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

State of the Science and Practice in Resilience Analytics: Application to DFW

Igor Linkov, PhD

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

Adjunct Professor, University of Florida

Ilinkov@yahoo.com

Robert Horton

Vice President, Environmental Affairs & Sustainability

Dallas-Fort Worth International Airport

PhD Candidate, University of Florida

Peter Evangelakis, PhD

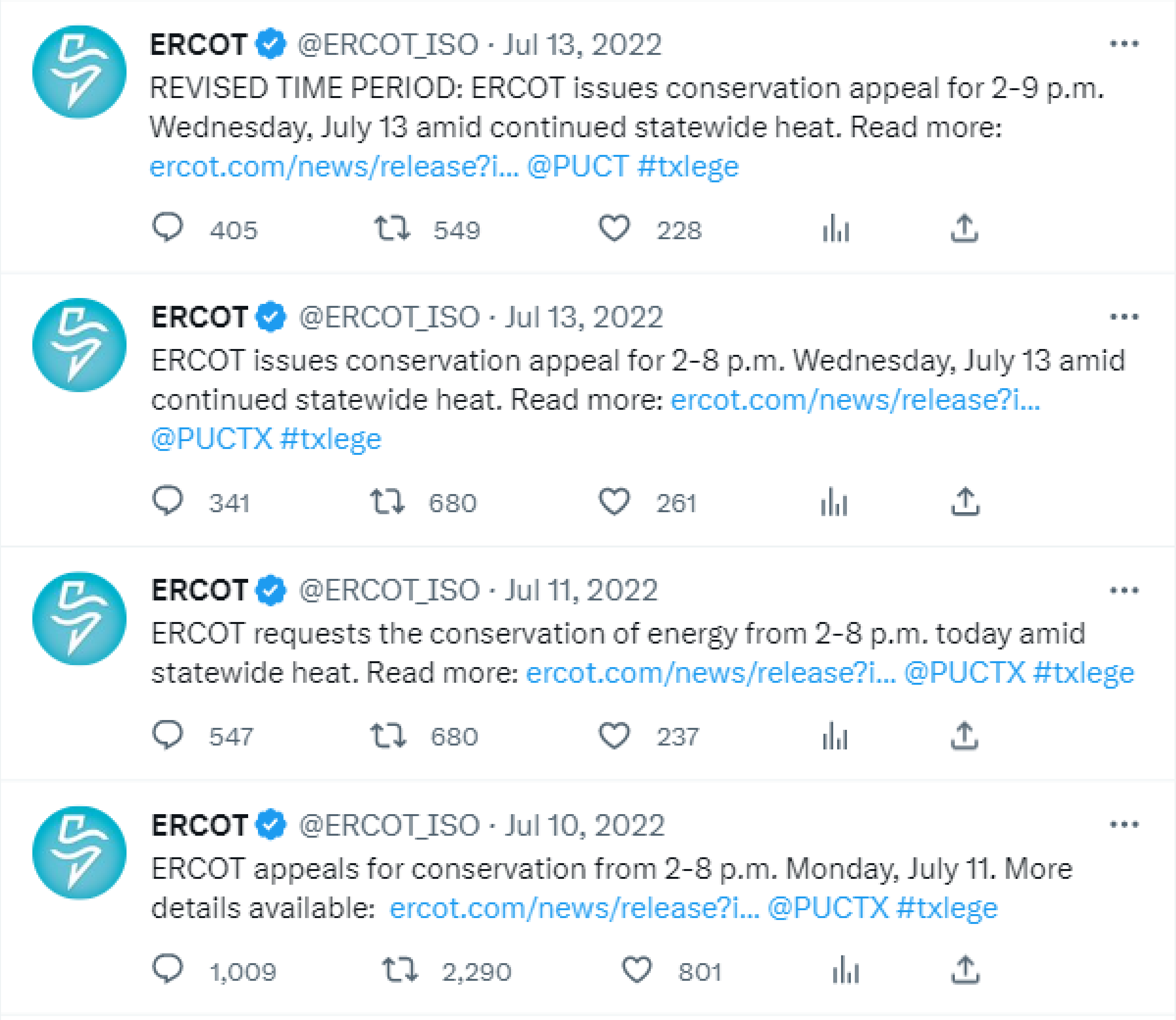
Senior Vice President of Economics & Consulting

REMI

February 21st, 2024

Texas’ Energy Demand on the Rise

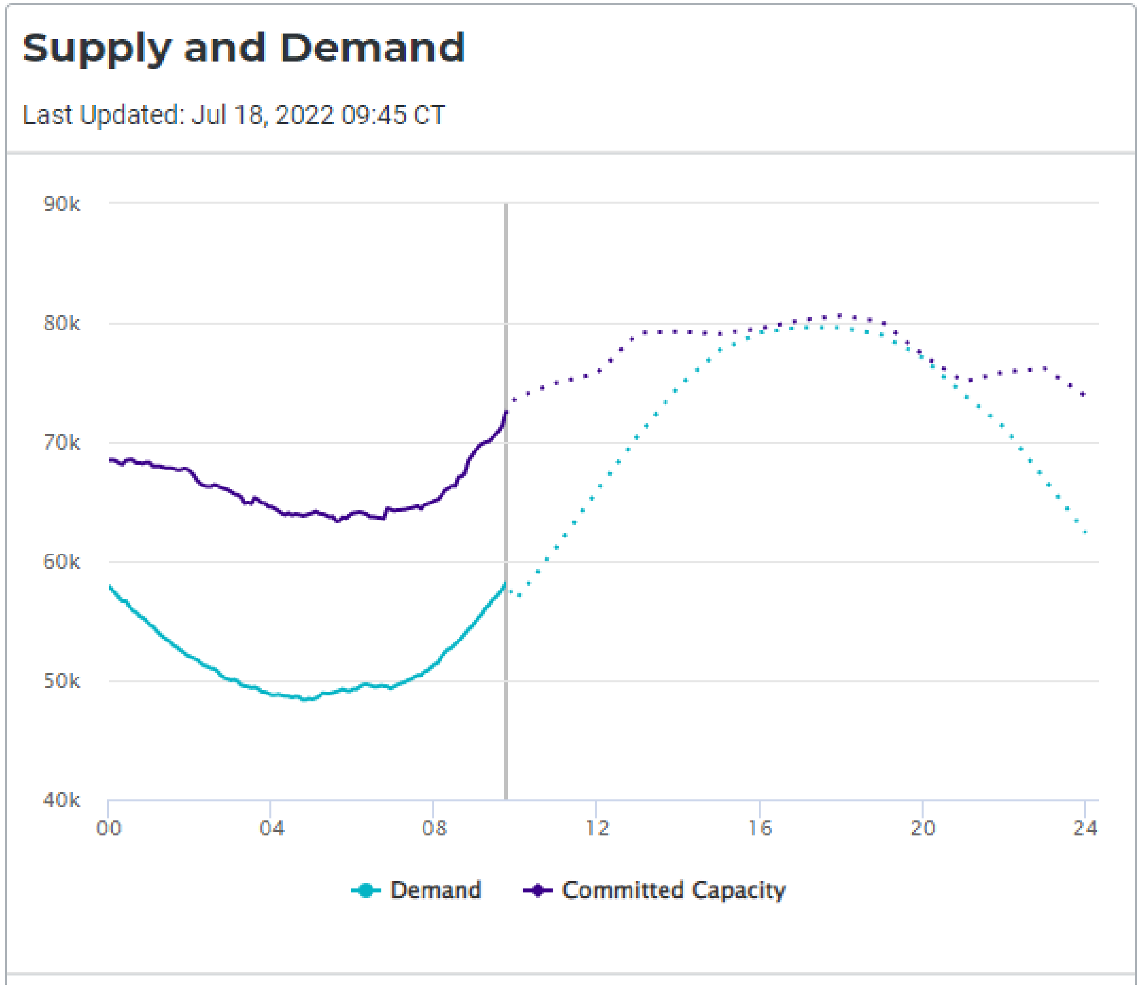
Existing strategies to meet near-future demand are not sustainable


