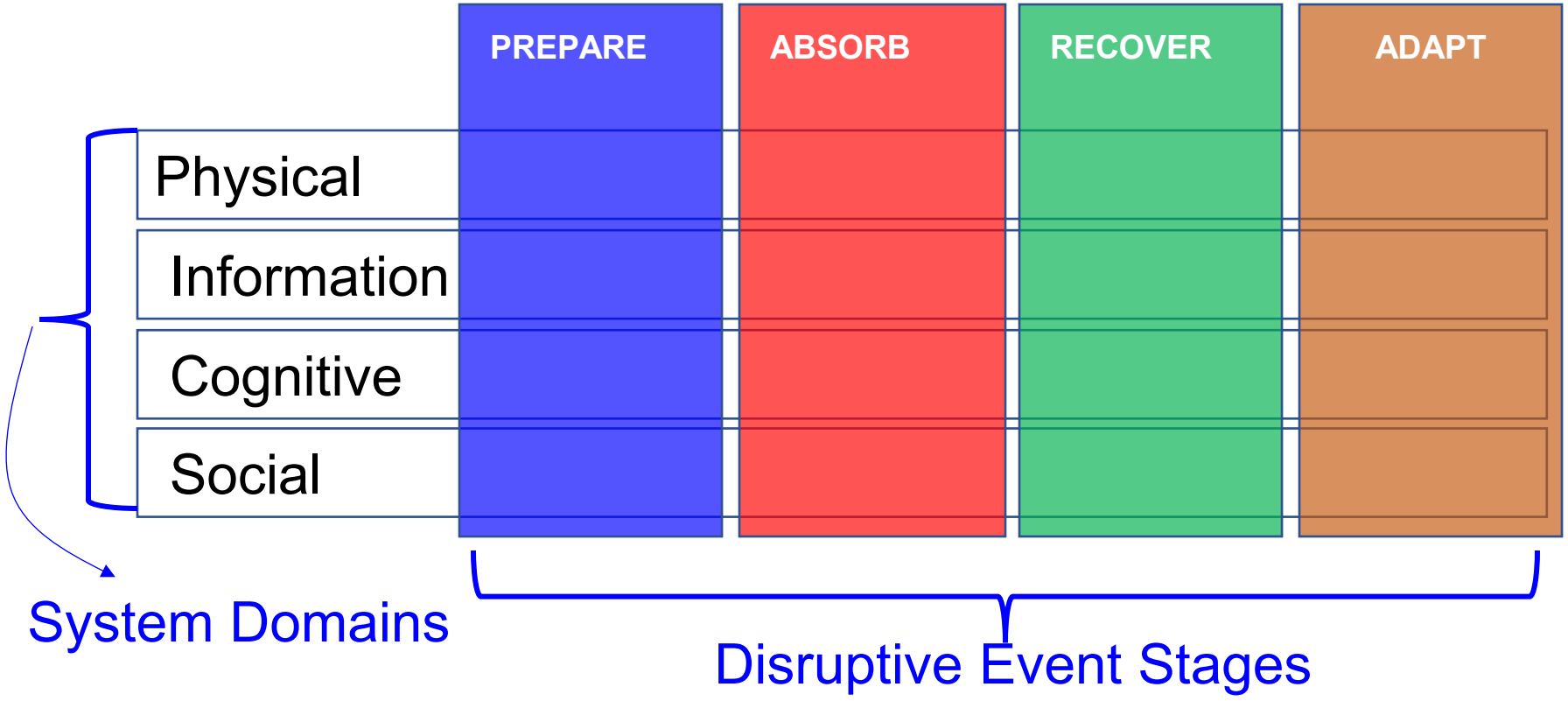
How to Quantify Resilience?

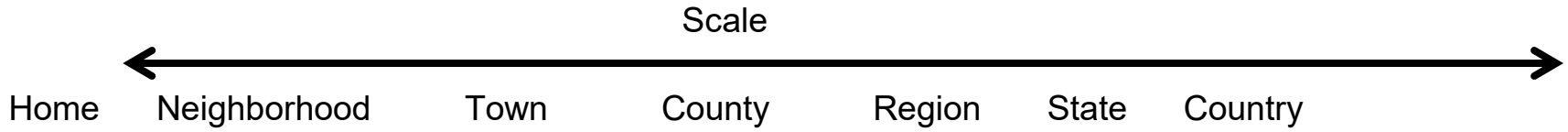


After 2019



Resilience Matrix





Assessment using Stakeholder Values

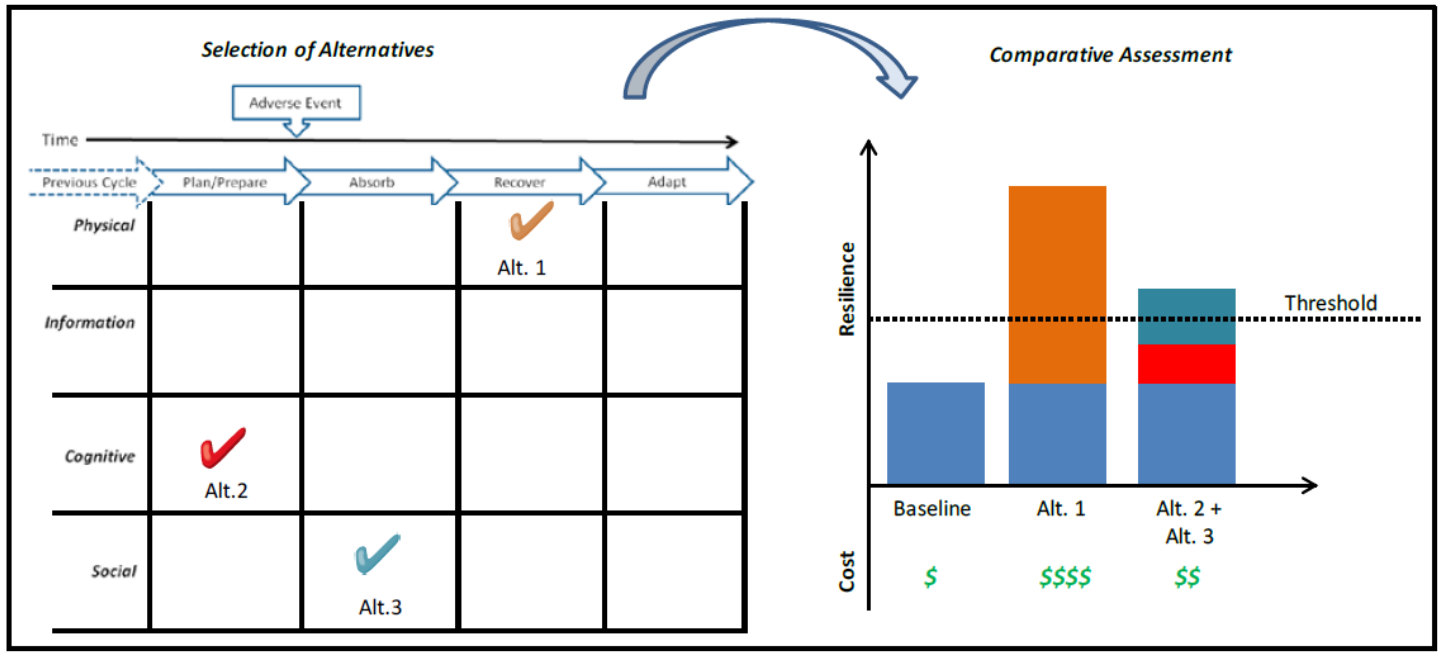


Figure 5: Comparative Assessment of Resilience-Enhancing Alternatives

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

After Fox-Lent et al., 2015

Contents lists available at ScienceDirect

Energy Policy

journal homepage: www.elsevier.com/locate/enpol

Short Communication

Metrics for energy resilience

Paul E. Roege [a], Zachary A. Collier [b], James Mancillas [c], John A. McDonagh [c], Igor Linkov [b,*]

Resilience Matrix: Energy

	Plan and Prepare for	Refs	Absorb	Refs	Recover from	Refs	Adapt to	Refs
Physical	Reduced reliance on energy/increased efficiency	A,B, E,F, H	Design margin to accommodate range of conditions	B,C, I,J,K	System flexibility for reconfiguration and/or temporary system installation	C,D, F,H, K	Flexible network architecture to facilitate modernization and new energy sources	C,D, F,K
	Energy source diversity/ local sources	A,E, F,H, K	Limited performance degradation under changing conditions	B,C, F,I,K	Capability to monitor and control portions of system	B,I, K	Sensors, data collection and visualization capabilities to support system performance trending	D,E, I,K
	Energy storage capabilities/ presaged equipment	B,H, K	Operational system protection (e.g., pressure relief, circuit breakers)	I,K	Fuel flexibility	C,D, E,F	Ability to use new/alternative energy sources	C,F, H
	Redundancy of critical capabilities	D,E, I,K	Installed/ready redundant components (e.g., generators, pumps)	D,I, K	Capability to re-route energy from available sources	C,D, F,I,K	Update system configuration/ functionality based upon lessons learned	C,D, L,F,I, K
	Preventative maintenance on energy systems	I,K	Ability to isolate damaged/ degraded systems/ components (automatic/ manual)	E,I,K	Investigate and repair malfunctioning controls or sensors	I	Phase out obsolete or damaged assets and introduce new assets	A,C, D,I, K
	Sensors, controls and communication links to support awareness and response	H,I, K	Capability for independent local/sub-network operation	D,K	Energy network flexibility to re-establish service by priority.	F,I,K	Integrate new interface standards and operating system upgrades	D,I, K
	Protective measures from external attack (physical/ cyber)	A,D, I,K	Alternative methods/ equipment (e.g., paper copy, flashlights, radios)	B,H, K	Backup communication, lighting, power systems for repair/recovery operations	I,K	Update response equipment/ supplies based upon lessons learned	D,L
Information	Capabilities and services prioritized based on criticality or performance requirements	B	Environmental condition forecast and event warnings broadcast	E,H, I	Information available to authorities and crews regarding customer/community needs/ status	D,I	Initiating event, incident point of entry, associated vulnerabilities and impacts identified	A,D, H,I, K
	Internal and external system dependencies identified	B,G, H	System status, trends, margins available to operators, managers and customers	D,E, H,I, K	Recovery progress tracked, synthesized and available to decision-makers and stakeholders	D,I	Event data and operating environment forecasts utilized to anticipate future conditions/ events	D,H, I,K
	Design, control, operational and maintenance data archived and protected	B,I	Critical system data monitored, anomalies alarmed	D,E, I,K	Design, repair parts, substitution information available to recovery teams	K	Updated information about energy resources, alternatives and emergent technologies available to managers and stakeholders	D,F, H,I
	Vendor information available	B	Operational/troubleshooting/ response procedures available	I,K	Location, availability and ownership of energy, hardware and services available to restoration teams	K	Design, operating and maintenance information updated consistent with system modifications	F,I,K

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]			
(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) Review physical a in order t decisions	

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

USACE Resilience Matrix Methodology

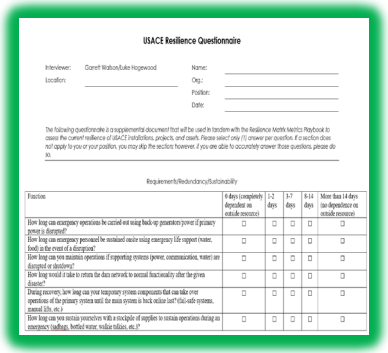
Resilience Matrix

	Absorb	Recover	Adapt
Physical	System Performance/Functionality System Reliability Robustness Consequences of failure System Vulnerability Hazard Mitigation Measures Redundancy Back-up Systems Emergency Resources	Recovery Time Temporary Facilities Recovery Resources	Adaptive Capacity Infrastructure Condition Modularity
Information	Failure Detection Systems Hazard Forecasting Risk Assessment/Data Emergency Planning Mitigation Planning Disaster Propagation Models	Recovery Tracking Data Models for Recovery Scenarios Recovery Planning	Post-disaster data collection Adaptation Planning Plan Improvements
Social	Emergency Staffing Emergency Support Agreements Community Communication Staff Emergency Training	Community Recovery Assistance Contractor Agreements Recovery Agreements	Training Exercises Community Education Improved Legislation

Master Metrics

Metric Identification and Categorization							
Metric Name	Unit of Analysis	System Domain	Resilience Phase	Metric Category	Critical Function	Measure Full Name	Level of Detail
Risk Assessment Score	Capability	Physical	Absorb	System Vulnerability	FRM	Score from most recent Risk Assesment	Tier 2
Last Inspection Date	Capability	Information	Absorb	Risk Assessment	FRM	Years since the most recent comprehensive inspection of the dam	Tier 2
Last EAP Revision	Capability	Information	Adapt	Planning Improvements	FRM	Years since the most recent revision to the emergency action plan (EAP)	Tier 2
Last EAP Exercise	Capability	Social	Adapt	Training Exercises	FRM	Years since the most recent EAP exercise	Tier 2
Worst Case Consequences Estimate	Capability	Physical	Absorb	Consequences of Failure	FRM	Estimated economic cost for the worst-case dam failure scenario (Maximum High Pool - Breach)	Tier 2
Operations Plans	Capability	Information	Absorb	Mitigation Planning	FRM	Degree (1-5) of completeness of operations plan	Tier 1
Planning Review	Capability	Information	Adapt	Planning Improvements	FRM	Years since the most recent review and update of the operations plans	Tier 2
Emergency Exercises	Capability	Social	Adapt	Training Exercises	FRM	Years since the most recent emergency operation test exercise (or most recent emergency response)	Tier 2
After-Action Reports	Capability	Information	Adapt	Post-disaster Data Collection	FRM	% of exercises/events in the past 5-10 years where an after-action report was generated and reviewed by the district	Tier 2

Solicitation Template



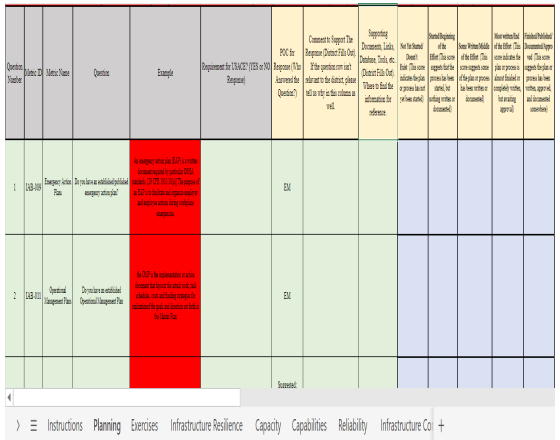
USACE Resilience Questionnaire

Interviewer: Garrett Walton/Luke Hogewood
Name:
Location:
Org.:
Position:
Date:

The following questionnaire is a supplemental document that will be used in tandem with the Resilience Matrix Metrics Playbook to assess the current resilience of USACE installations, projects, and assets. Please select only (1) answer per question. If a section does not apply to you or your position, you may skip the section; however, if you are able to accurately answer those questions, please do so.

