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

Resilience Quantification for Cross-agency Disaster Response

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

8 December 2024

Action:

- Submit 1page Vision Statement on Resilience Quantification to evidence@omb.eop.gov and CC to Igor.Linkov@usace.army.mil by 12/20/2024

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

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, tł 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

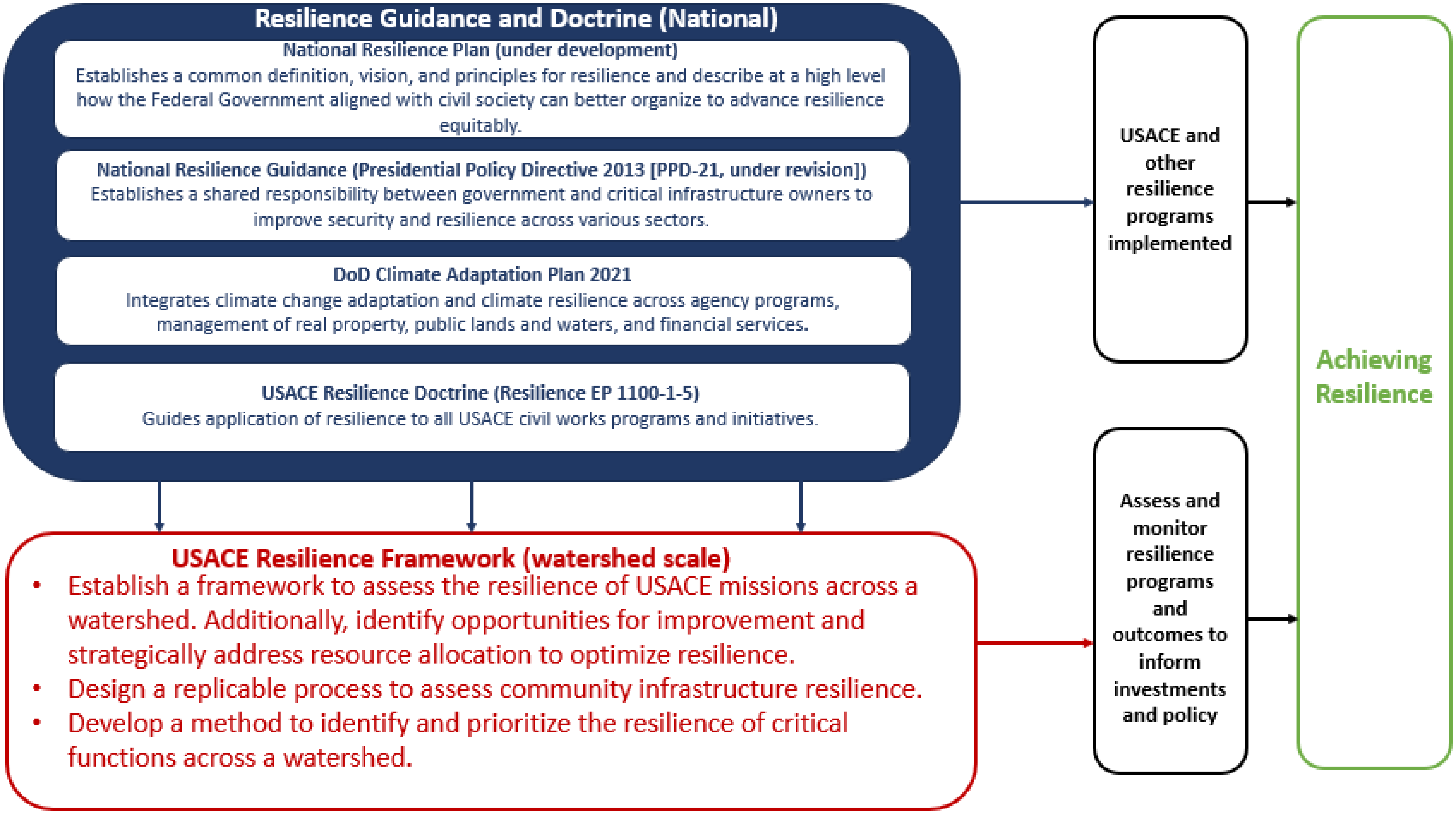
Office of the Press Secretary

For Immediate Release May 11, 2017

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

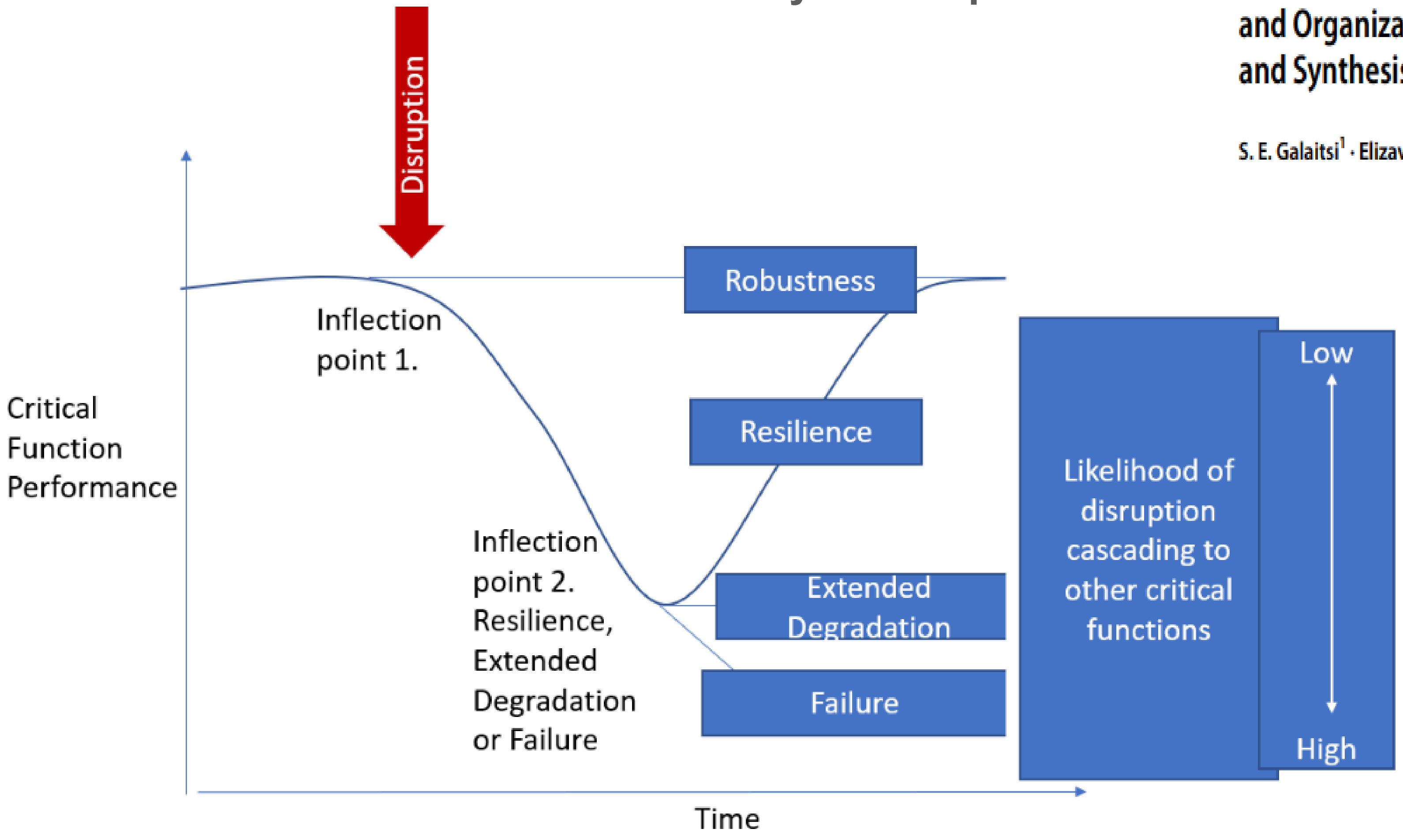
EXECUTIVE ORDER

Resilience at the National Scale (USACE example)