ERCOT @ERCOT_ISO · Jul 13, 2022
REVISED TIME PERIOD: ERCOT issues conservation appeal for 2-9 p.m. Wednesday, July 13 amid continued statewide heat. Read more: ercot.com/news/release?i... @PUCT #txlege
405 549 228

ERCOT @ERCOT_ISO · Jul 13, 2022
ERCOT issues conservation appeal for 2-8 p.m. Wednesday, July 13 amid continued statewide heat. Read more: ercot.com/news/release?i... @PUCTX #txlege
341 680 261

ERCOT @ERCOT_ISO · Jul 11, 2022
ERCOT requests the conservation of energy from 2-8 p.m. today amid statewide heat. Read more: ercot.com/news/release?i... @PUCTX #txlege
547 680 237

ERCOT @ERCOT_ISO · Jul 10, 2022
ERCOT appeals for conservation from 2-8 p.m. Monday, July 11. More details available: ercot.com/news/release?i... @PUCTX #txlege
1,009 2,290 801

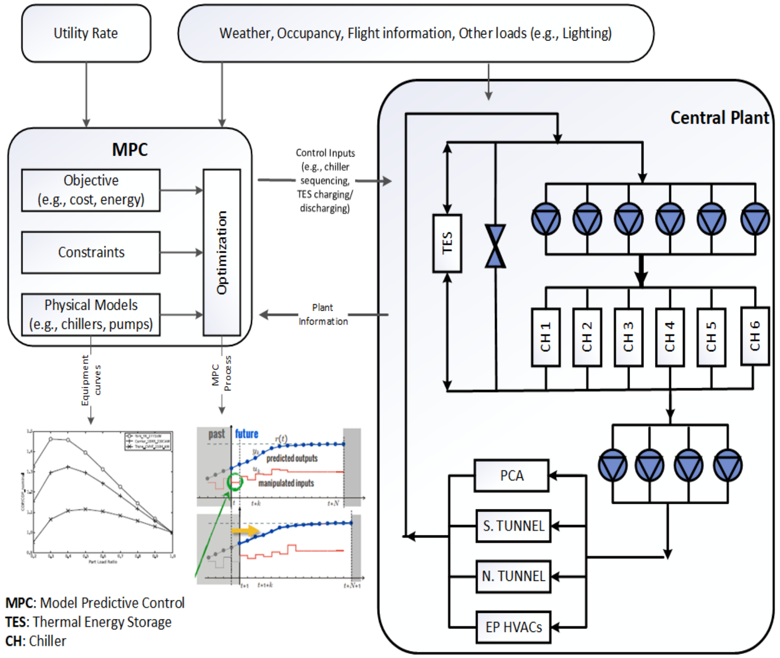


DFW-DOE-NREL Research Collaboration

Central Plant Optimization – Model Predictive Control (MPC)

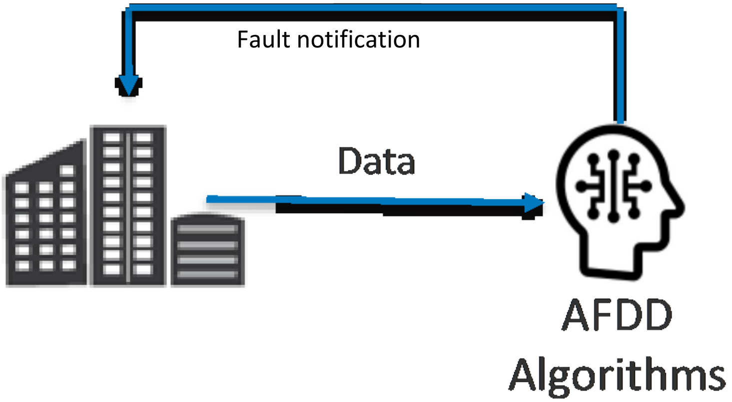
Central Plant Optimization

Development of Model Predictive Control (MPC) that optimizes sequencing of chillers and thermal energy storage in the central plant



Automatic Fault Detection and Diagnostic (AFDD)

Development of rule-based FDD tools for pilot AHUs in terminal D



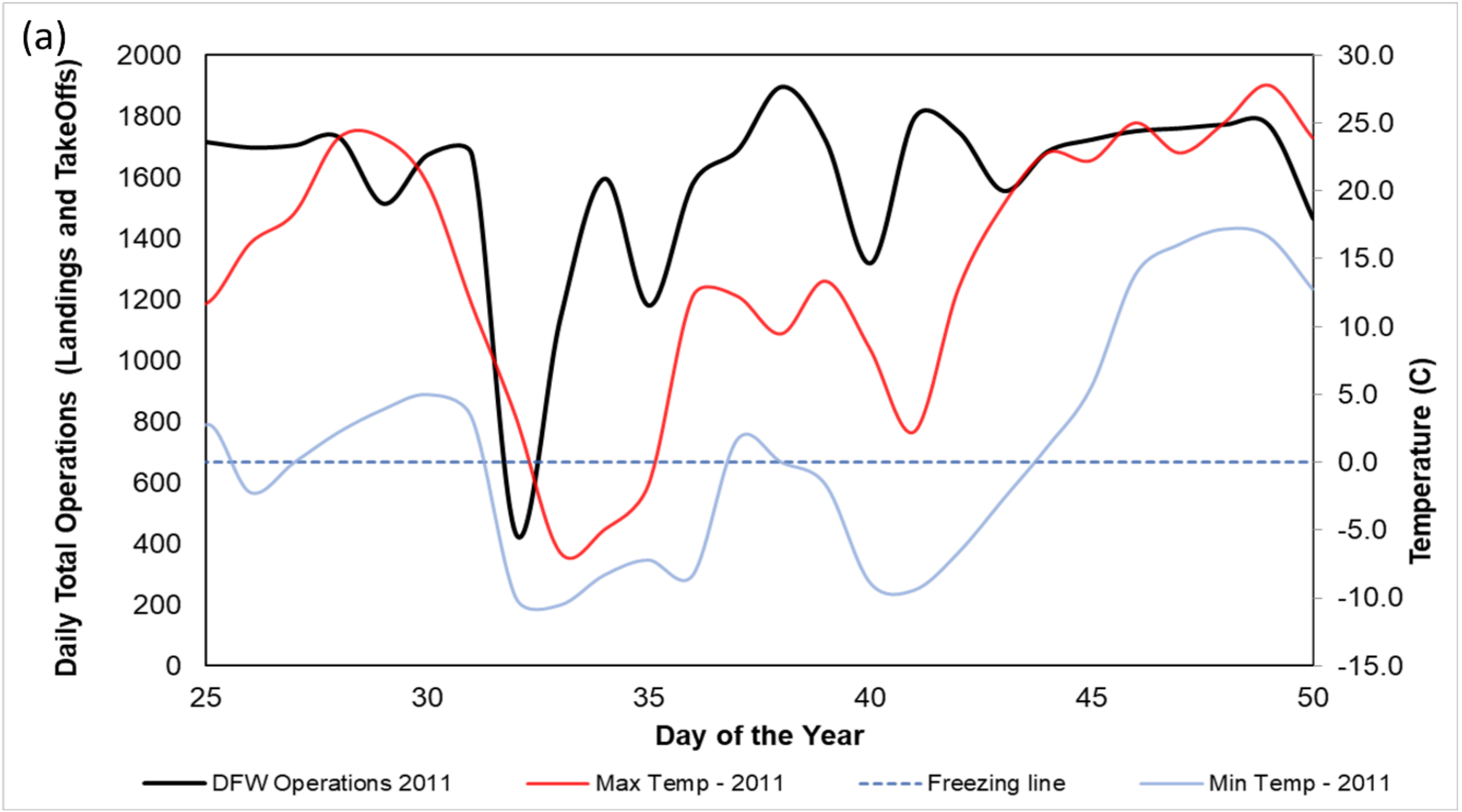
Automated & Improved Analytics

Development of informative analytics for facility managers

CUP Optimization with MPC

Simulated Performance and Savings

Dallas Fort Worth (DFW) Airport in 2011



DFW Airport in 2011 and 2021

<u>Example of Texas Polar Vortex</u>:

- Electric demand shock
- Decreased capacity from lack of winterization and supply of natural gas
- Electric Reliability Council of TX 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?