Requirement/Redundancy/Sustainability

Function	0 days (completely dependent on outside resources)	1-2 days	3-7 days	8-14 days	More than 14 days (no dependence on outside resources)
How long can emergency operations be carried out using back-up generators/power if primary power is disrupted?	☐	☐	☐	☐	☐
How long can emergency personnel be sustained onsite using emergency life support (water, food) in the event of a disruption?	☐	☐	☐	☐	☐
How long can you maintain operations if supporting systems (power, communication, water) are disrupted or destroyed?	☐	☐	☐	☐	☐
How long would it take to return the data network to normal functionality after the given disaster?	☐	☐	☐	☐	☐
During recovery, how long can your temporary systems components that can take over operations of the primary system until the main system is back online last? (Grid-scale systems, manual ESs, etc.)	☐	☐	☐	☐	☐
How long can you sustain yourselves with a stockpile of supplies to sustain operations during an emergency (sandbags, bottled water, walkie-talkies, etc.)?	☐	☐	☐	☐	☐

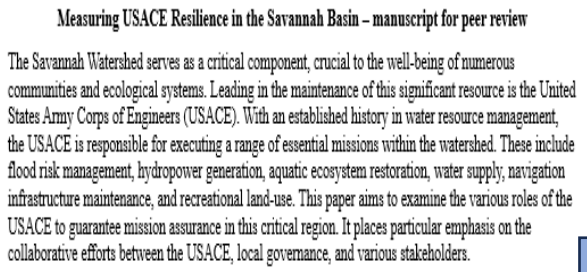


Instructions | Planning | Exercises | Infrastructure Resilience | Capacity | Capabilities | Reliability | Infrastructure Co

Scorecard

	Absorb	Recover	Adapt
Physical	3.8	5.0	3.5
Information	4.4	3.8	4.4
Social	3.7	5.0	5.0

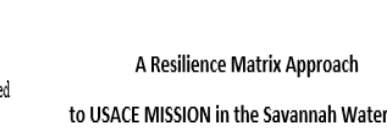
SRB-FRM Case Study



Measuring USACE Resilience in the Savannah Basin – manuscript for peer review

The Savannah Watershed serves as a critical component, crucial to the well-being of numerous communities and ecological systems. Leading in the maintenance of this significant resource is the United States Army Corps of Engineers (USACE). With an established history in water resource management, the USACE is responsible for executing a range of essential missions within the watershed. These include flood risk management, hydropower generation, aquatic ecosystem restoration, water supply, navigation infrastructure maintenance, and recreational land-use. This paper aims to examine the various roles of the USACE to guarantee mission assurance in this critical region. It places particular emphasis on the collaborative efforts between the USACE, local governance, and various stakeholders.

USACE Report



A Resilience Matrix Approach

to USACE MISSION in the Savannah Watershed

Academic Literature Review → Restructuring of Resilience Matrix → Development of Decision Support Tool → USACE Document Review → Development of Master Metrics → Development of Solicitation Survey → Development of Resilience Scorecard → Conducting/ Writing FRM Case Study → Compiling/ Writing Report on USACE Resilience →

Development of a documented/published methodology for a transferrable/replicable process that provides a cost effective and accurate procedure that can be used to assess USACE and Community Resilience from infrastructure, to critical function, to mission.

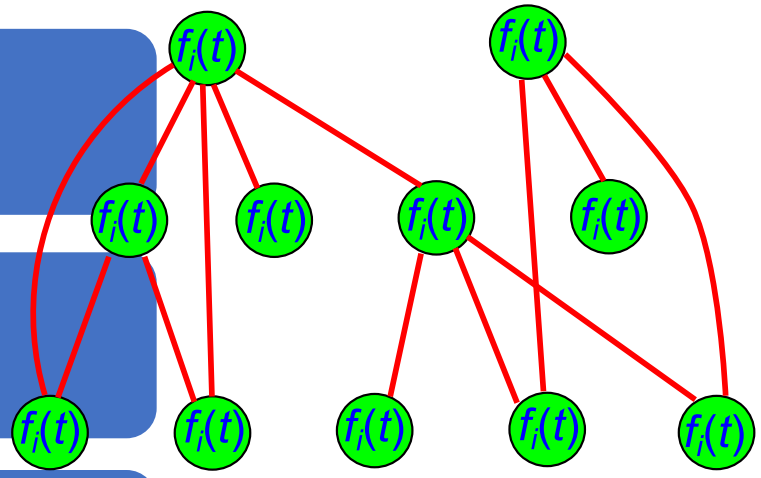
Network-based Resilience Theory?

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 ($\boldsymbol{E}$)

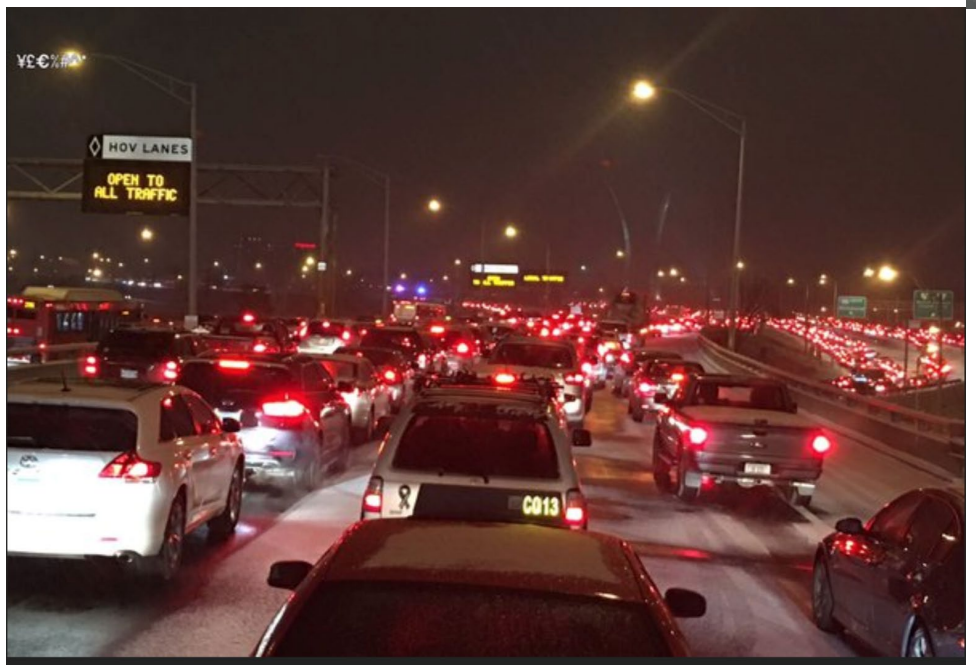


$$R = f(\mathcal{N}, \mathcal{L}, \mathcal{C}, \boldsymbol{E})$$

Poor Efficiency:

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

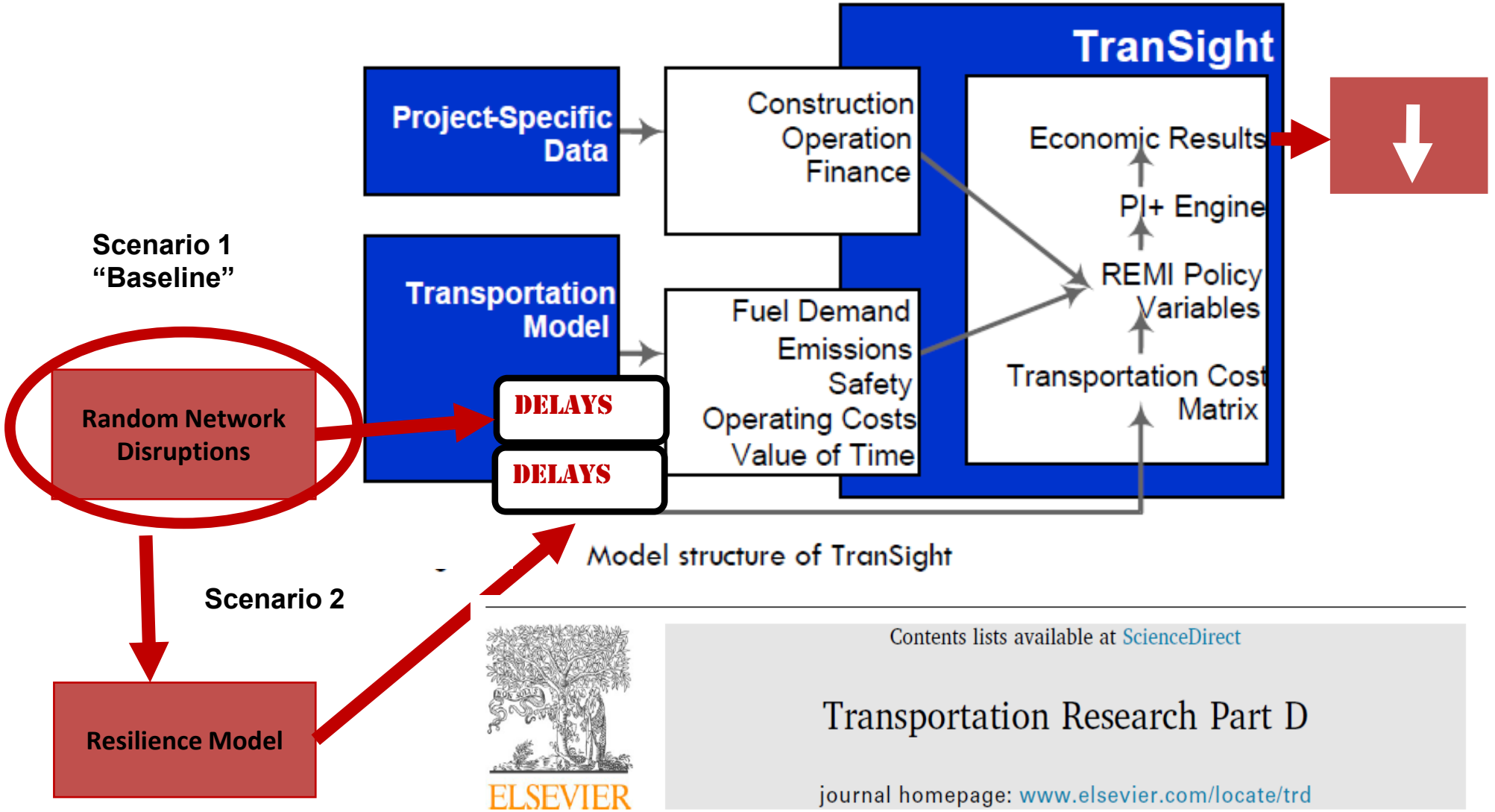
Traffic congestions are predictable and are typically of moderate level.



Lack of Resilience:

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

Traffic disruptions are not predictable and of variable scale.