Crisis Management, Risk and Resilience

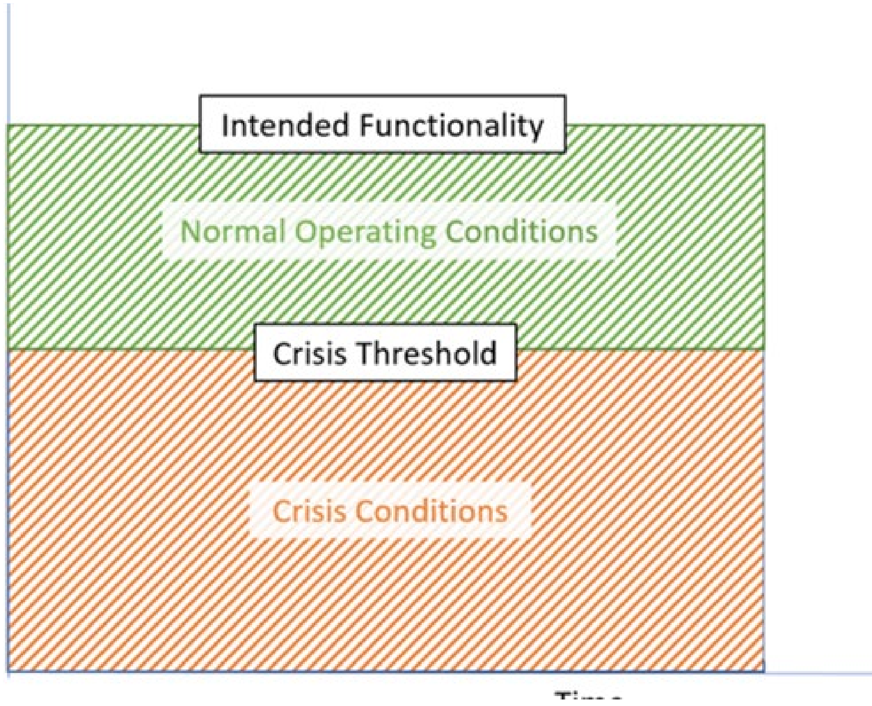
Risk~ Threat*Vulnerability*Consequence



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

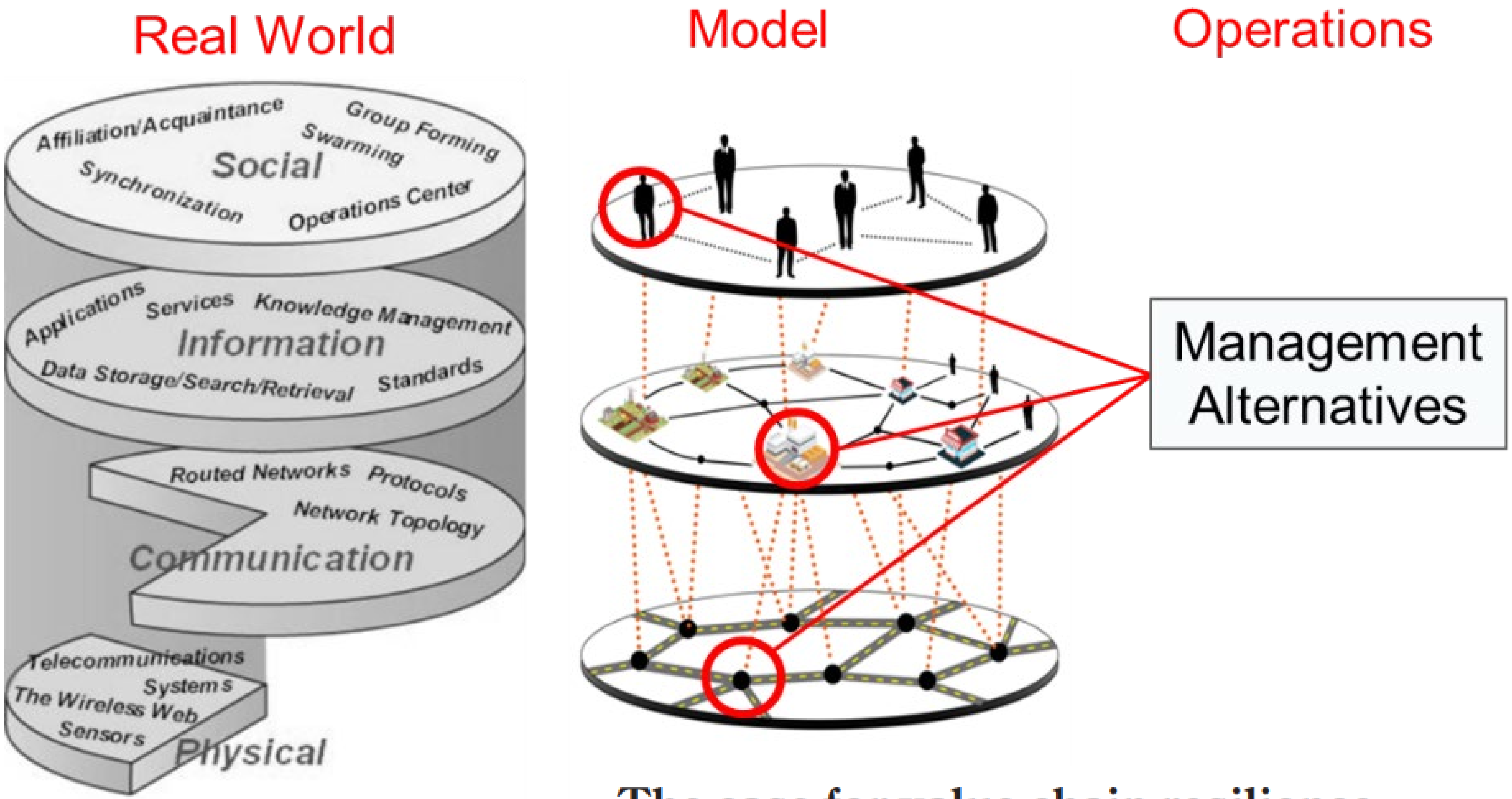
Business Continuity Management, Operational Resilience, and Organizational Resilience: Commonalities, Distinctions, and Synthesis