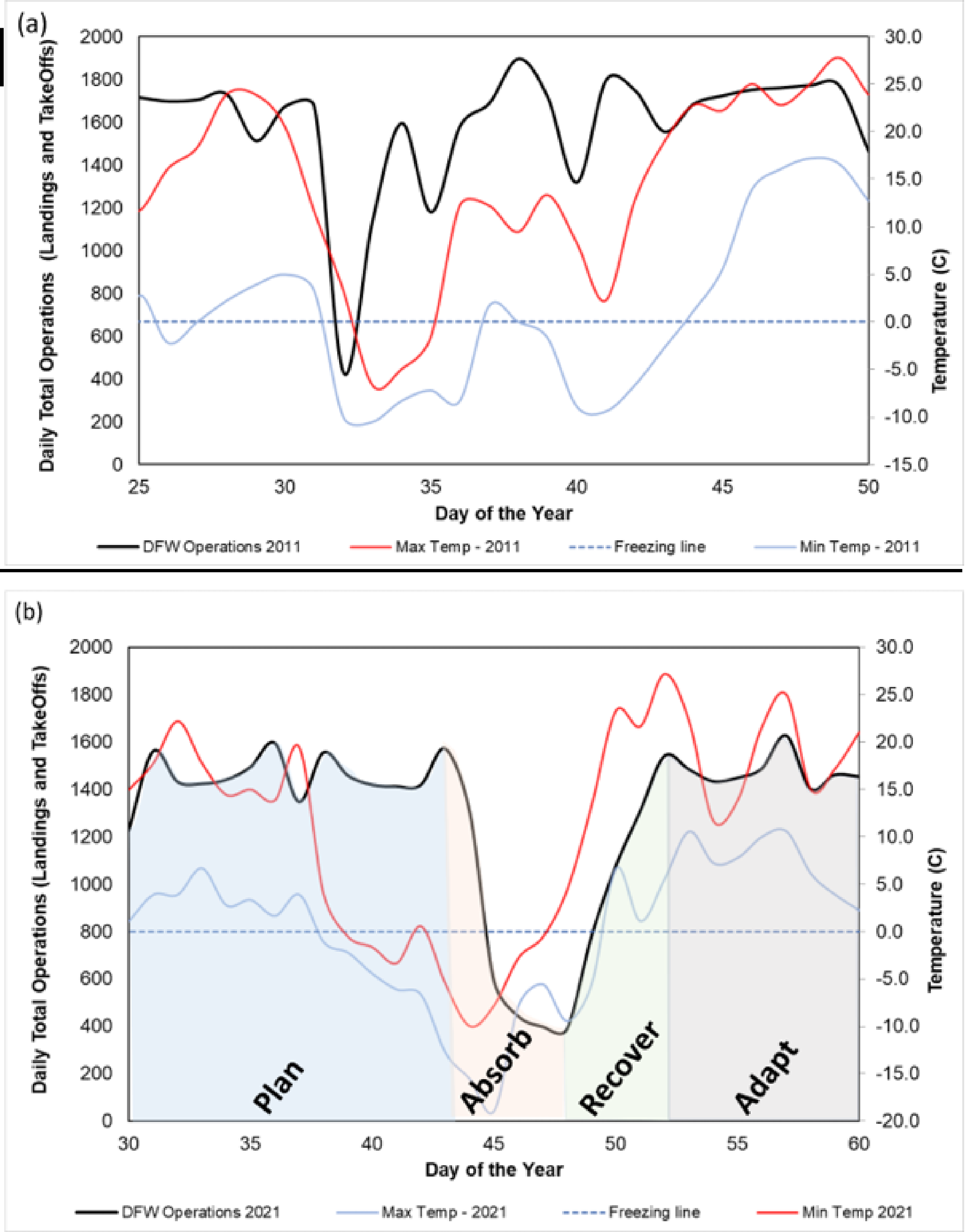
Received: 16 February 2022 | Accepted: 17 February 2022
DOI: 10.1111/1468-5973.12401