Model structure of TranSight

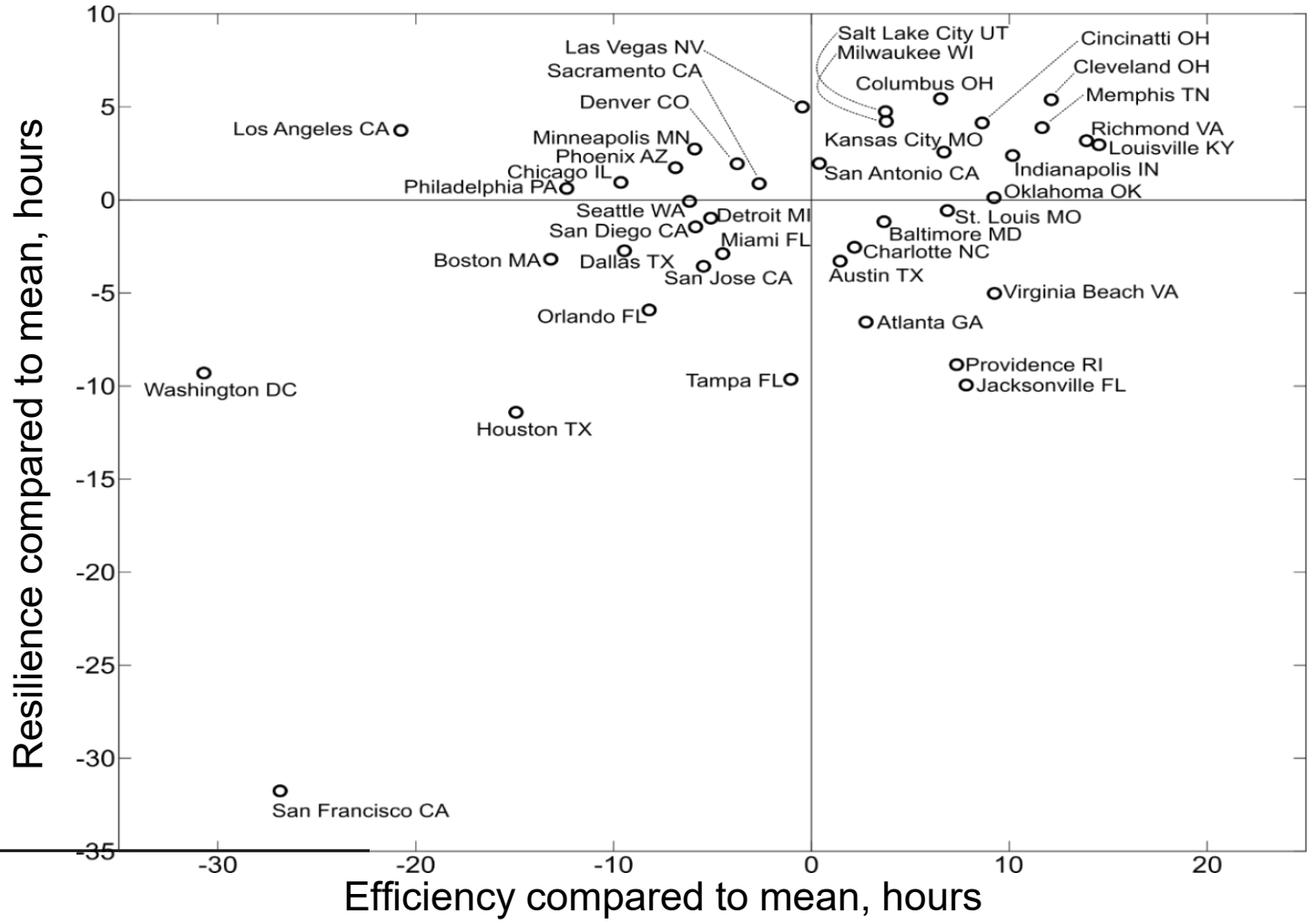
Contents lists available at ScienceDirect

Transportation Research Part D

journal homepage: www.elsevier.com/locate/trd

Lack of resilience in transportation networks: Economic implications

Resilience vs Efficiency at 5% disruption



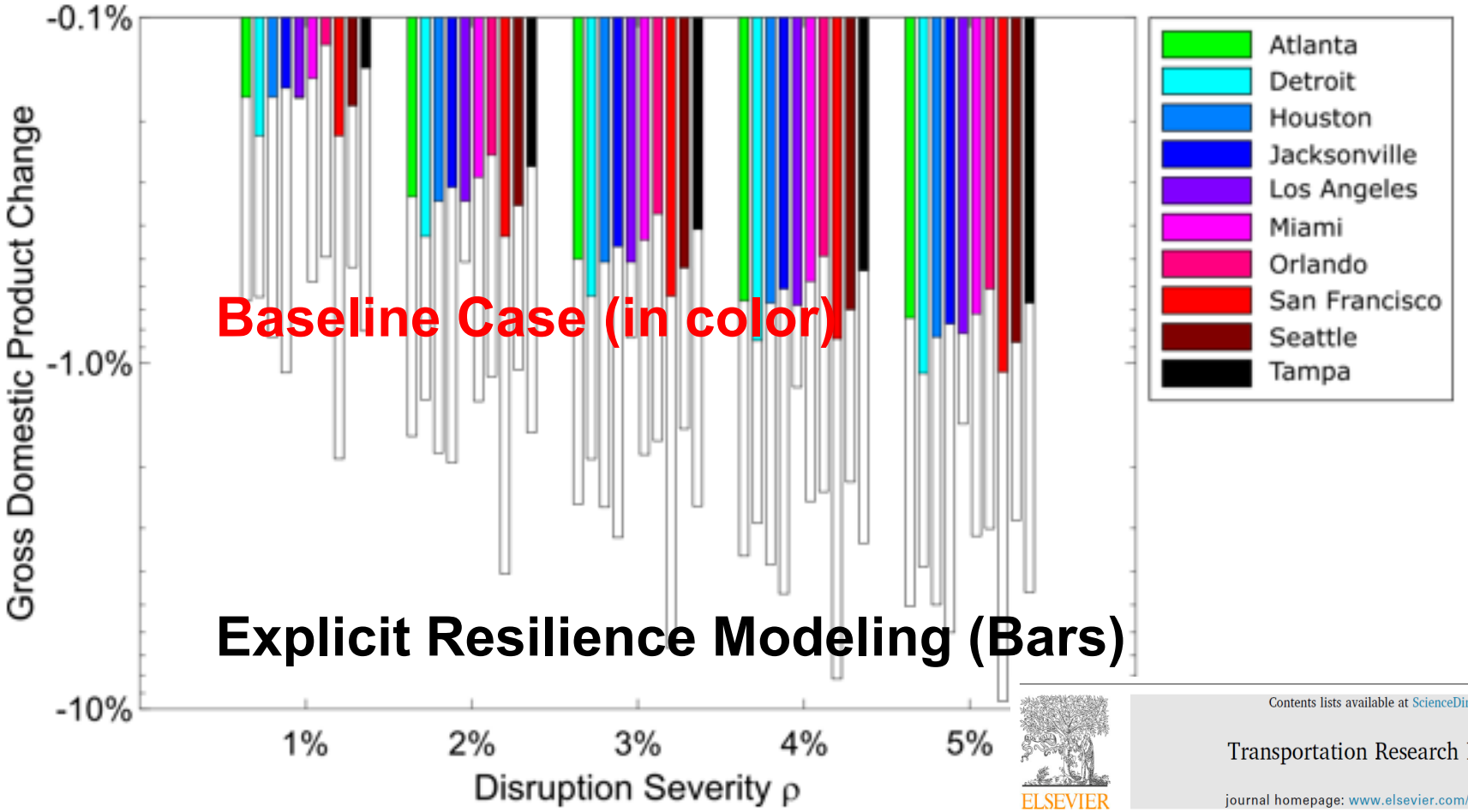
SCIENCE ADVANCES | RESEARCH ARTICLE

NETWORK SCIENCE 2017

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]*

Lack of Resilience: Impact on GDP

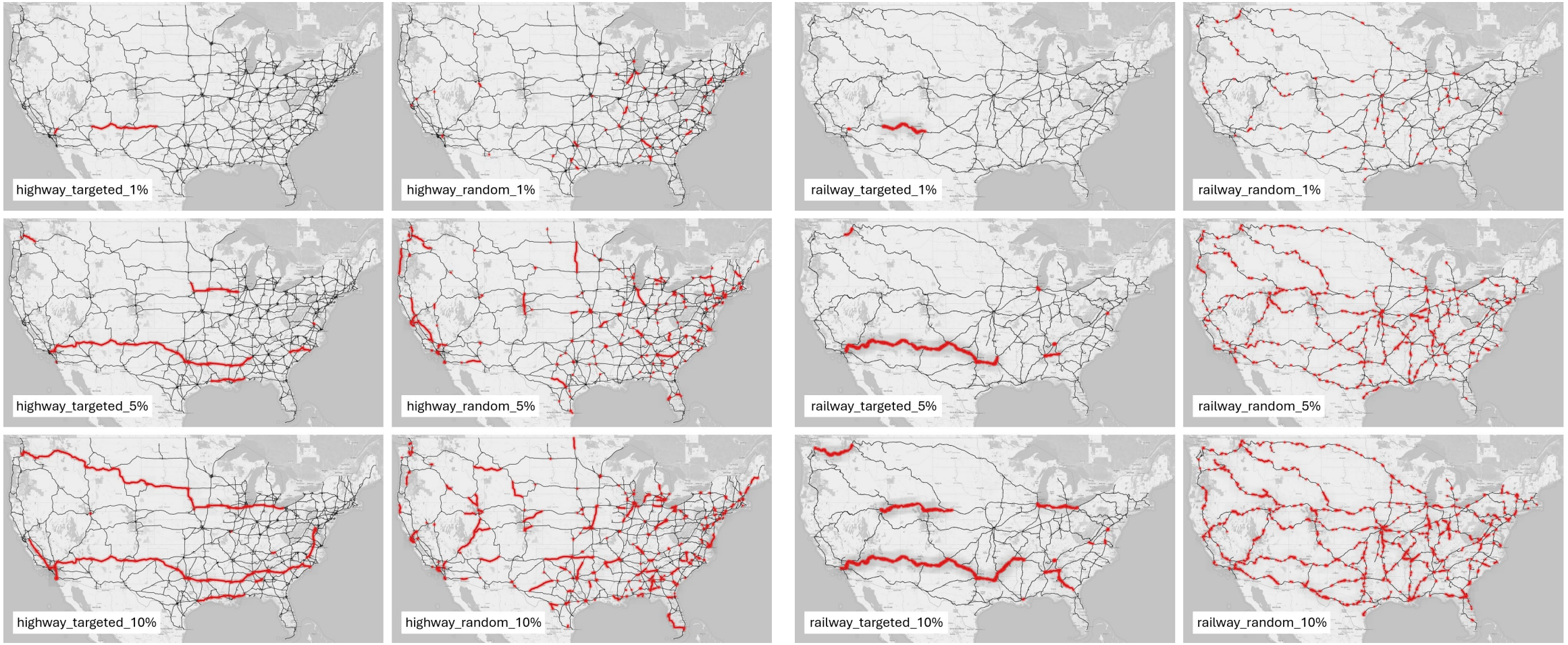


Contents lists available at ScienceDirect

Transportation Research Part D

journal homepage: www.elsevier.com/locate/trd

Lack of resilience in transportation networks: Economic implications



red

Chung (2024, submitted)

New York City Under Crisis: Which regions *lose* emergency services?

Transportation Research Interdisciplinary Perspectives
Volume 25, May 2024, 101111

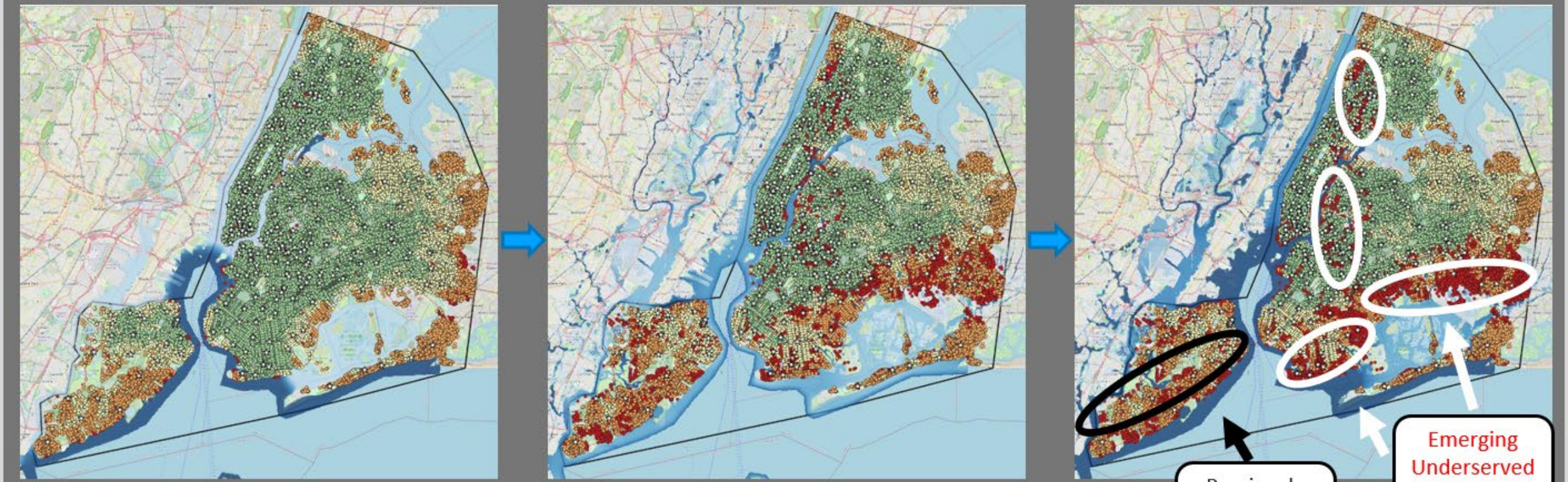
Access to Emergency Services: A New York City Case Study