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

Vision for System Resilience



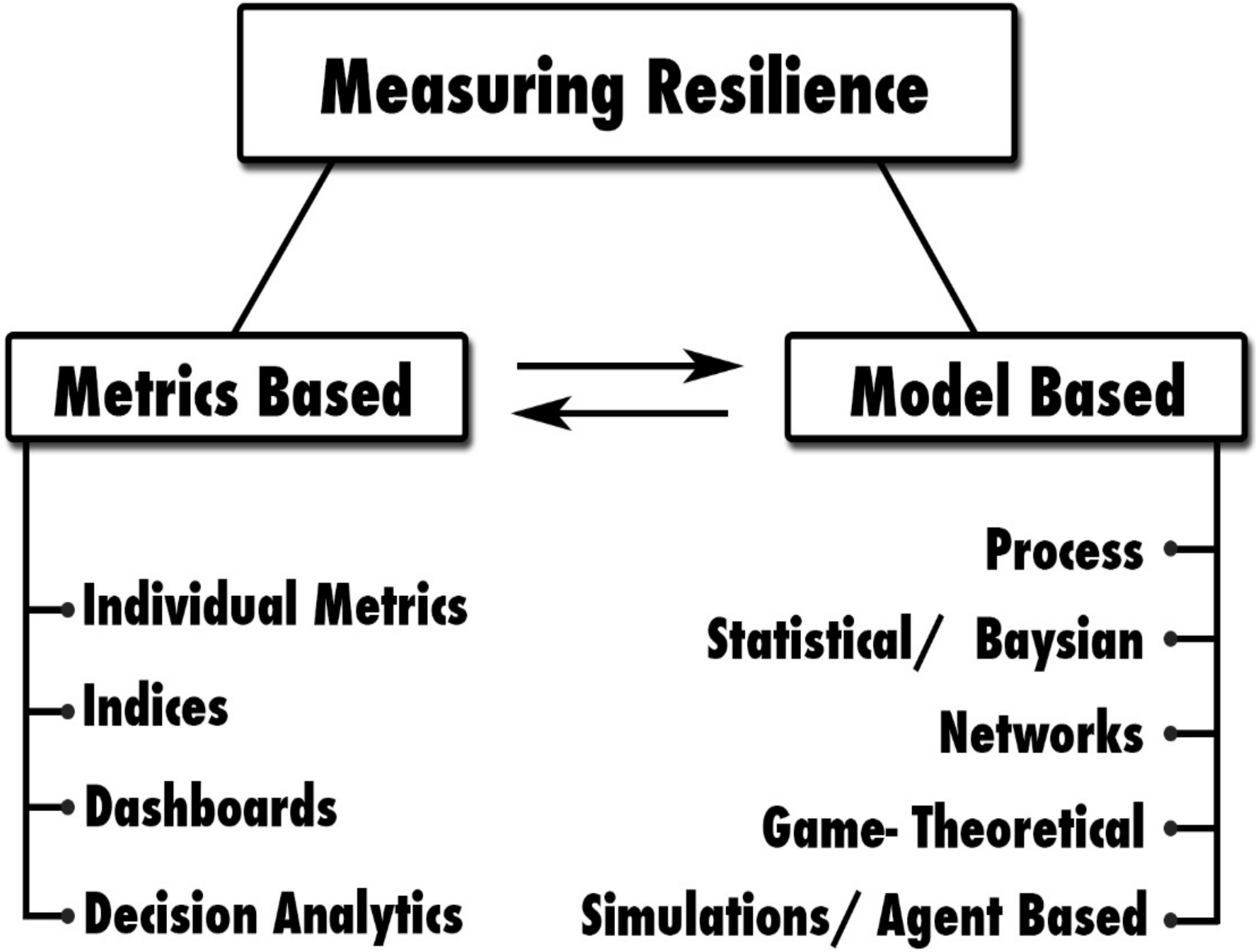
The case for value chain resilience

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

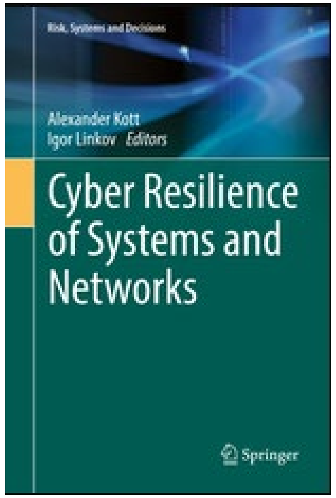
Management Research Review

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

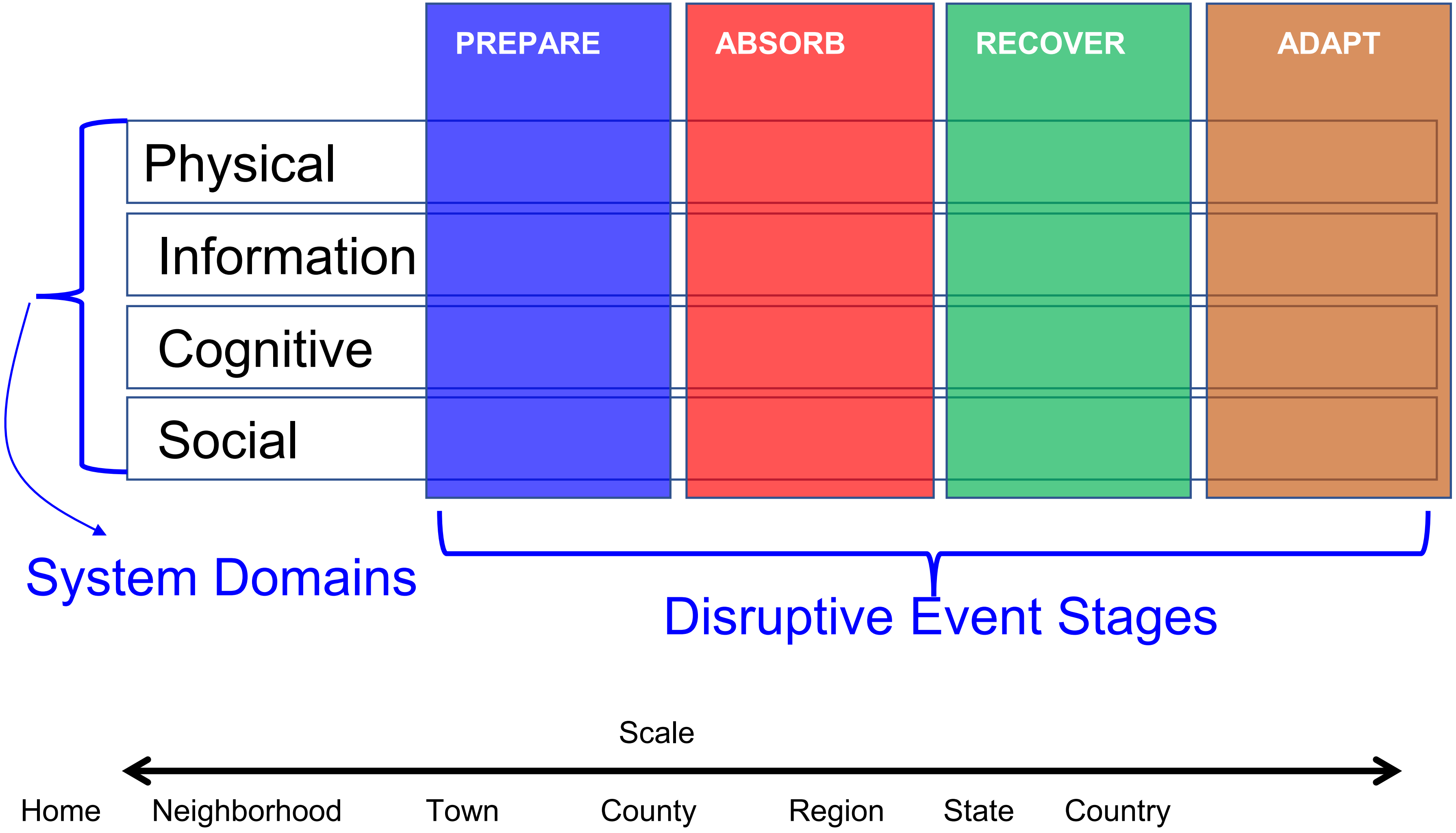
How to Quantify Resilience?