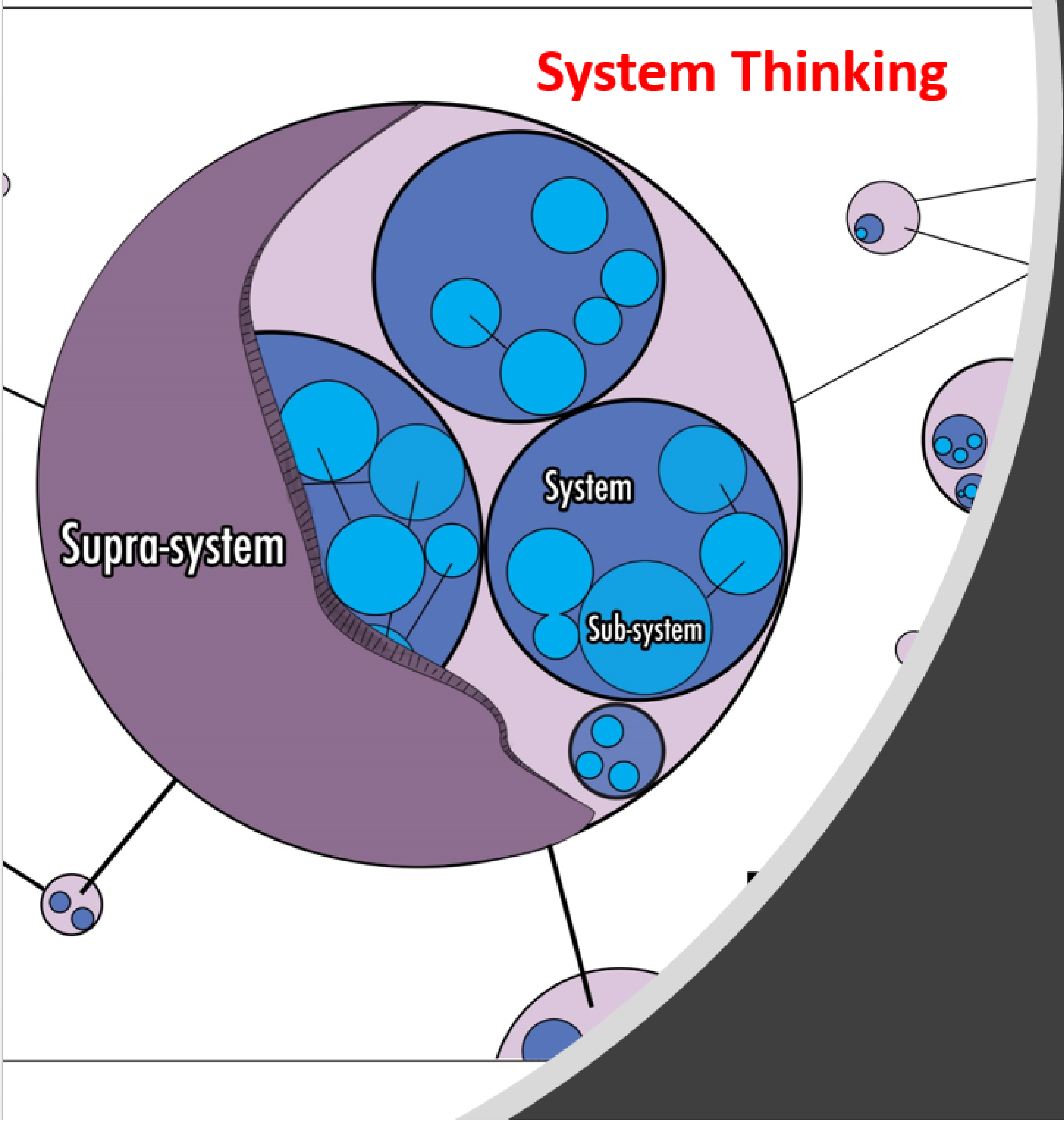
FORUM

WILEY

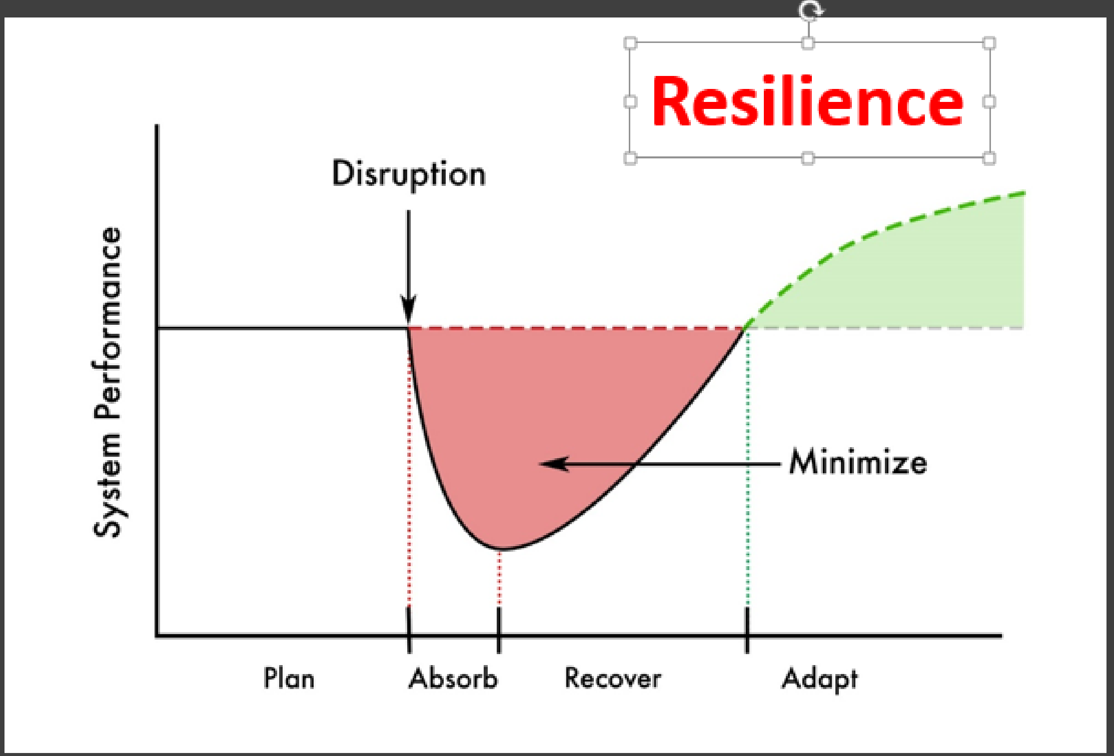
International airports as agents of resilience

Robert Horton[1] | Gregory A. Kiker[2] | Benjamin D. Trump[3] | Igor Linkov[4]





What Makes Complex Systems (Communities) Susceptible to Threat?



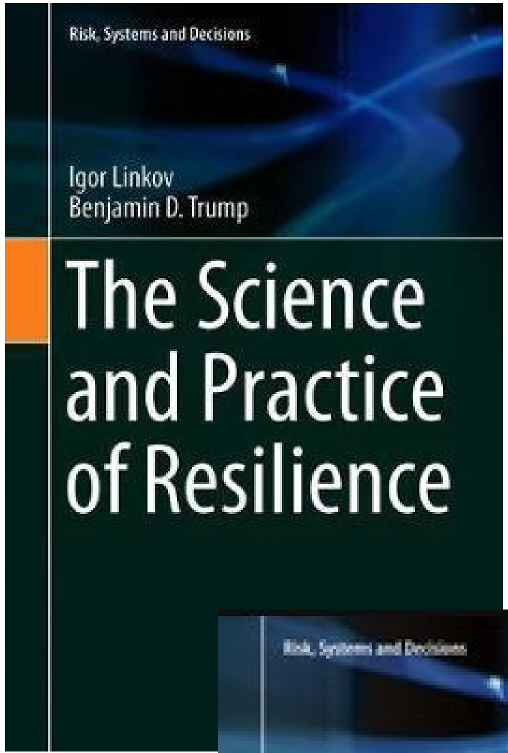
After Linkov and Trump, 2019

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



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

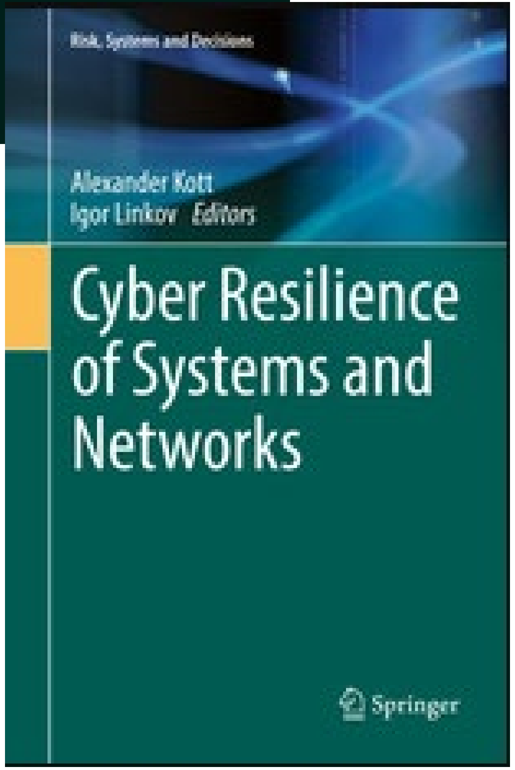
COMPUTER PUBLISHED BY THE IEEE COMPUTER SOCIETY

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



112 COMPUTER PUBLISHED BY THE IEEE COMPUTER SOCIETY

4

Cyber Resilience: by Design or by Intervention?

Alexander Kott, U.S. Army DEVCOM Army Research Laboratory

Maureen S. Golan, U.S. Engineer Research and Development Center and Credere Associates

Benjamin D. Trump, U.S. Engineer Research and Development Center and University of Michigan

Igor Linkov, U.S. Engineer Research and Development Center and Carnegie Mellon University