Sukhwan Chung [a], Madison Smith [a], Andrew Jin [a], Luke Hogewood [a], Maksim Kitsak [b], Jeffrey Cegan [a], Igor Linkov [a]

Beginning of the Flood

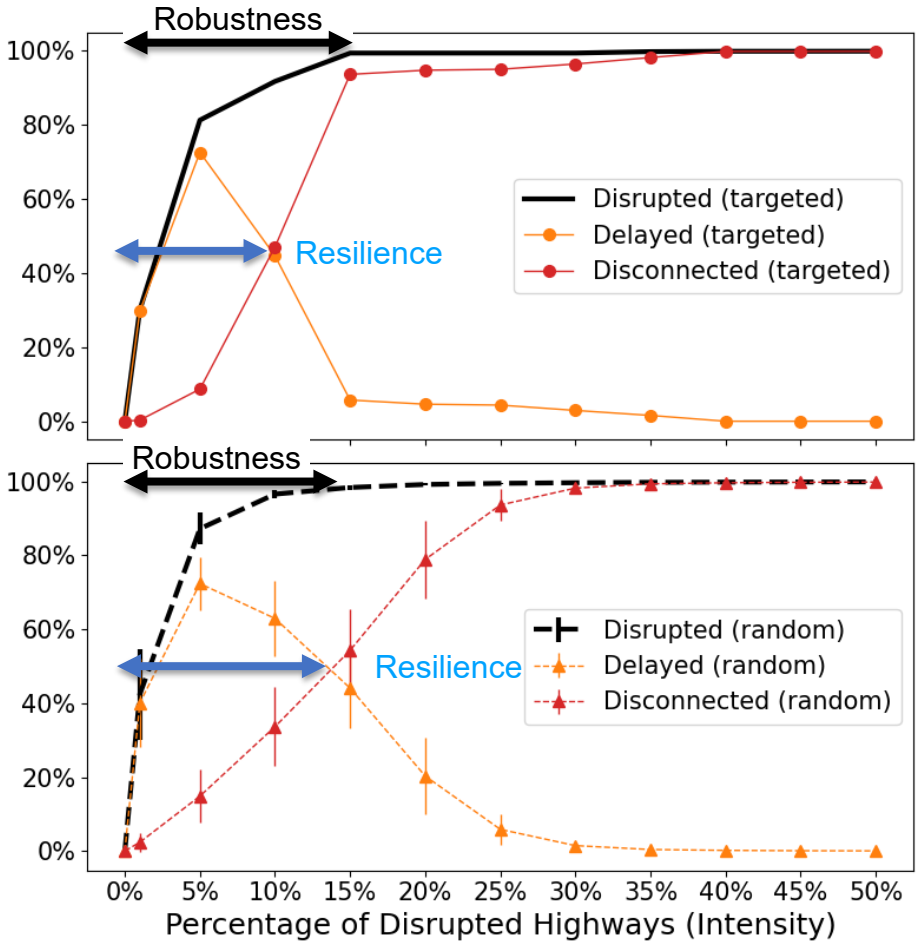
Intermediary Flood

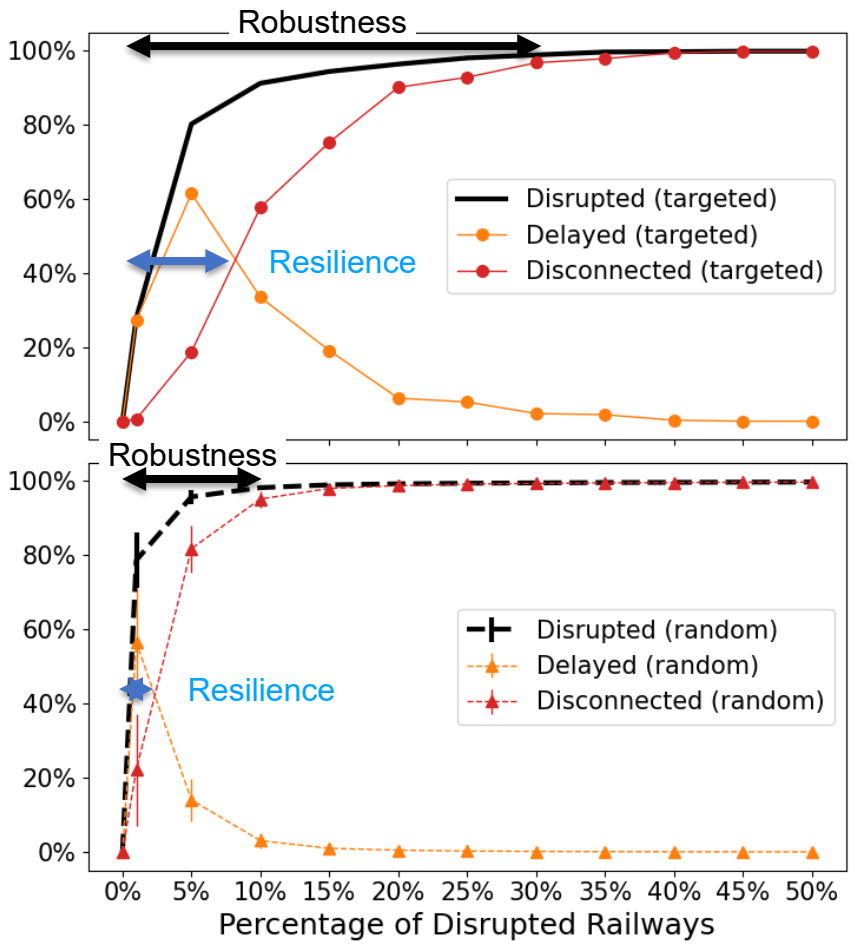
Peak of the Flood



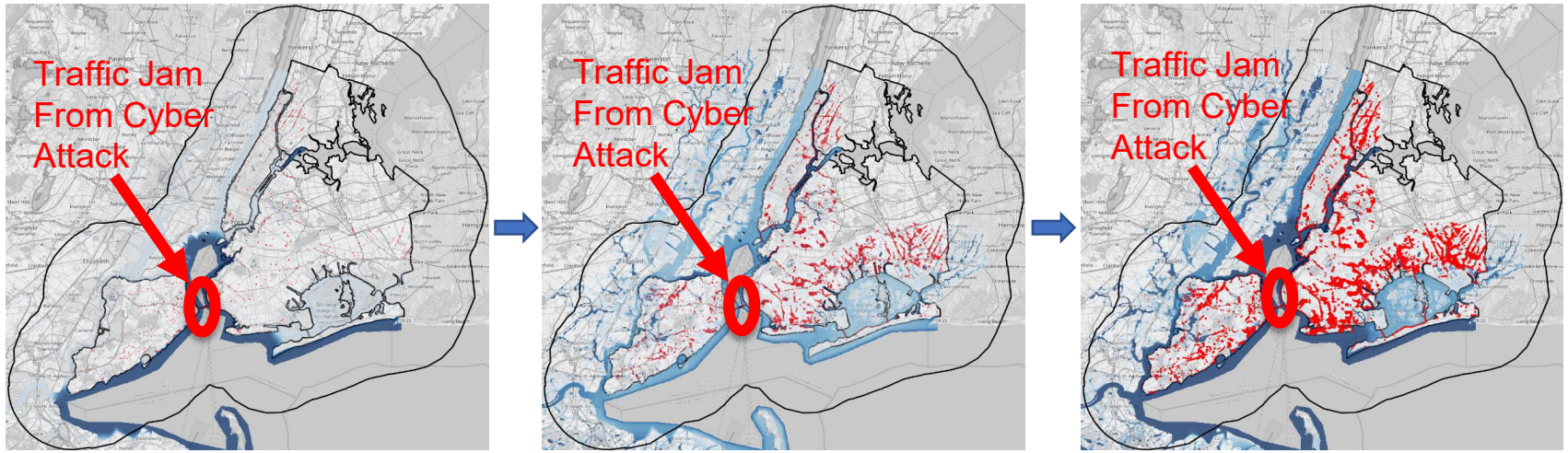
Green: Maximally Accessible
Yellow: Medium Accessible
Orange: Minimally Accessible
Red: No Access

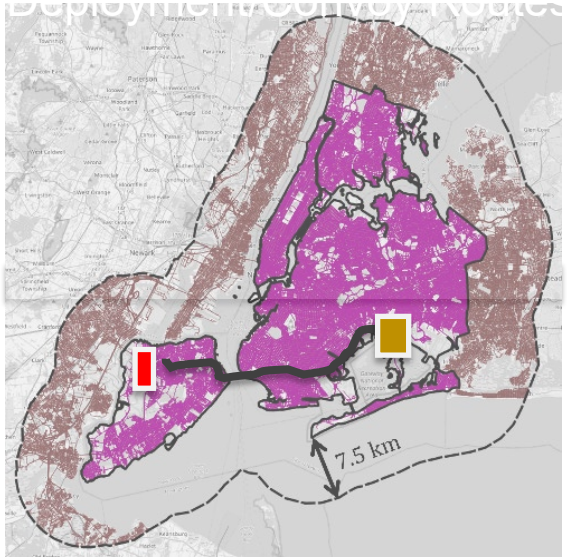
ERDC ENVIRONMENTAL LABORATORY





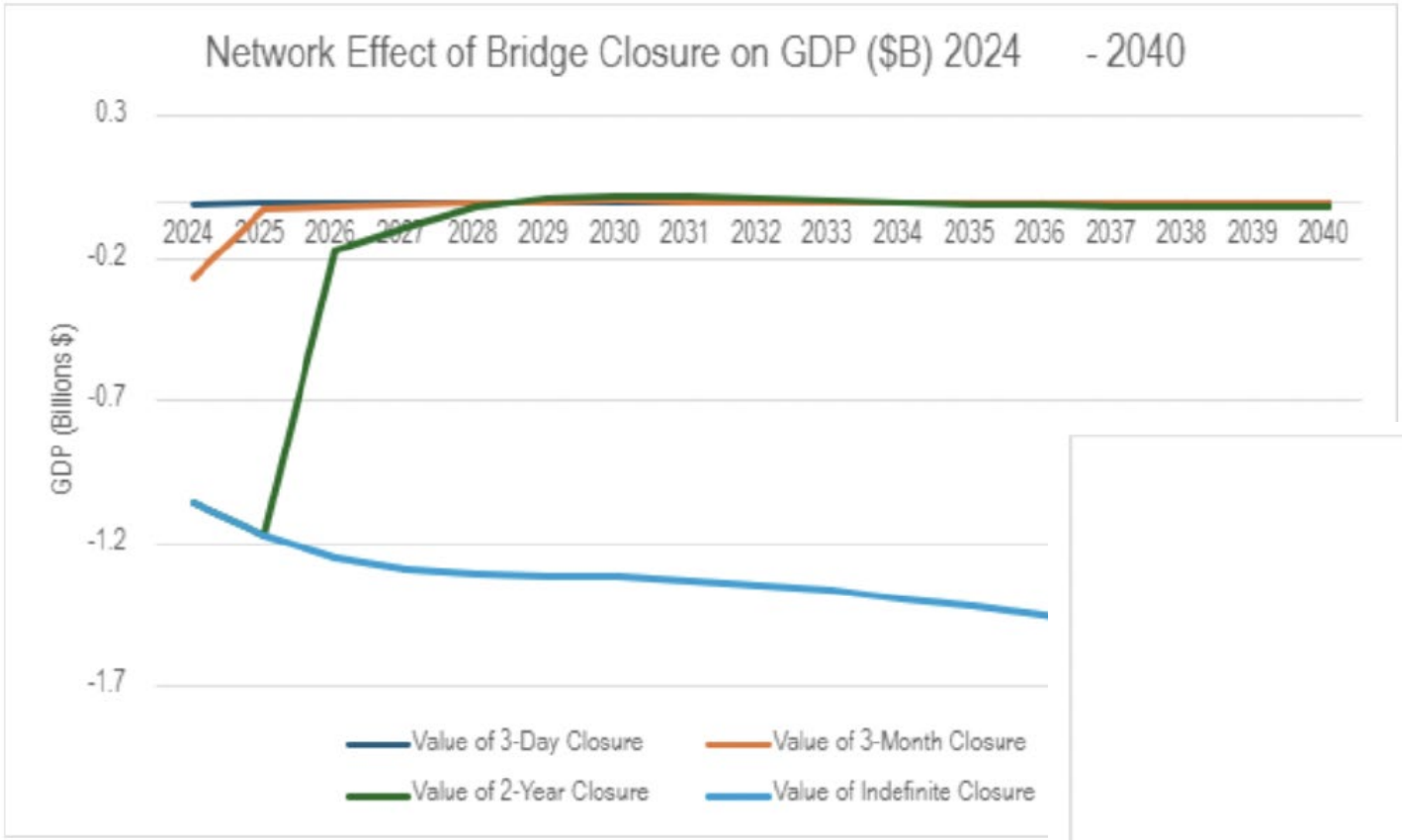
Chung (2024, submitted)





Military Base
Point of Entry
Convoy Route

Economics of Collapse: Baltimore Bridge or Port?



Treyz et al (2024, submitted)

Wildfire resilience projects

- Wildfires are an increasing threat to environments and human life

- The three aspects we address in our research are:
  - Preparedness
  - Response
  - Recovery

News | Climate Crisis

Thousands forced to evacuate as wildfires rage in western Turkey

Nearly 4,000 residents in the region have been moved to safety and six arrested for alleged sabotage, authorities said.