After
2019



Resilience Matrix



Assessment using Stakeholder Values

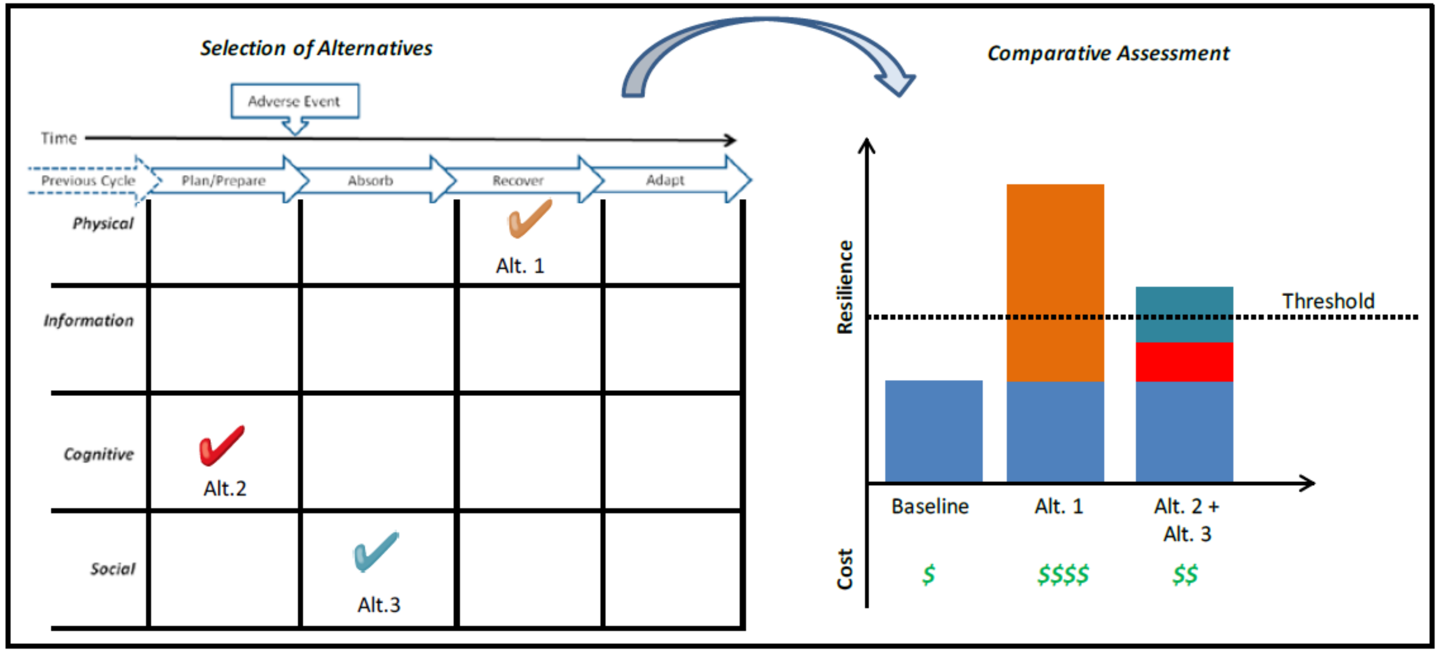


Figure 5: Comparative Assessment of Resilience-Enhancing Alternatives

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, I,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,I.
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

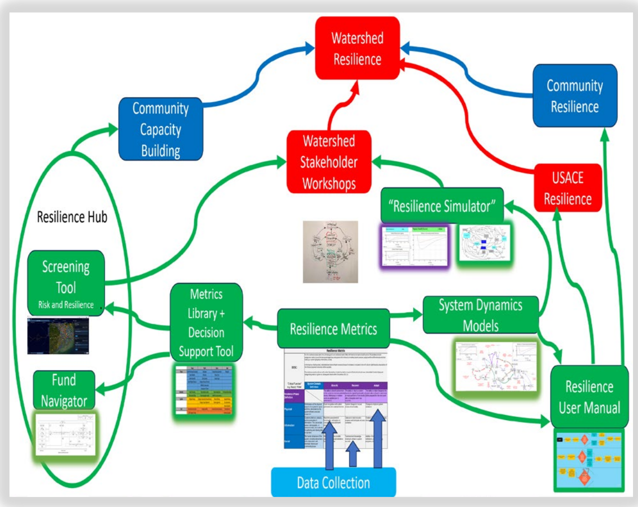
USACE Watershed Resilience

- **Project Objective:**
- Develop a framework and replicable process to measure the resilience of:
  1. USACE missions
  2. Community-level infrastructure
  3. Critical functions across the watershed

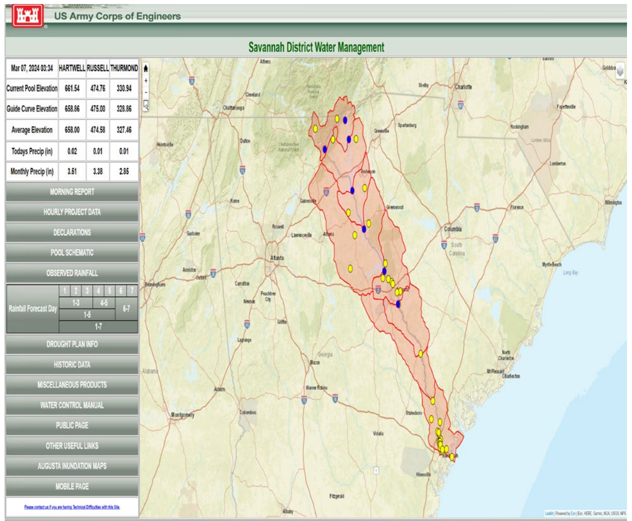
DSR3P Hypothesis #1:
Resilience Capacity Building

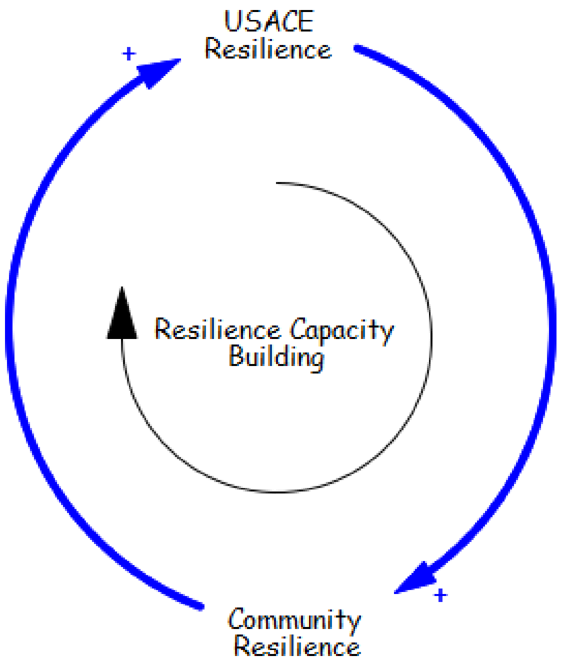
- The resilience of USACE projects improves community resilience.
- Community resilience improves the resilience of USACE projects.