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

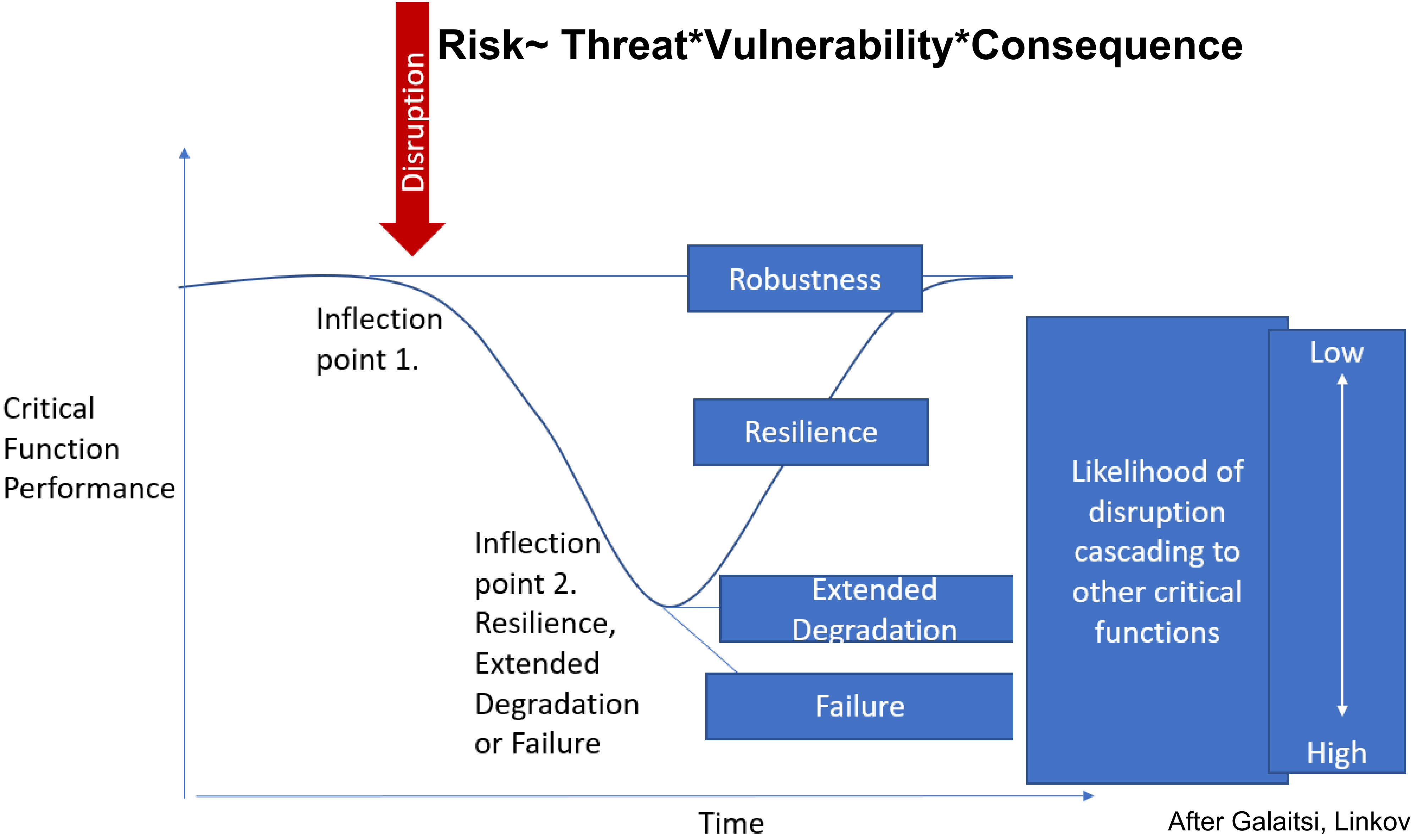
Don’t conflate risk and resilience

‘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

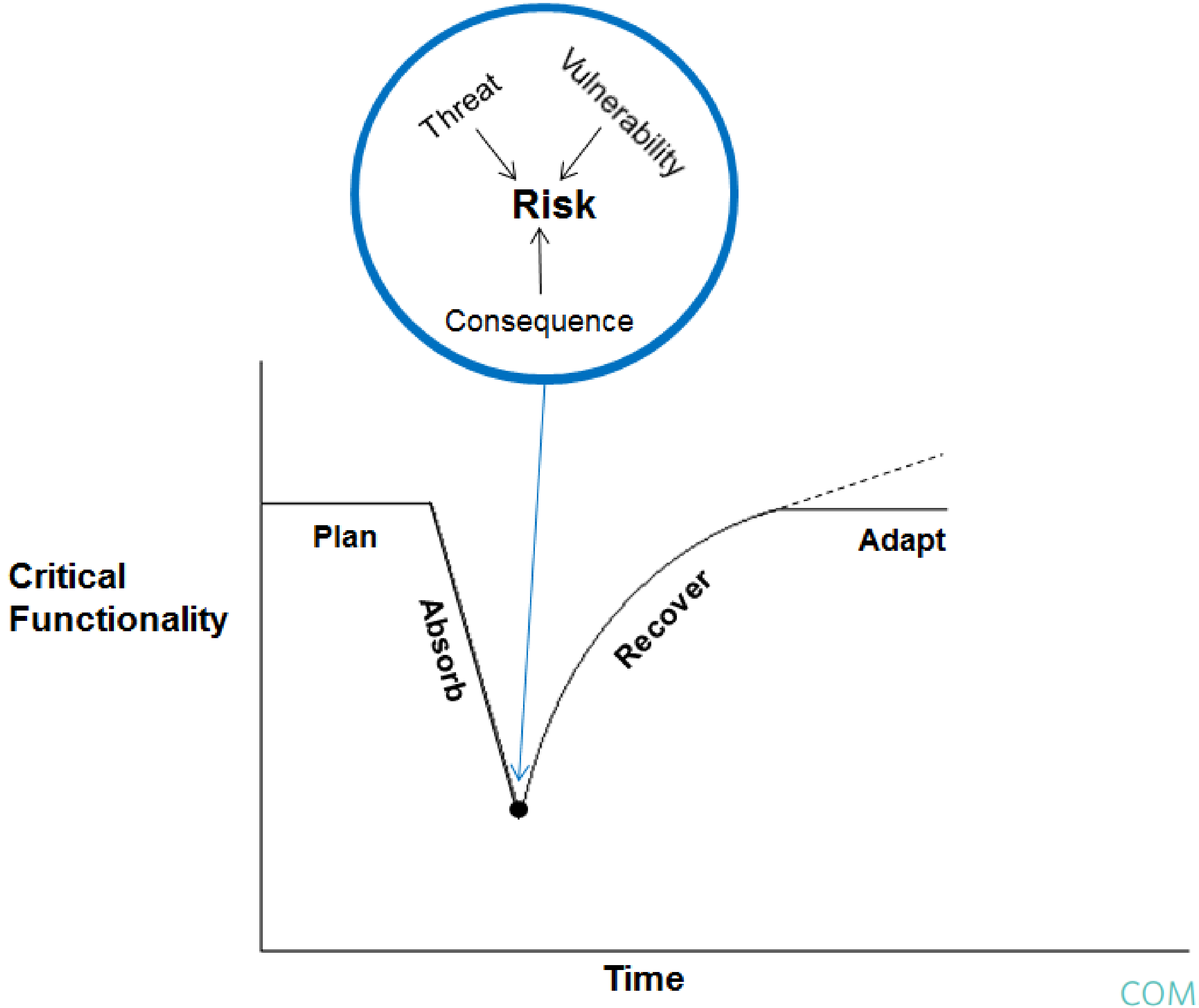
Risk and Resilience at the Time of Crisis

Risk~ Threat*Vulnerability*Consequence



After Galaitsi, Linkov et al, 2023

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,

Evolution of Risk Assessment

- 1970's- Risk=Probability x Consequence
- 1980's- Risk=Hazard x Exposure x Consequence

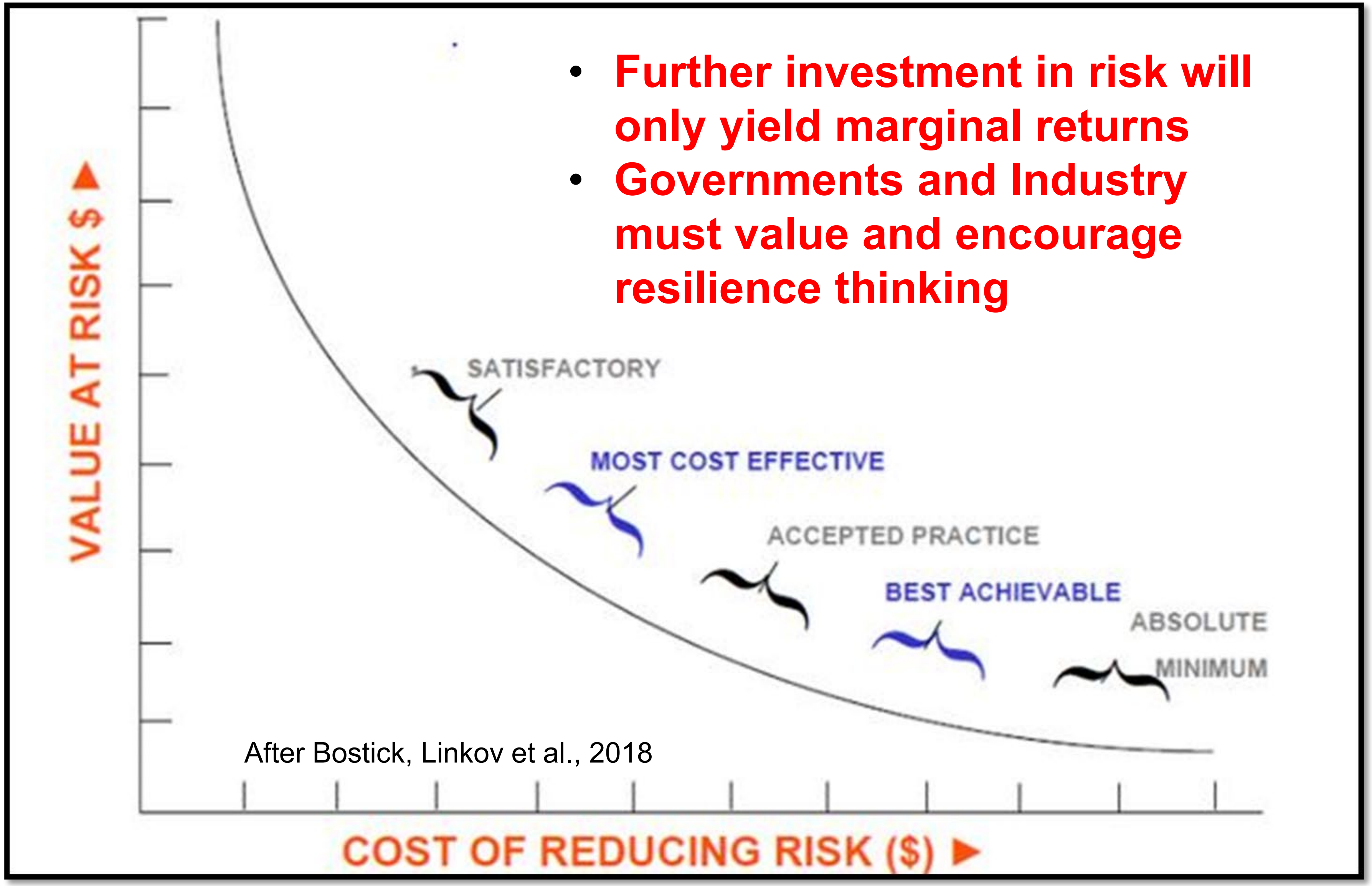
  =Threat x Vulnerability x Consequence
- 2000's- Risk$\sim$f (H x E x E_{ff})