Madeira battles wildfire for fifth day

By **Reuters**

August 19, 2024 12:15 PM EDT · Updated 3 hours ago

'Exceptionally difficult': grueling wildfires test the resolve of US crews

Thousands of firefighters are deployed as an all time record for acres burned – and it's only August. Now some worry about the long months ahead

Network Separation with Quantum Computing

- **Background:**
- Fuel breaks are areas critical to wildfire preparedness and response

- **Approach:**
- Model forests as network of trees with edges created based on fire-spreading criteria

- Use D Wave quantum computing services to find best points in the tree network to separate groups (i.e., stop fire spread)

- **Project Aim:**
- Find fast and efficient ways to identify optimal areas to interrupt wildfire spread. Can rerun in real time as situation evolves.

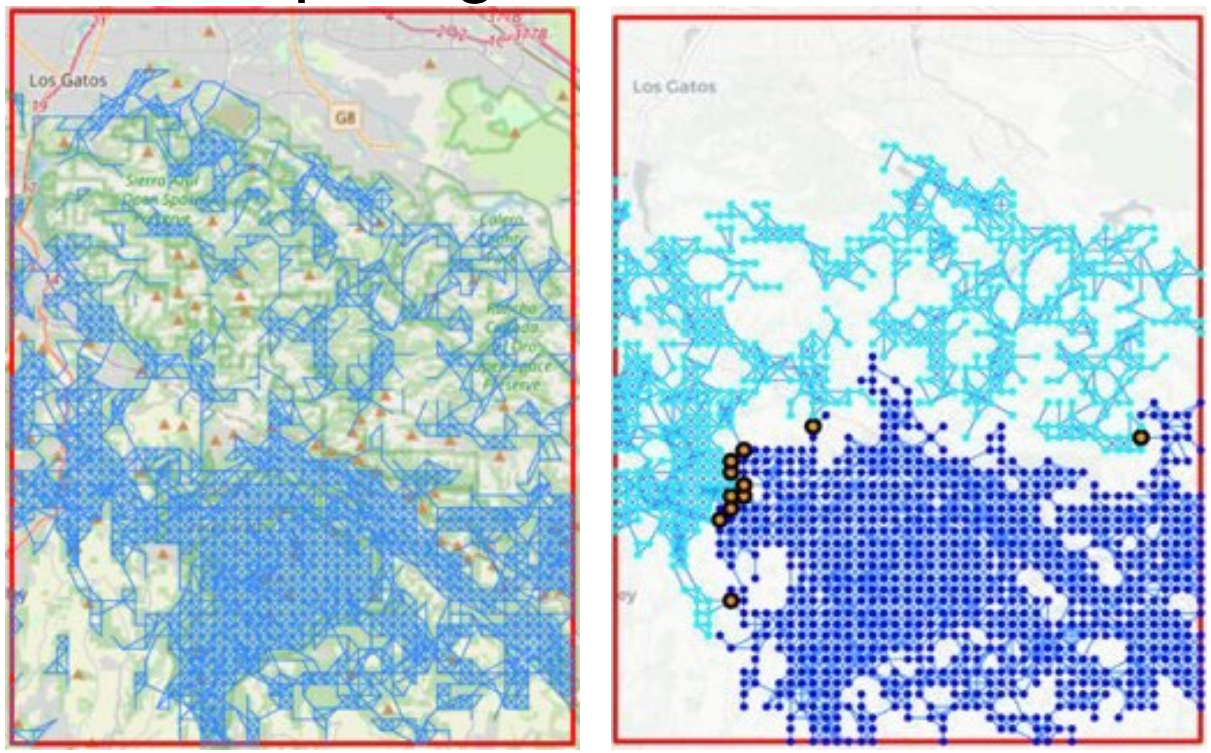
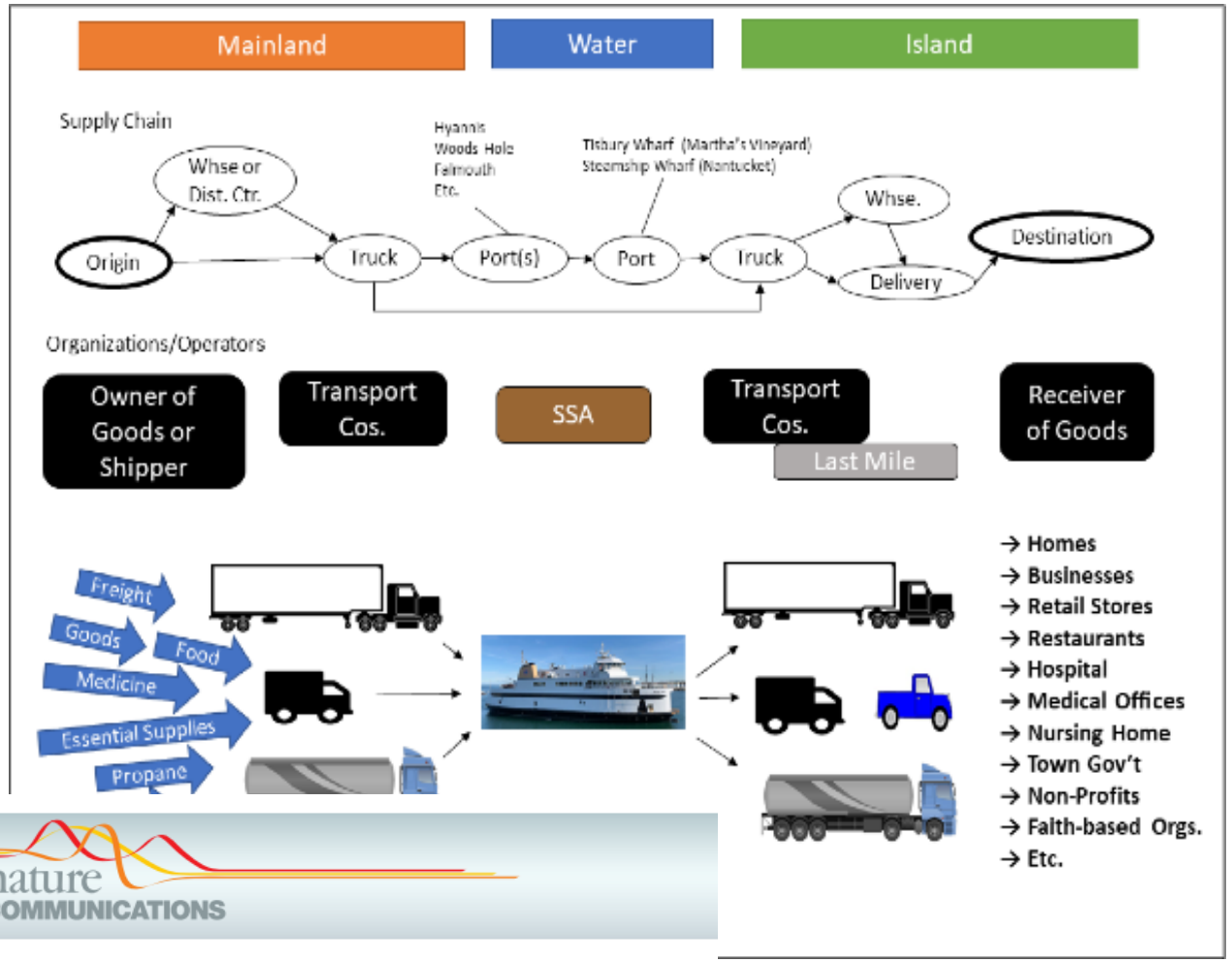
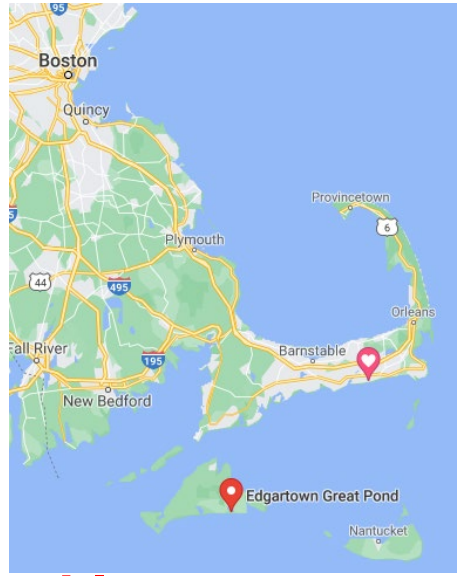


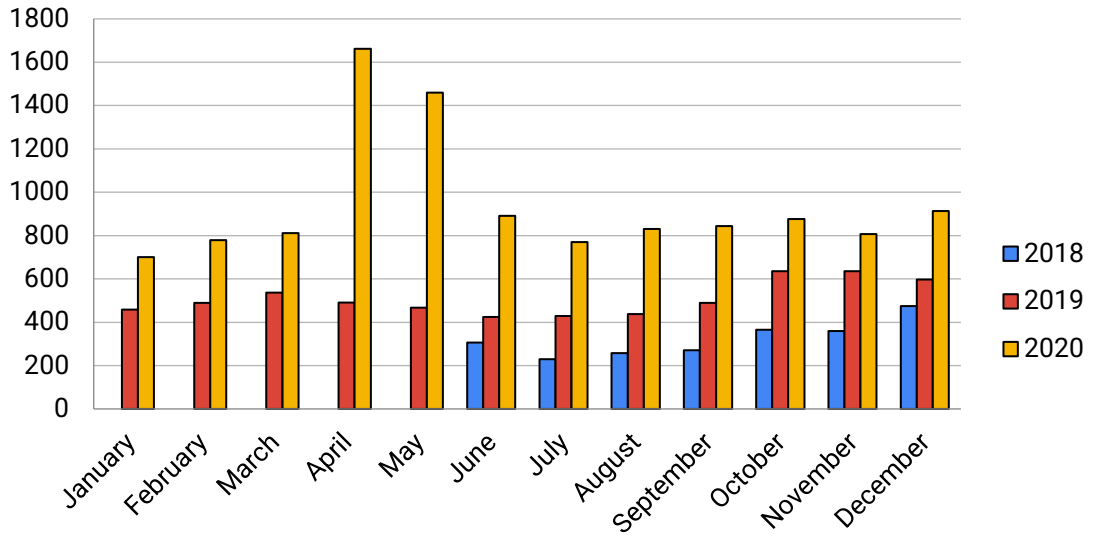
Figure 1: Forest network before and after network separation QC algorithm is run. Separator group is in orange on the right.

Food Availability and Supply Chains





Martha's Vineyard: Monthly Pantry Visits



nature COMMUNICATIONS

COMMENT

https://doi.org/10.1038/s41467-022-28734-6 OPEN

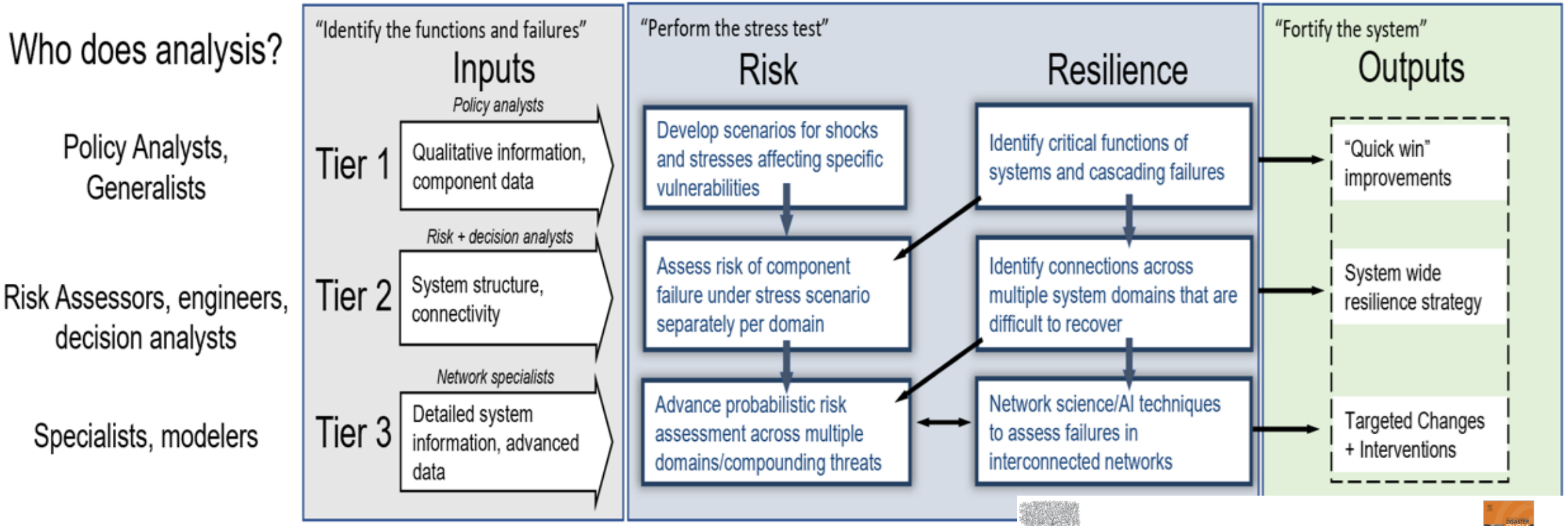
Resilience-by-Design and Resilience-by-Intervention in supply chains for remote and indigenous communities

Emerson Mahoney[1,2], Maureen Golan[2], Margaret Kurth[2], Benjamin D. Trump[2] & Igor Linkov[2]✉

Pronounced need ongoing in remote, austere, or island communities – example includes Tribal communities on Martha's Vineyard.