*green boxes are products in development



Pilot in the Savannah River Basin
USACE Projects include: Hartwell, Russell, Thurmond





USACE Resilience Matrix Methodology

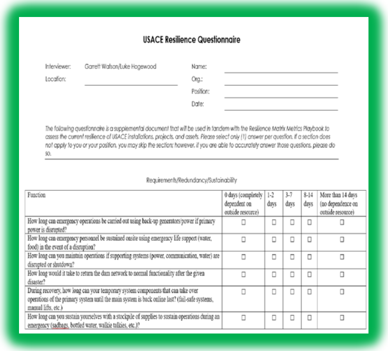
Resilience Matrix

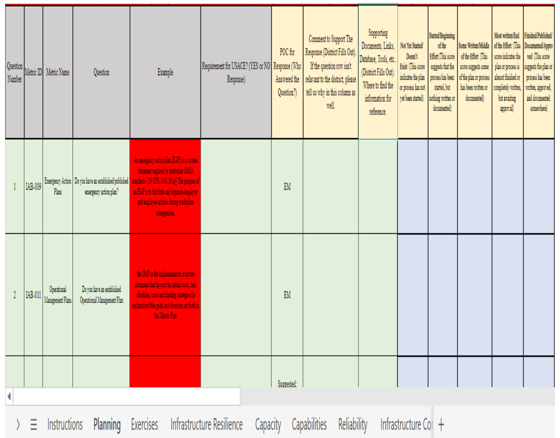
	Absorb	Recover	Adapt
Physical	System Performance/Functionality System Reliability Robustness Consequences of failure System Vulnerability Hazard Mitigation Measures Redundancy Back-up Systems Emergency Resources	Recovery Time Temporary Facilities Recovery Resources	Adaptive Capacity Infrastructure Condition 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						Me	
Metric Name	Unit of Analysis	System Doma	Resilience Phas	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





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

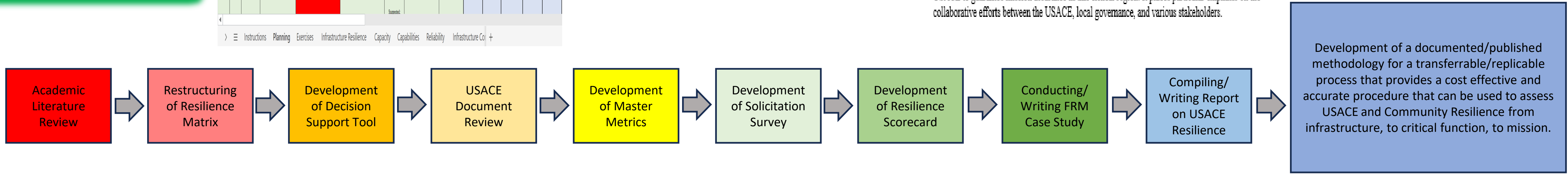
Measuring USACE Resilience in the Savannah Basin – manuscript for peer review

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



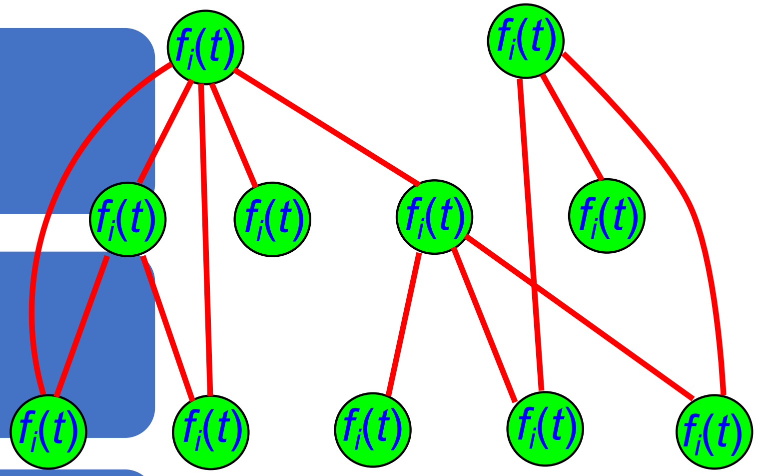
Network-based Resilience Theory?

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 ($\boldsymbol{E}$)

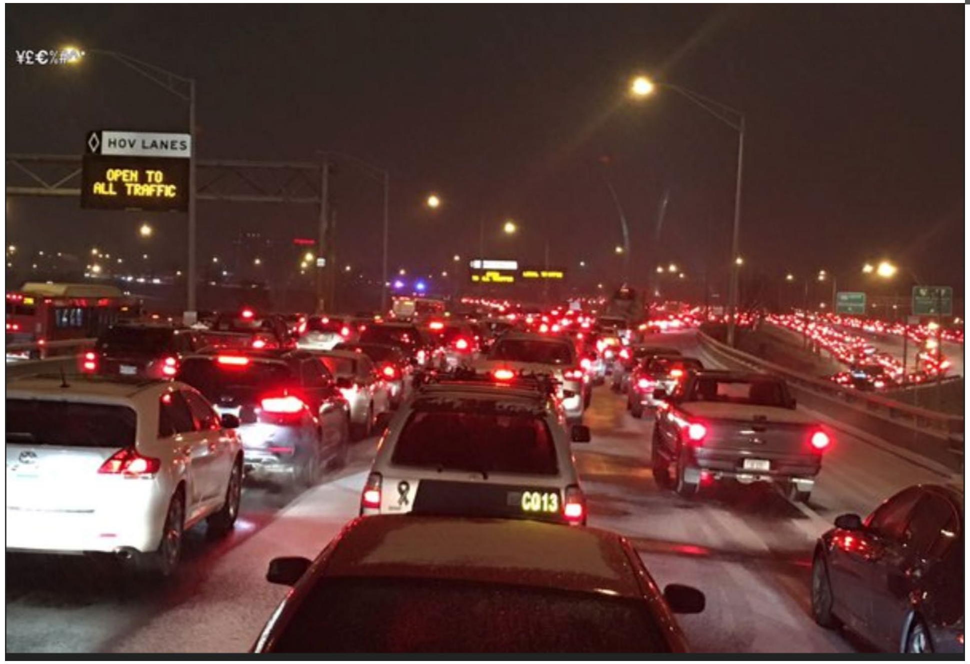


$$R = f(\mathcal{N}, \mathcal{L}, \mathcal{C}, \boldsymbol{E})$$

Poor Efficiency:

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

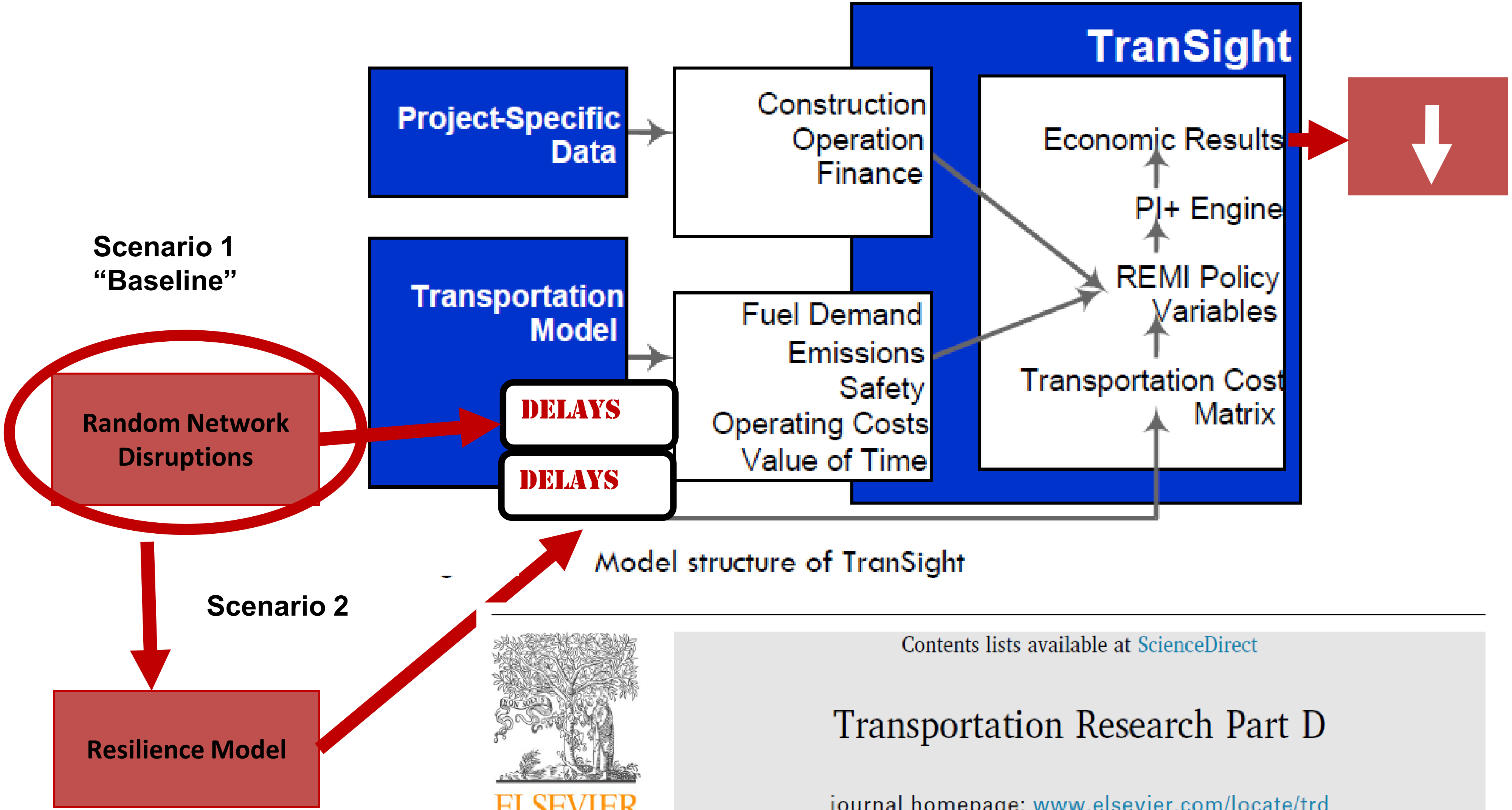
Traffic congestions are predictable and are typically of moderate level.