$$m_{Eff1}\ m_{Eff2}\ \ldots m_{Effn}$$

$$m_{H1} m_{H1}\ \ldots m_{Hn} m_{E1}\ m_{E1}\ \ldots m_{En}$$

Cost of Buying Down Risk

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



After Bostick, Linkov et al., 2018

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

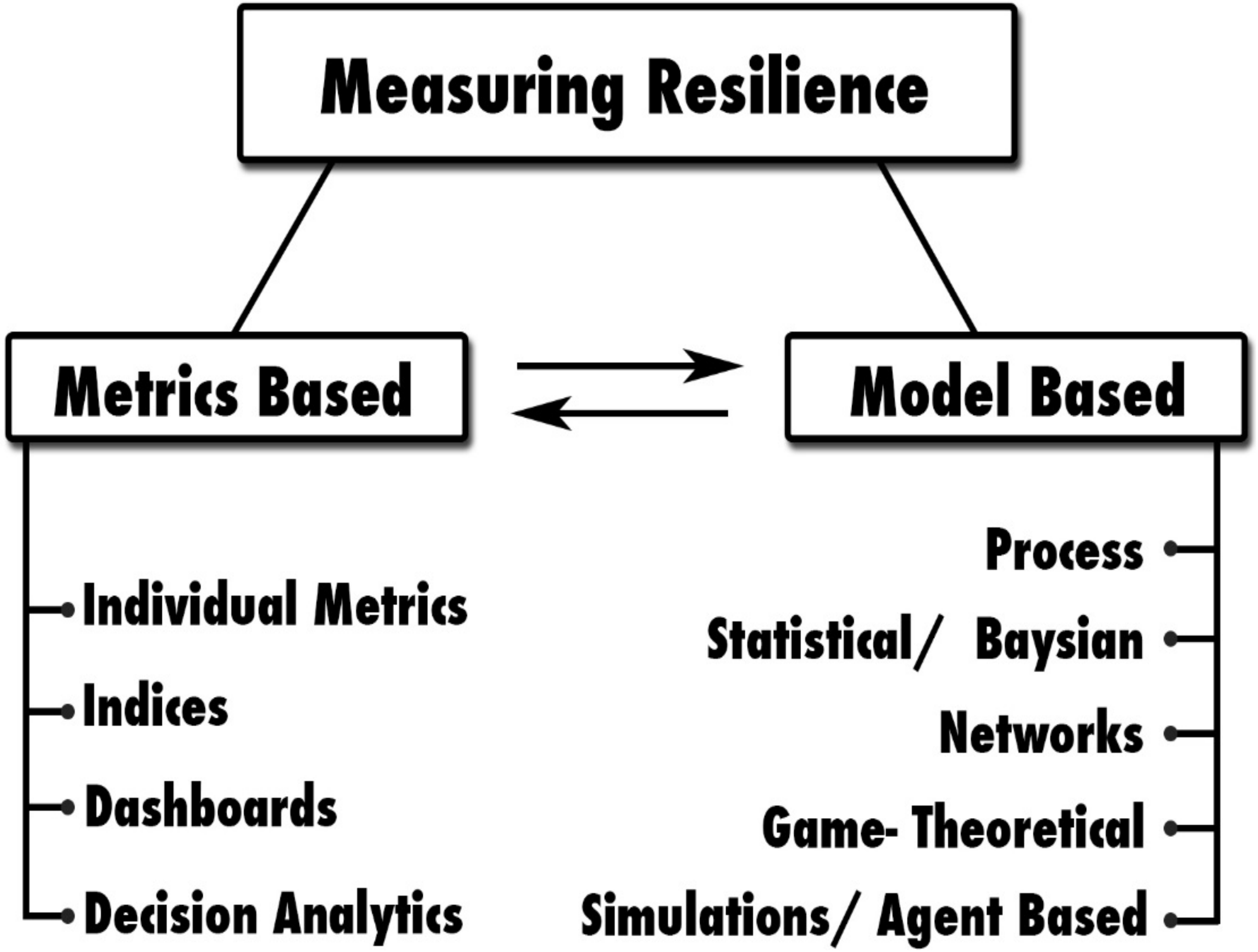
Office of the Press Secretary

For Immediate Release May 11, 2017

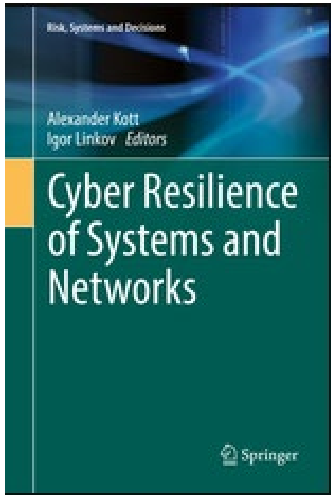
Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure

EXECUTIVE ORDER

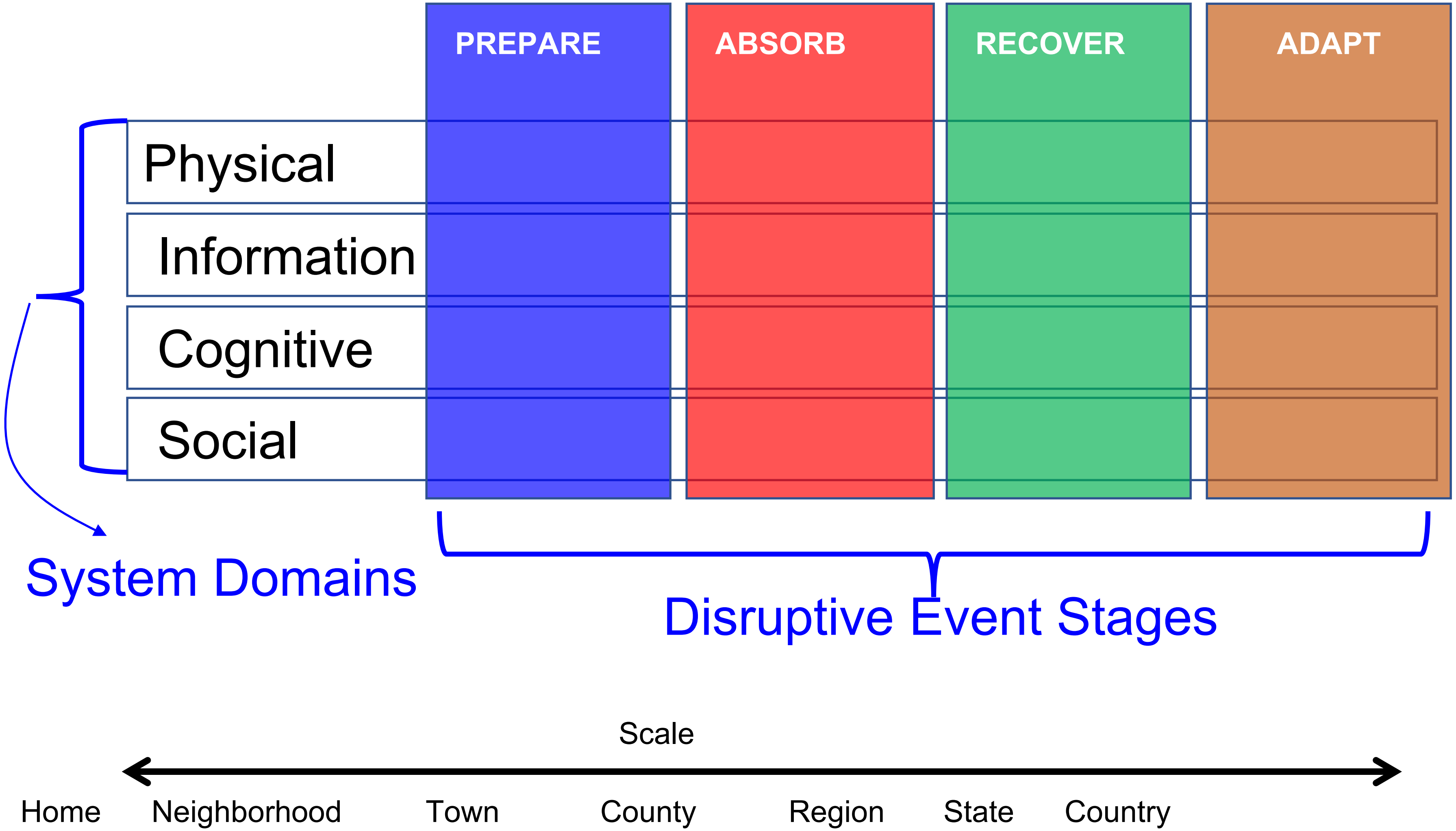
How to Quantify Resilience?