Integrated Risk/Resilience Stress Testing

How Do We Increase Resilience In Complex, Interconnected Infrastructure?



Three-Tiered Approach:

Tier 1: Define and identify more important critical functions & risks

Tier 2: Refine with interconnections, and define KPI

Tier 3: Asset-level data-driven analysis

ELSEVIER
International Journal of Disaster Risk Reduction
Volume 82, November 2022, 103323

Resilience stress testing for critical infrastructure

Igor Linkov [a b], Benjamin D. Trump [a c], Joshua Trump [d], Gianluca Pescaroli [e], William Hynes [f], Aleksandrina Mavrodieva [g h], Abhilash Panda [h i]

Artificial Intelligence and Resilience Analytics

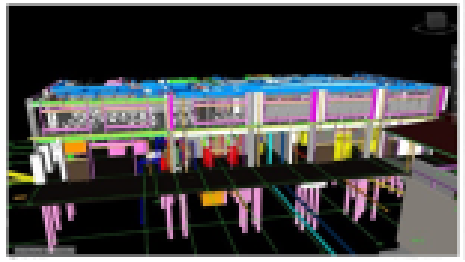
Artificial Intelligence and Machine Learning can incorporate data to create a Systems of Systems approach to better understanding of resilience complex systems.

Descriptive Analytics
What happened?

Diagnostic Analytics
Why did it happen?

Predictive Analytics
What will happen next?

Prescriptive Analytics
What should we do about it?



Digital Twin

Resilient AI

Insights into Resilient Systems

CYBERTRUST

COMPUTER 0018-9162/20©2020IEEE

PUBLISHED BY THE IEEE COMPUTER SOCIETY SEPTEMBER 2020

Cybertrust: From Explainable to Actionable and Interpretable Artificial Intelligence

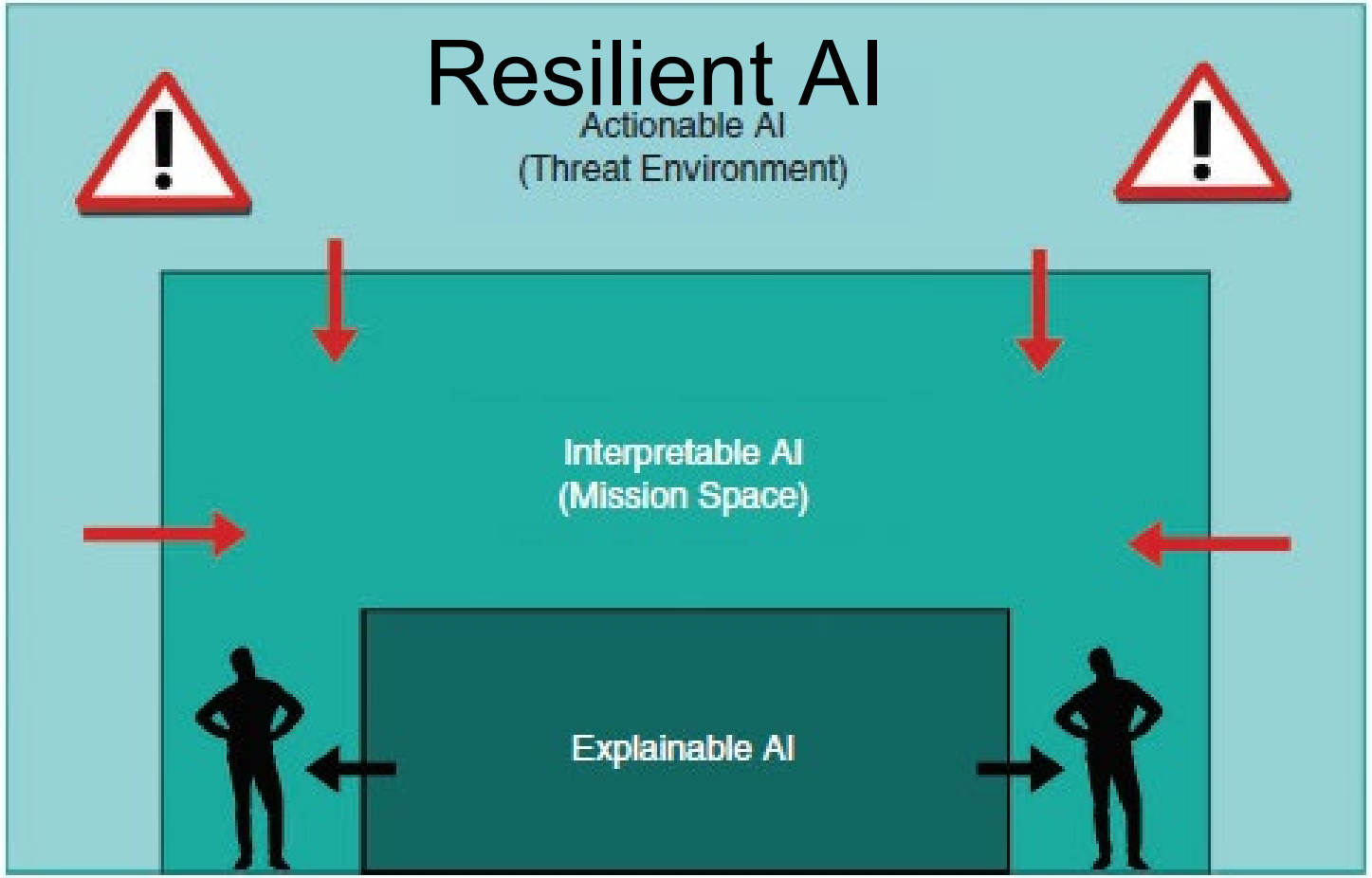
Igor Linkov, Stephanie Galaitsi, and Benjamin D. Trump, U.S. Army Corps of Engineers

Jeffrey M. Keisler, University of Massachusetts

Alexander Kott, U.S. Army Futures Command

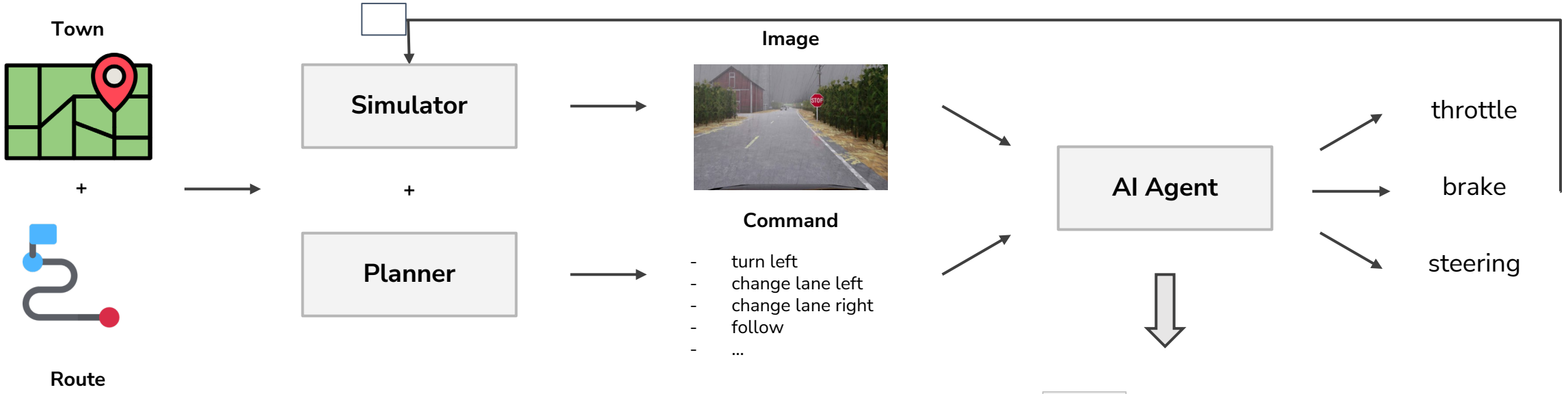
TABLE 1. The typology of human–AI assessments of decision strategy.

		AI	
		Yes	No
Human	Yes	Agreement	Disagreement
	No	Disagreement	Agreement



Resilient AI

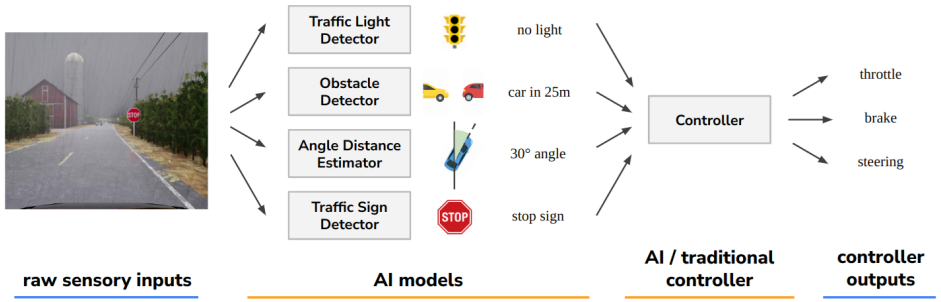
σ_{sim}	σ_{image}	σ_{agent}	$\sigma_{controller}$
- add/remove objects - change properties - change weather	- blur & saturation - color - Lp-norm, ISO, noise	possible but not required now	- amplification - dampening - noise



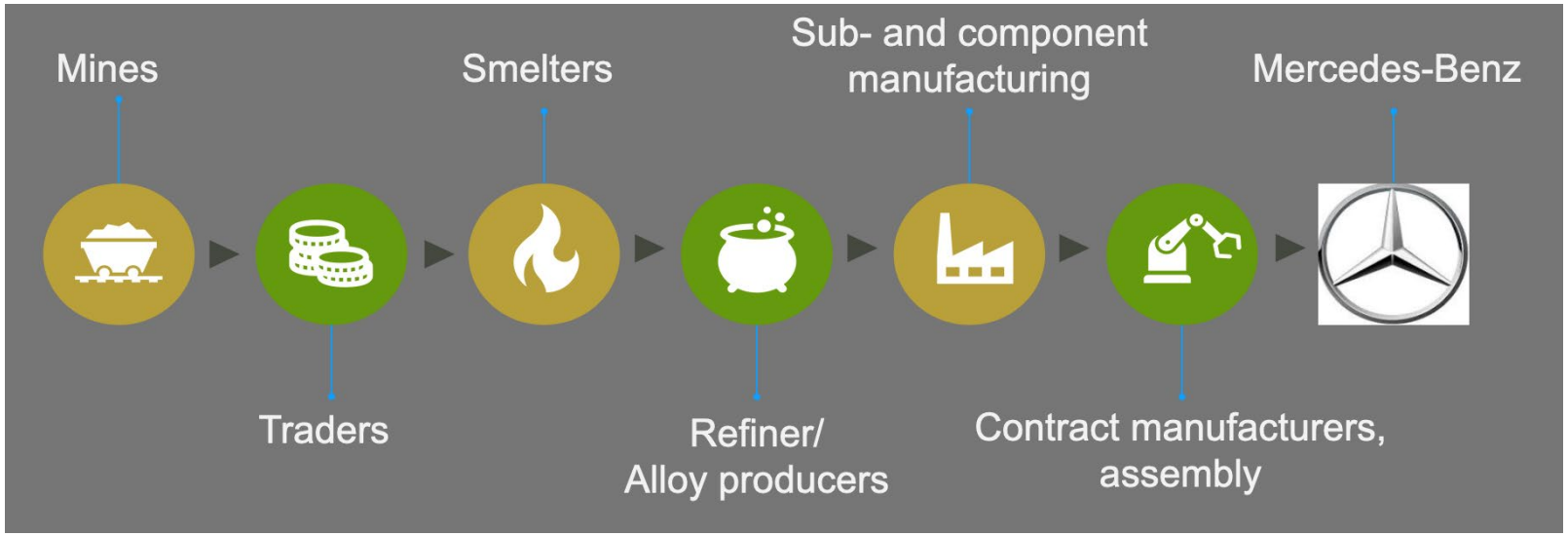
Disruption → image noise, image rotations, stickers, ...