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

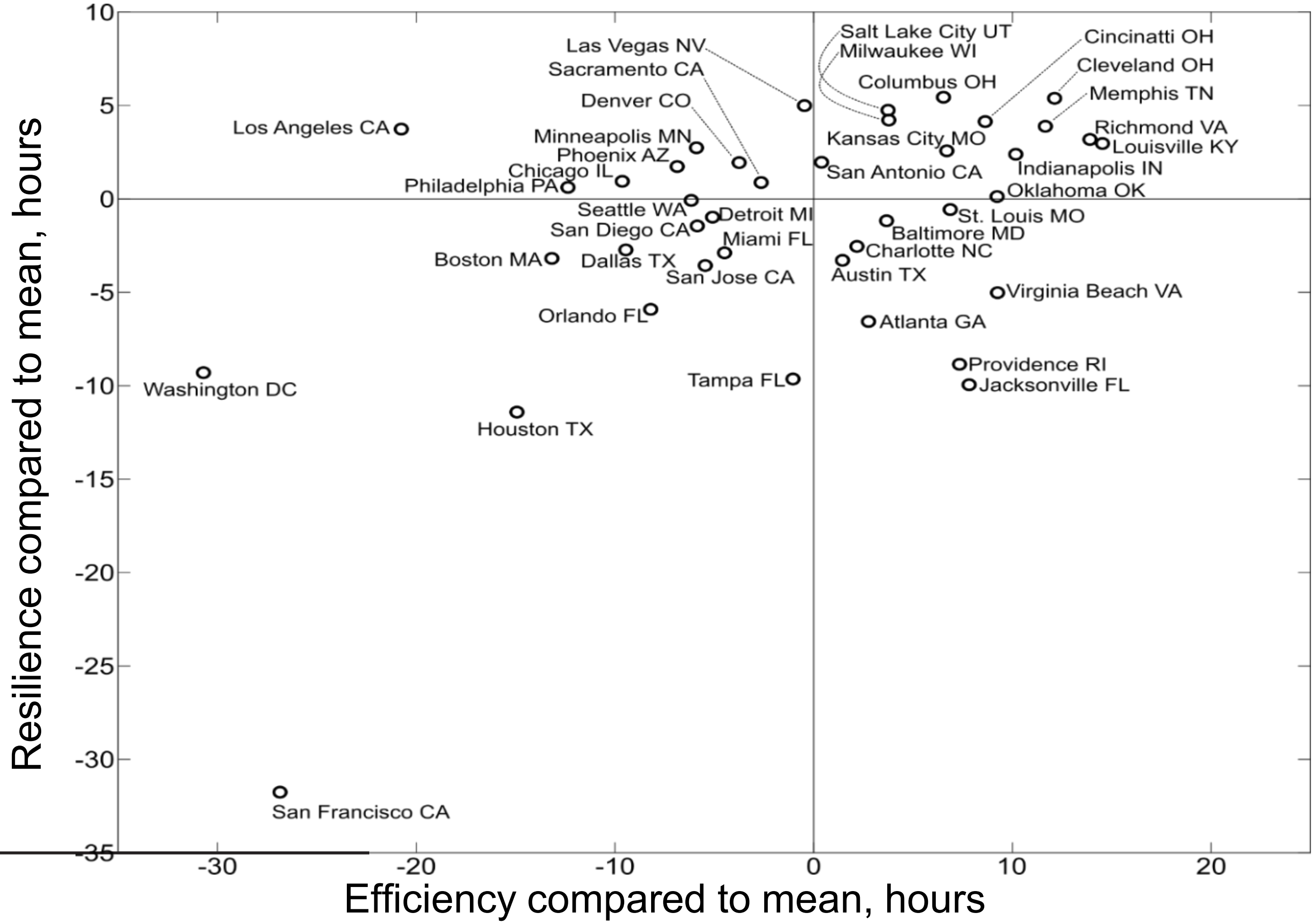
Contents lists available at ScienceDirect