Efficiency → **"driving performance"** System level property

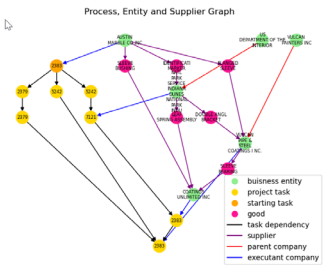
Resilience → change in **"driving performance"** relative to disruptions

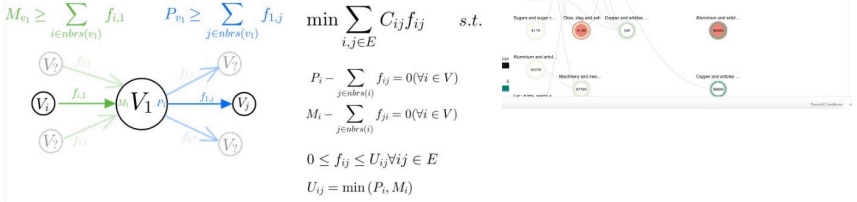


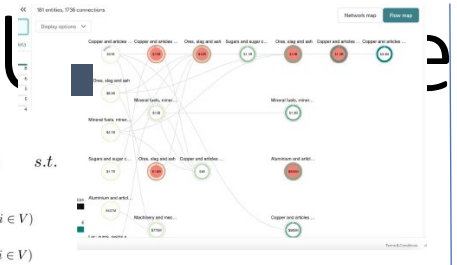
39

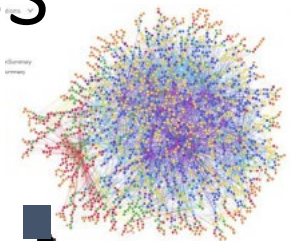

Mines
Traders
Smelters
Refiner/
Alloy producers
Sub- and component
manufacturing
Contract manufacturers,
assembly
Mercedes-Benz

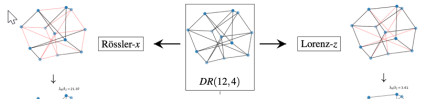
.PA RSDN U ess

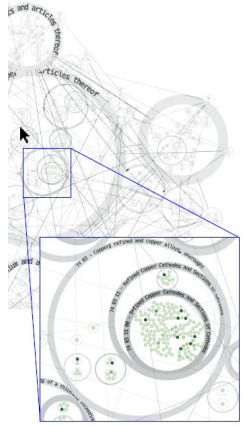








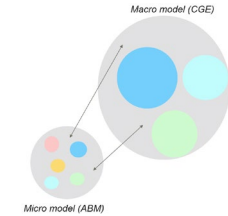


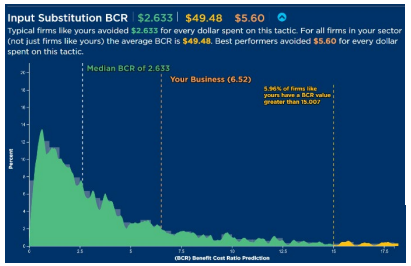


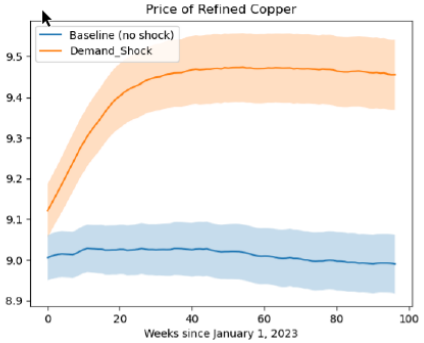
- **What do I need to know about the supply chain?** – Focus on data that is really needed (hypothesis)
- **How can I fill gaps?**
  - **Find data** - Web scraping, ML & AI, flow imputation
  - **Extract tiers –** Hierarchy algorithms
  - **Clean data** - Align entities

- **How does my supply chain look & behave?** - Intuitive user interface & powerful analytics
  - **Where is risk and resilience?** - Analyze & quantify for system and components
  - **Where does my copper come from?** - Explore and group entities, links, characteristics; create scenarios

- **What is going to happen?** - Link macro & micro to model network behavior
  - **What will happen if there's an earthquake in Chile?** - *Forward* stress-testing
  - **What might cause me to not have enough copper for munitions?** - *Reverse* stress-testing
  - **What if Chile stops producing copper?** - Test counterfactuals
  - **What if I stockpile copper?** - Analyze mitigation strategies
  - **How certain am I?** - Quantify uncertainty





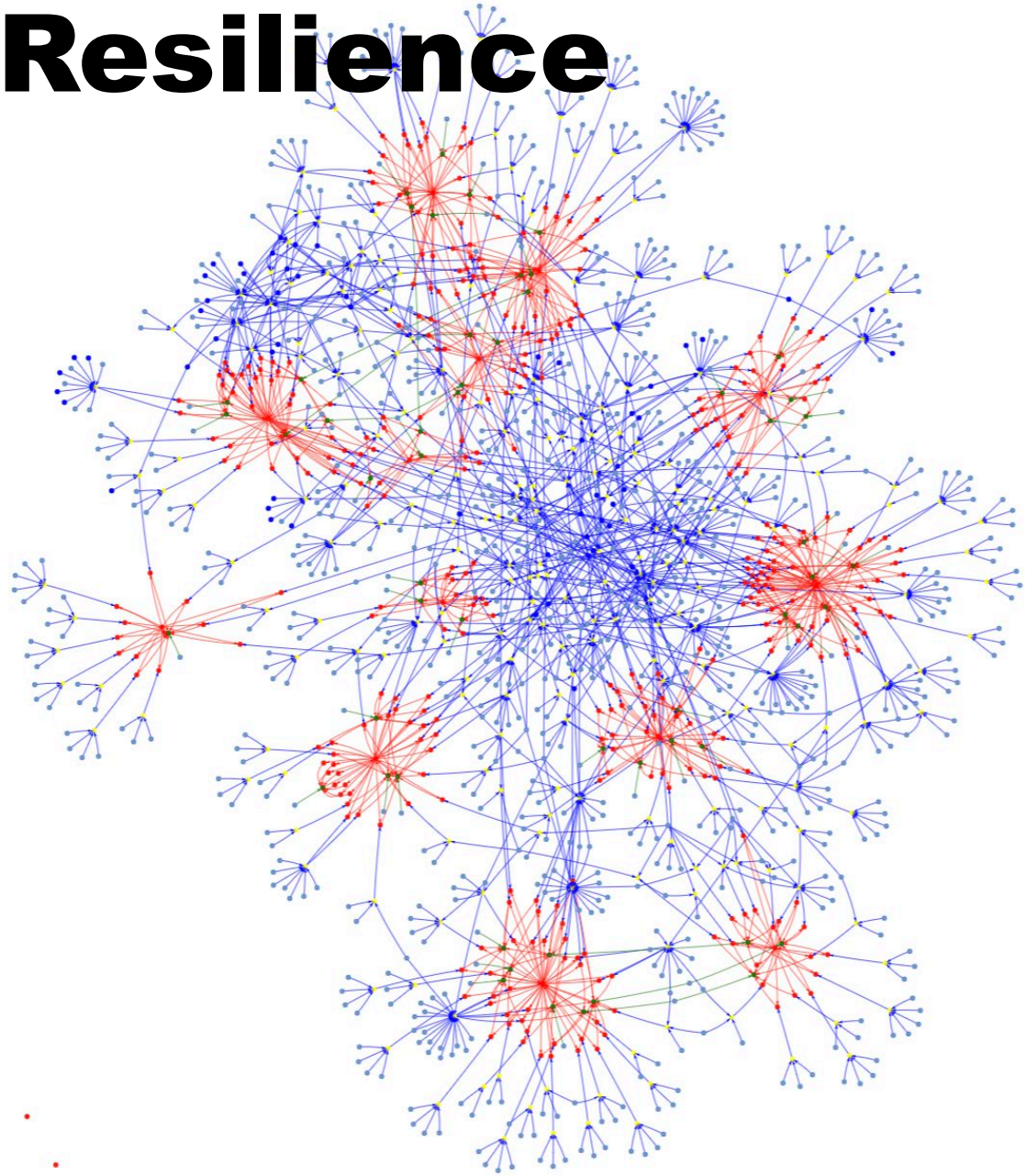


Generative AI and Resilience

DARPA surrogate data to build supply demand network

Synthetic, plausible supply chain:

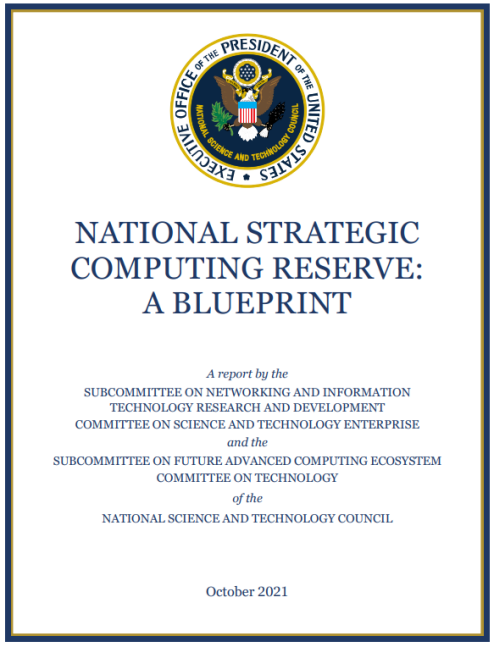
- Current DARPA surrogate SDN is limited in scope
- Leveraged *LLMs* to build out SDNs
- Demonstrates how LLMs can be used for imputation when data is unavailable



Cyber Resilience by Design or by Intervention?

Alexander Kott, U.S. Army DEVCOM Army Research Laborat
Maureen S. Golan, U.S. Engineer Research and Developmen Credere Associates
Benjamin D. Trump, U.S. Engineer Research and Developme University of Michigan
Igor Linkov, U.S. Engineer Research and Development Cente Carnegie Mellon University

	Risk management	RBD	RBI
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 the context of societal needs; there may be a constellation of networks across systems
Consequence	Vulnerable nodes and/or links fail as a result of a threat	Degradation of critical functions in time and capacity to achieve system's function	Degradation of the critical societal function due to cascading failure in interconnected networks
Actor	Either internal or external to the system	Internal to the system	Ext
Corrective action	Either loosely or tightly integrated with the system	Tightly integrated with the system	Loc
Stages/ analytics	Prepare and absorb (the risk is a product of a 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)	Pre (ex to r soc the



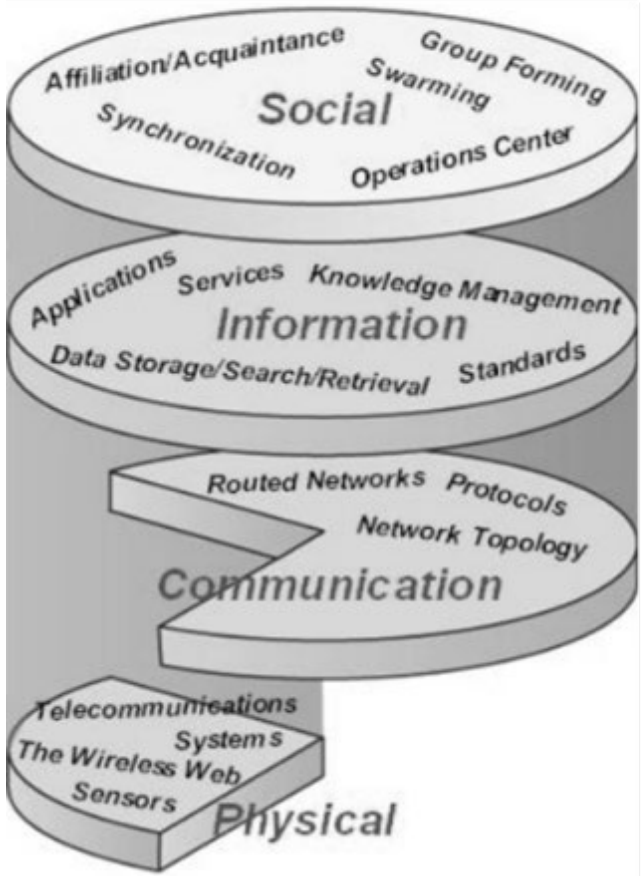
NATIONAL STRATEGIC COMPUTING RESERVE: A BLUEPRINT

A report by the
SUBCOMMITTEE ON NETWORKING AND INFORMATION TECHNOLOGY RESEARCH AND DEVELOPMENT
COMMITTEE ON SCIENCE AND TECHNOLOGY ENTERPRISE
and the
SUBCOMMITTEE ON FUTURE ADVANCED COMPUTING ECOSYSTEM
COMMITTEE ON TECHNOLOGY
of the
NATIONAL SCIENCE AND TECHNOLOGY COUNCIL

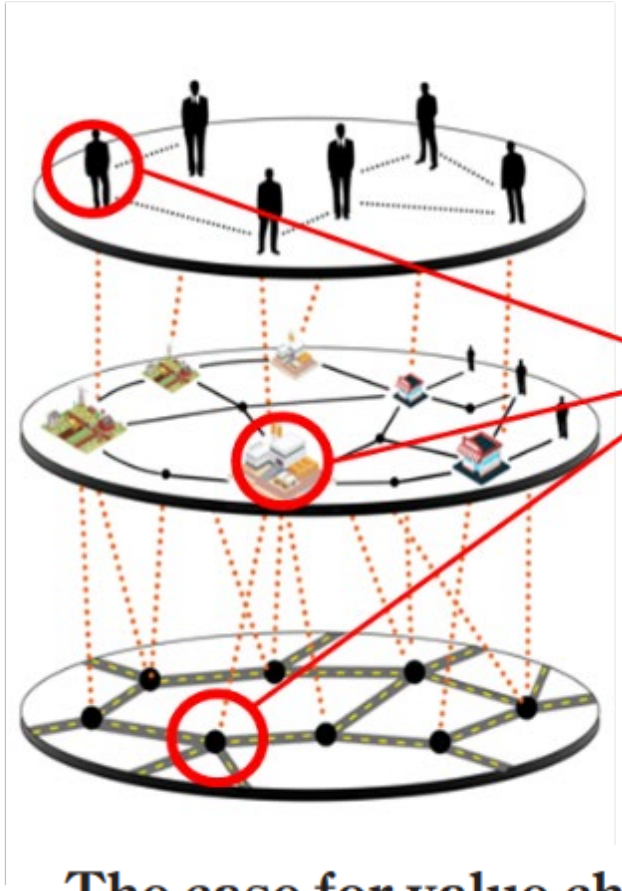
October 2021

Vision for System Resilience

Real World



Model



Operations

Management Alternatives

The case for value chain resilience

Igor Linkov, Savina Carluccio, Oliver Pritchard, Áine Ní Bhreasail, Stephanie Galaitsi, Joseph Sarkis and Jeffrey M. Keisler