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



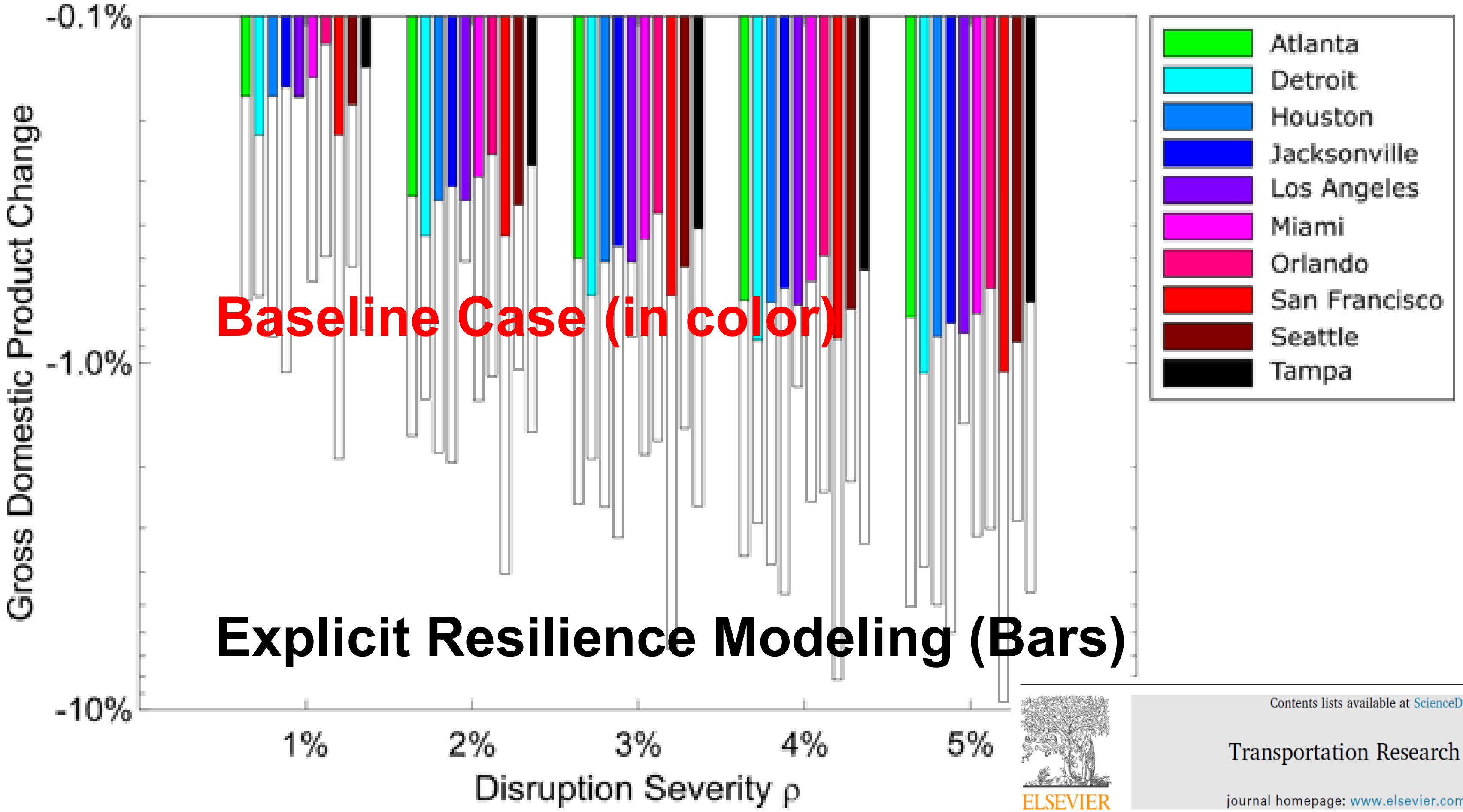
SCIENCE ADVANCES | RESEARCH ARTICLE

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

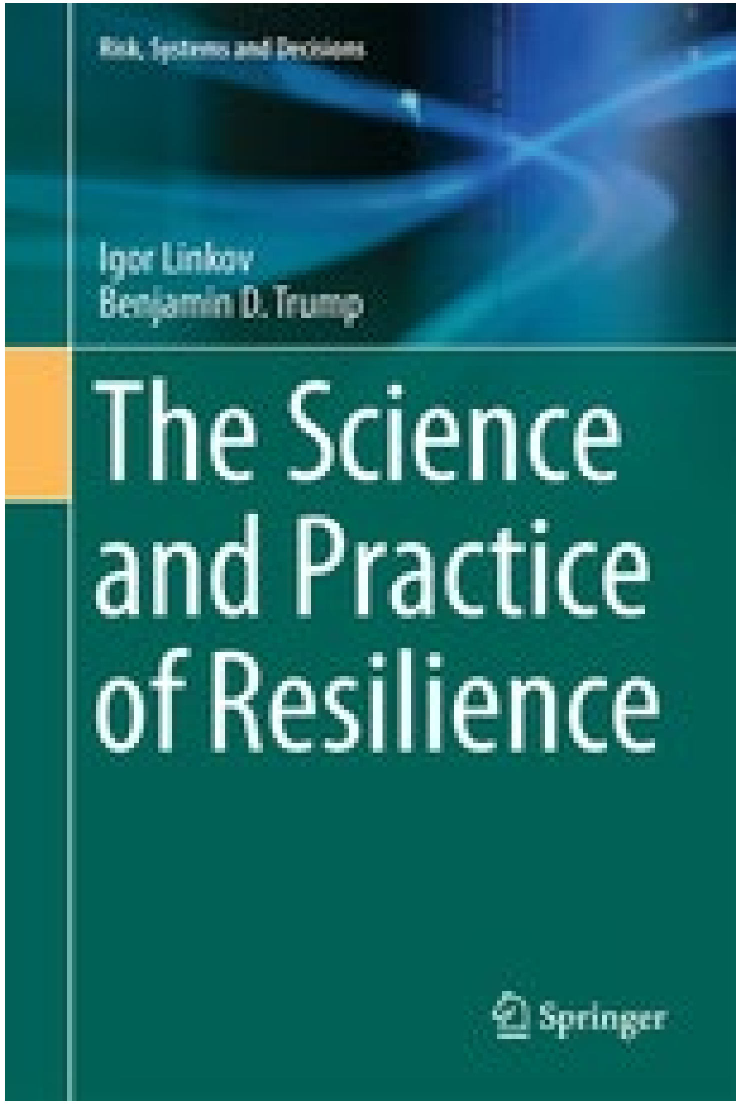


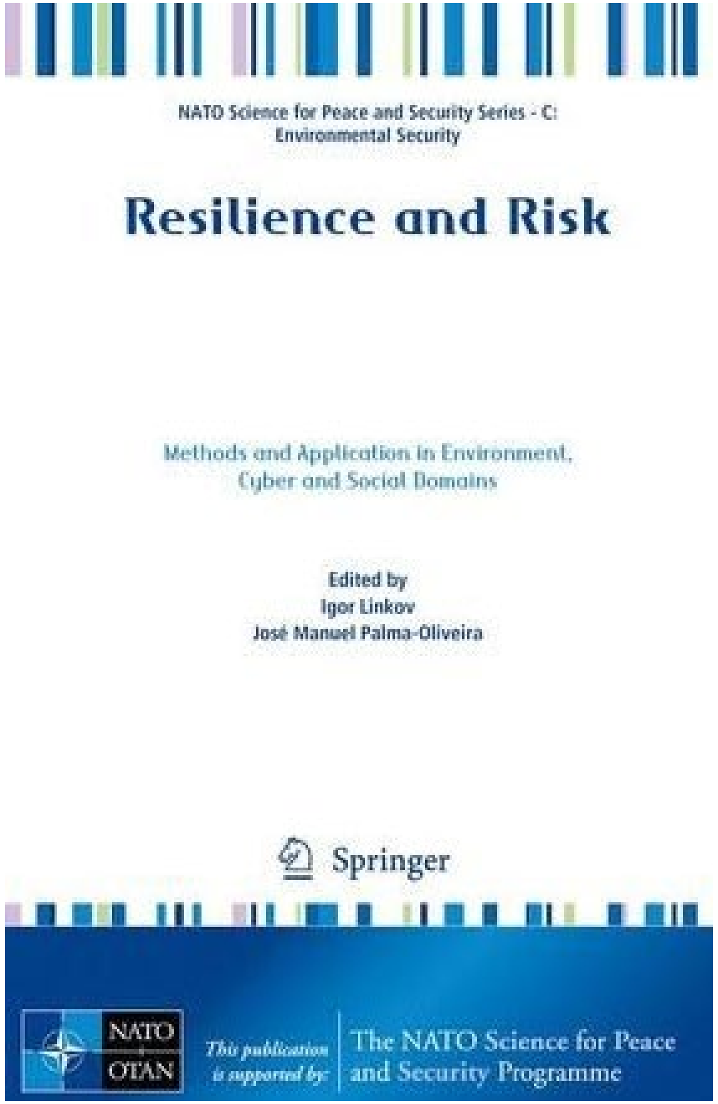
Contents lists available at ScienceDirect

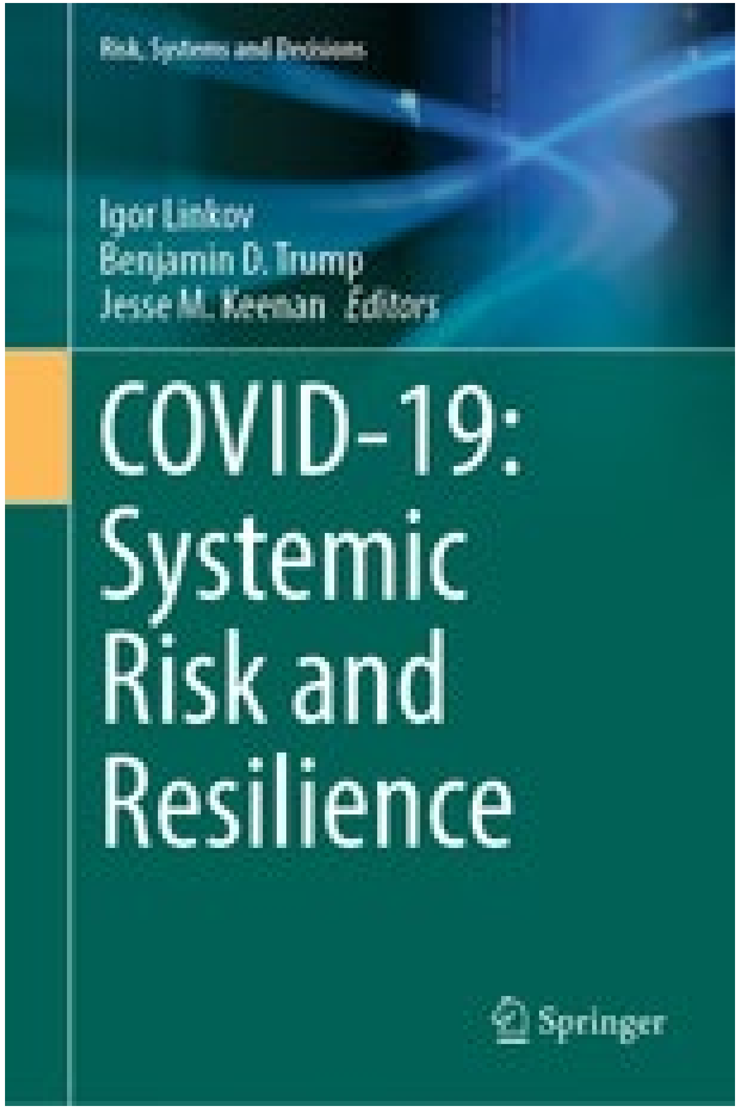
Transportation Research Part D

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

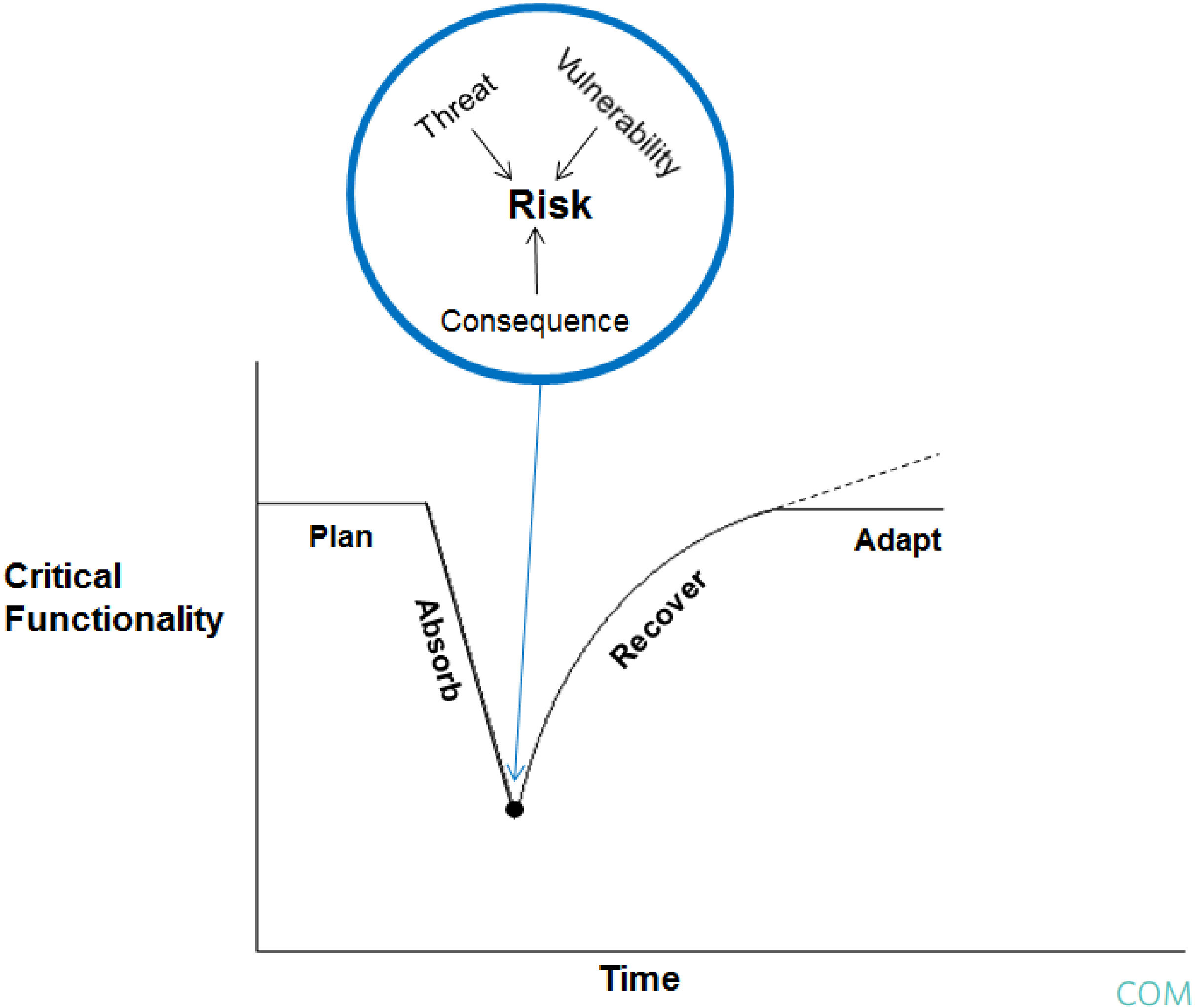
Lack of resilience in transportation networks: Economic implications


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

System Risk/Security and Resilience



Risk Analysis

System Resilience

Nature Climate Change 2014

COMMENTARY:

Changing the resilience paradigm

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

Risks: Conventional, emerging, systemic

Type of risk	Definition	Main features	Example	Implications
Conventional risks	Known, well-defined risks	**Familiarity–** recognisable patterns and management regimes that are relatively stable and have proven to be effective if implemented according to certain rules	• Bicycle theft • Salmonella infection • Car accidents • Obesity	Use **standard** risk management **practices**, e.g., regulation
Emerging risks	New risks or known risks that become apparent in new context conditions (IRGC 2015)	**Uncertainty** regarding causes, potential consequences, and probabilities of occurrence **Lack of familiarity** with the risk	• New processes and products in the field of synthetic biology • Malaria spreading to higher latitudes	Focus on **early detection** and analysis of elements that triggers emerging risks. Prepare to **revise** decisions and adapt.
Systemic risks	Threats that individual failures, accidents or disruptions present to a system through the process of contagion	**Highly interconnected risks** with complex causal structures, non-linear cause-effect relationships **Lack of knowledge** about interconnections in an interdependent and complex environment, prevention	• Desertification and collapse of the Aral Sea • 2008 global financial crisis • Pandemics • Cyber-security • Global climate change • Fish stocks depletion	Focus on **adaptation** and **transformation** of the organisation and the system

IRGC Guidelines for Dealing with Systemic Risks

IRGC, 2018