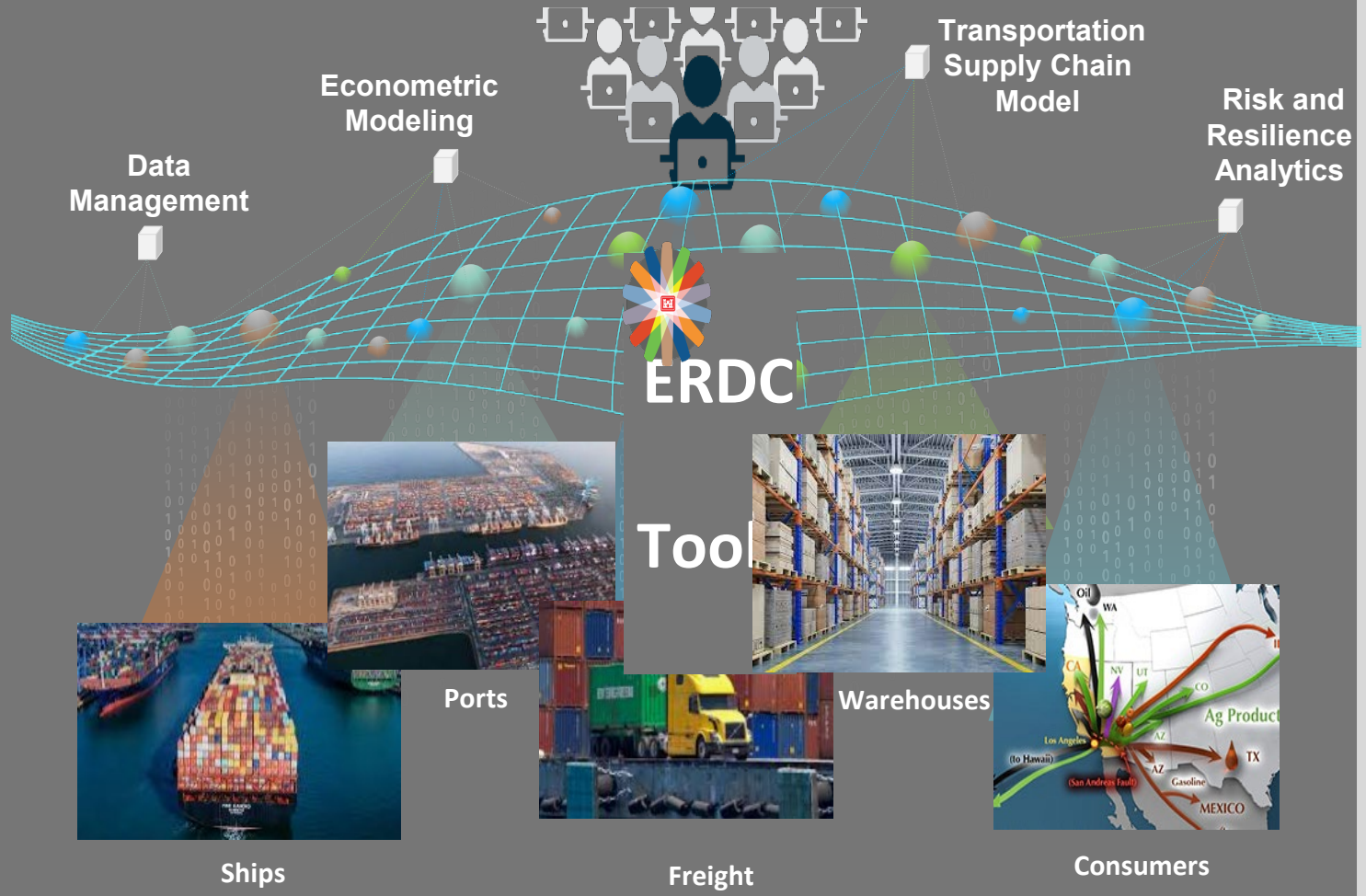
Management Research Review

2040-8269
DOI 10.1108/MRR-08-2019-0353

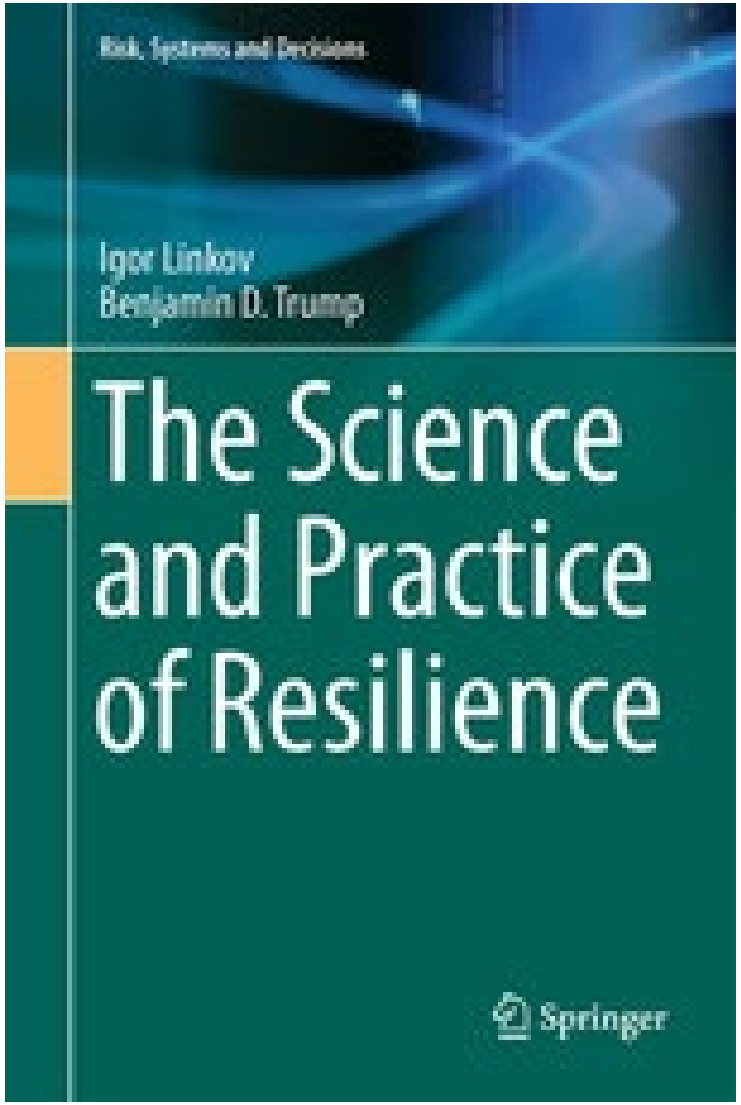
Approach:
Increase Resilience Through Networks + Analytics

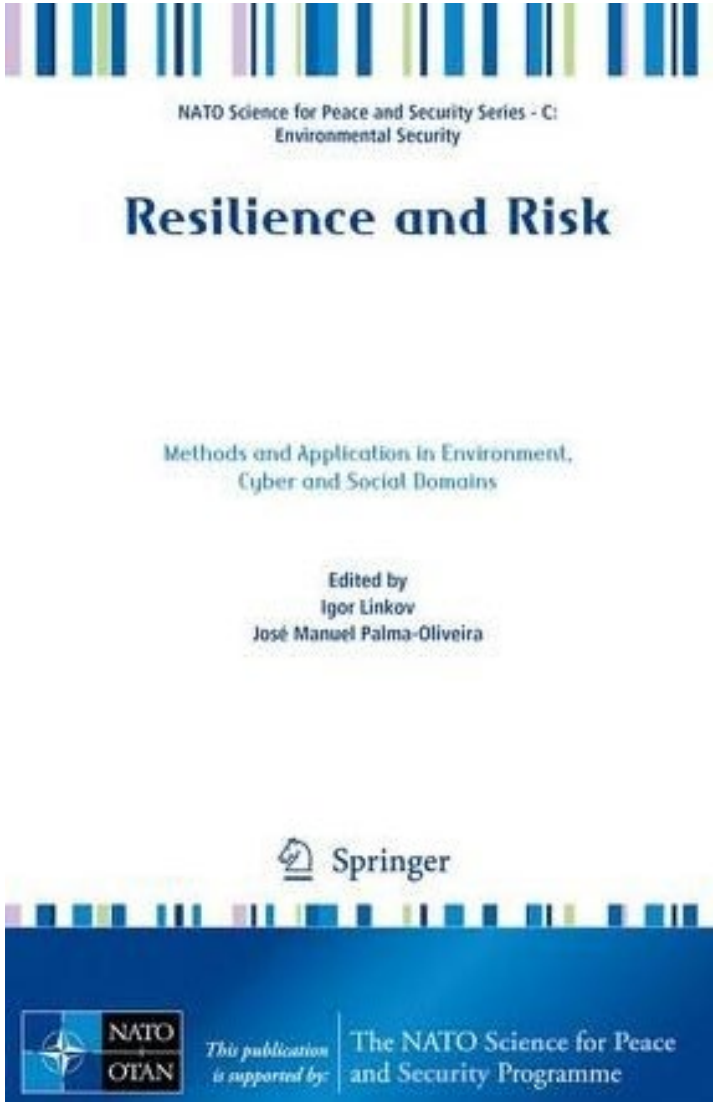
- **Motivations of Approach:**
  - Infrastructure is a large, interconnected systems
  - Limiting factors are non-obvious
  - Traditional approaches to comparing projects may not account for these factors

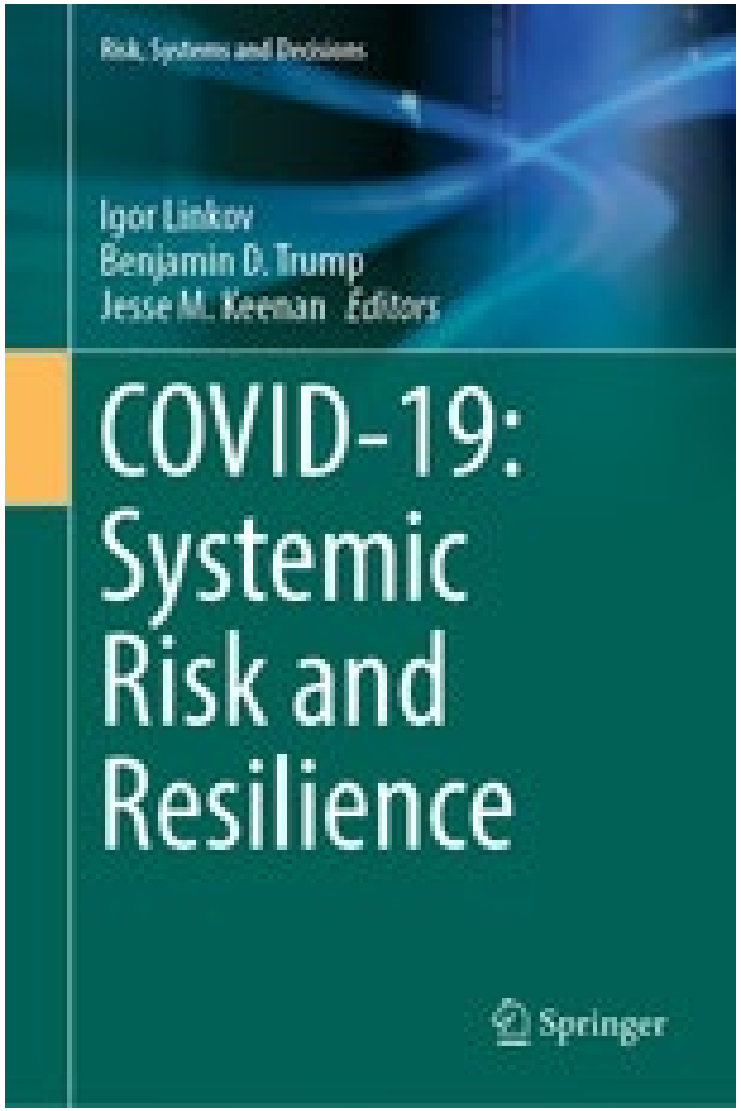
- **Technical Approach:**
  - Network-based, system-level approach
  - Combine with meaningful analytics
  - Relevant to government users



ENVIRONMENTAL LABORATORY


Risk, Systems and Decisions
Igor Linkov
Benjamin D. Trump
The Science and Practice of Resilience
Springer


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
Igor Linkov
Benjamin D. Trump
Jesse M. Keenan Editors
COVID-19: Systemic Risk and Resilience
Springer