After
2019



Resilience Matrix



Assessment using Stakeholder Values

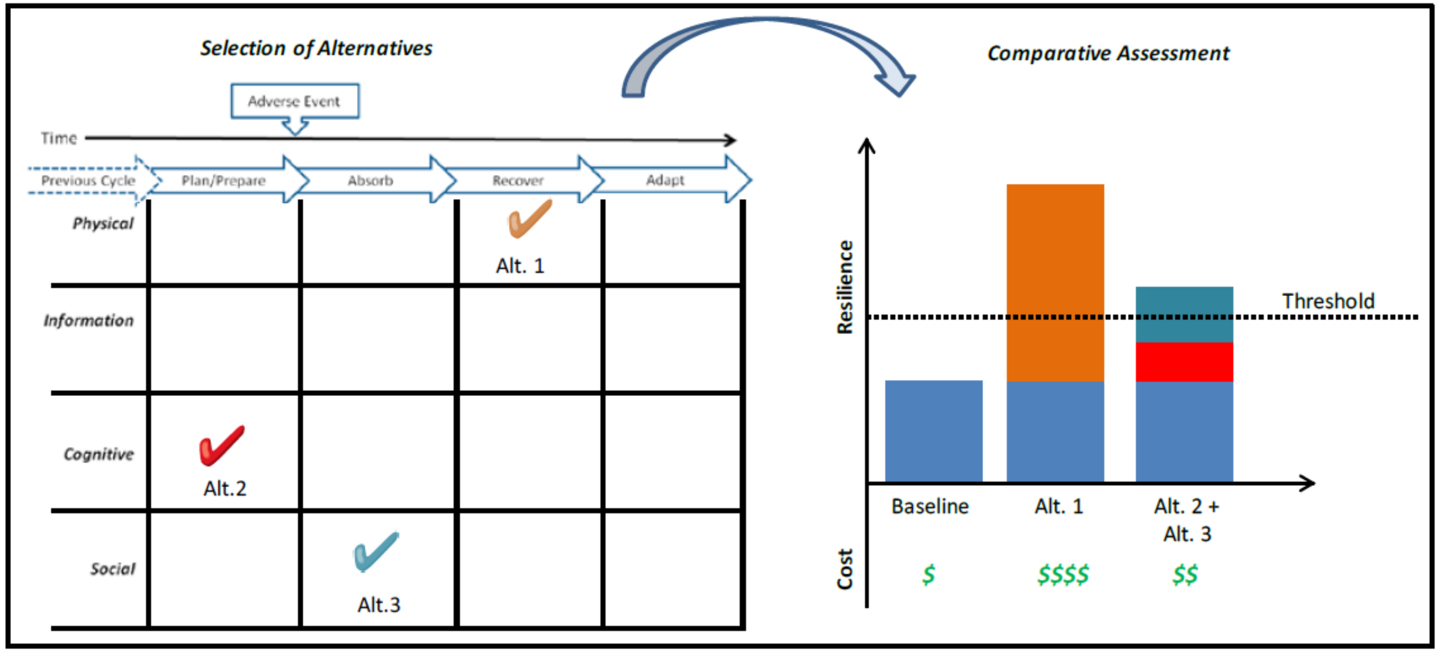


Figure 5: Comparative Assessment of Resilience-Enhancing Alternatives

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 to 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

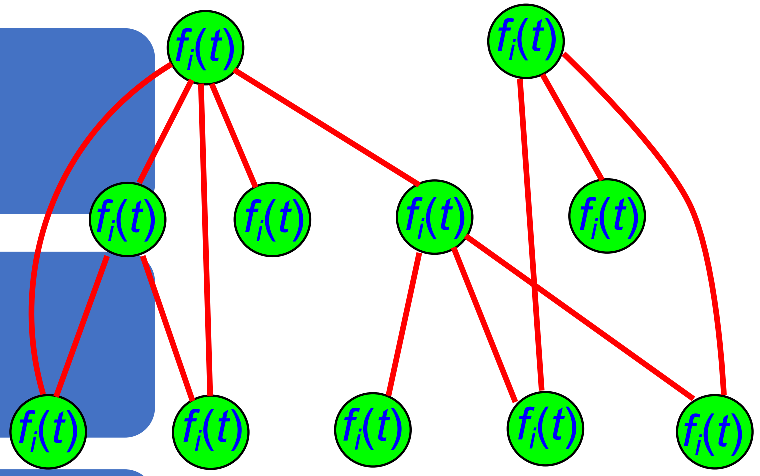
Network-based Resilience Theory?

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 ($\boldsymbol{E}$)

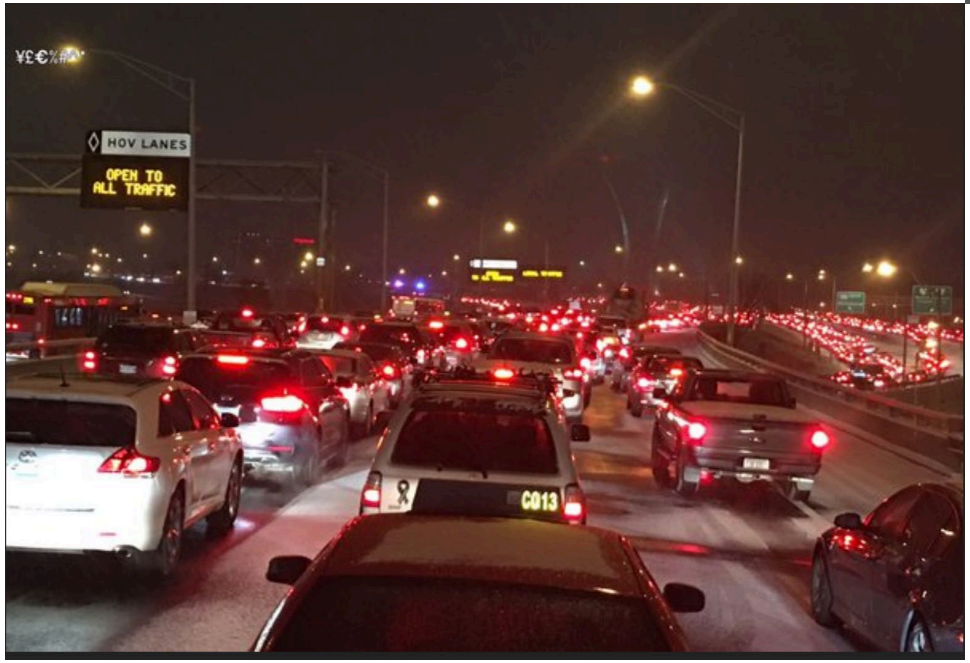


$$R = f(\mathcal{N}, \mathcal{L}, \mathcal{C}, \boldsymbol{E})$$

Poor Efficiency:

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

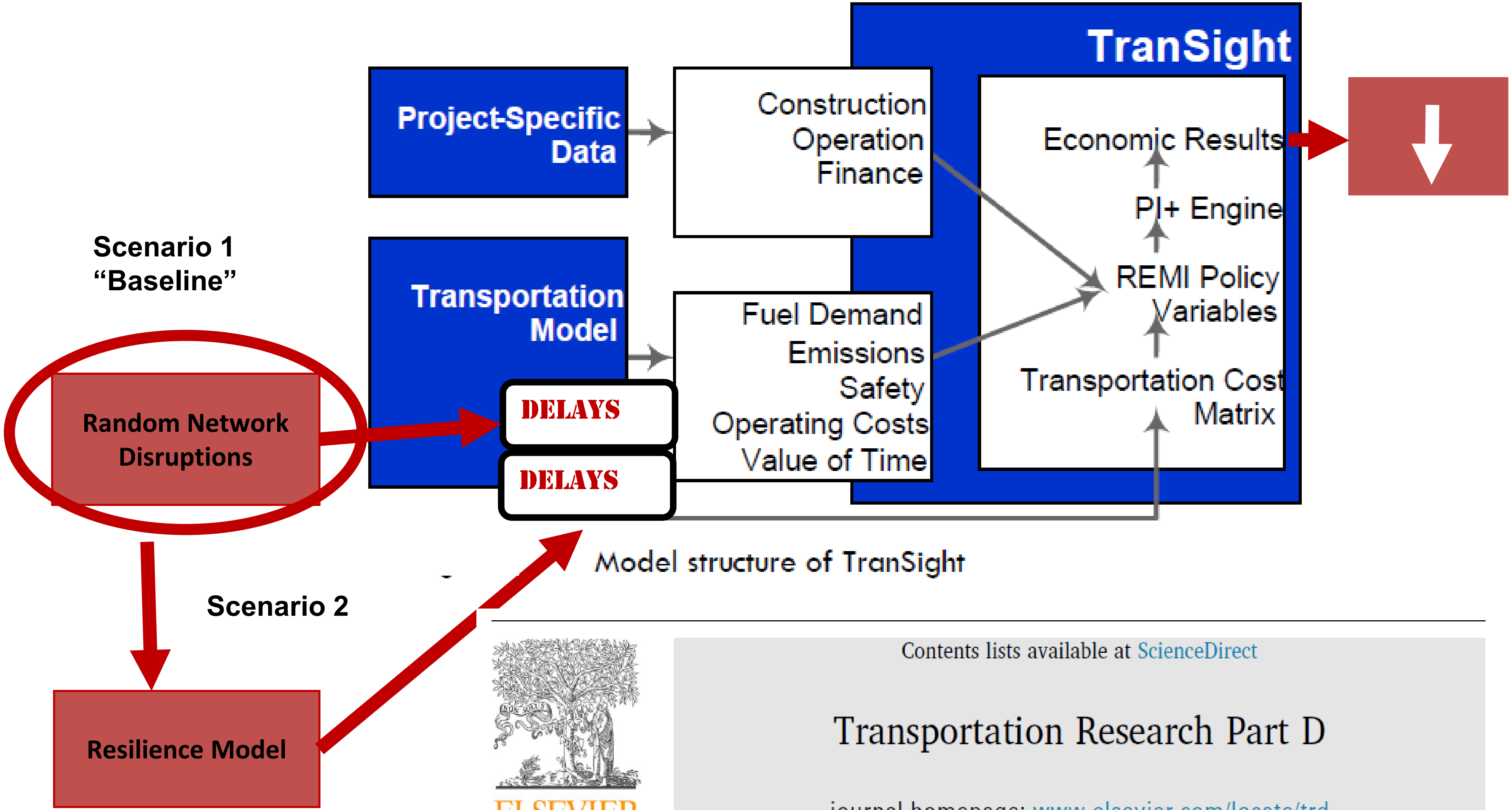
Traffic congestions are predictable and are typically of moderate level.



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

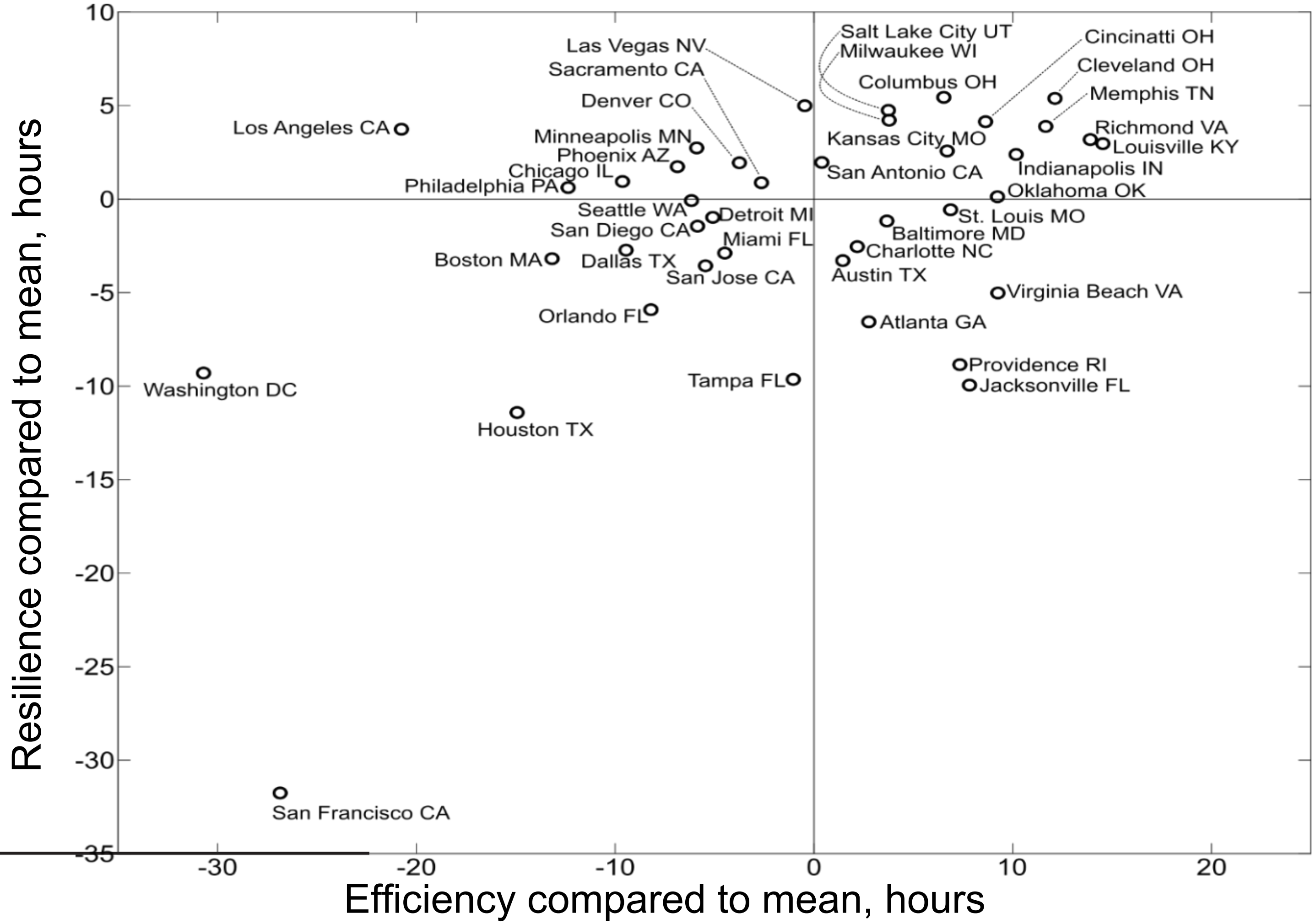
Contents lists available at ScienceDirect

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



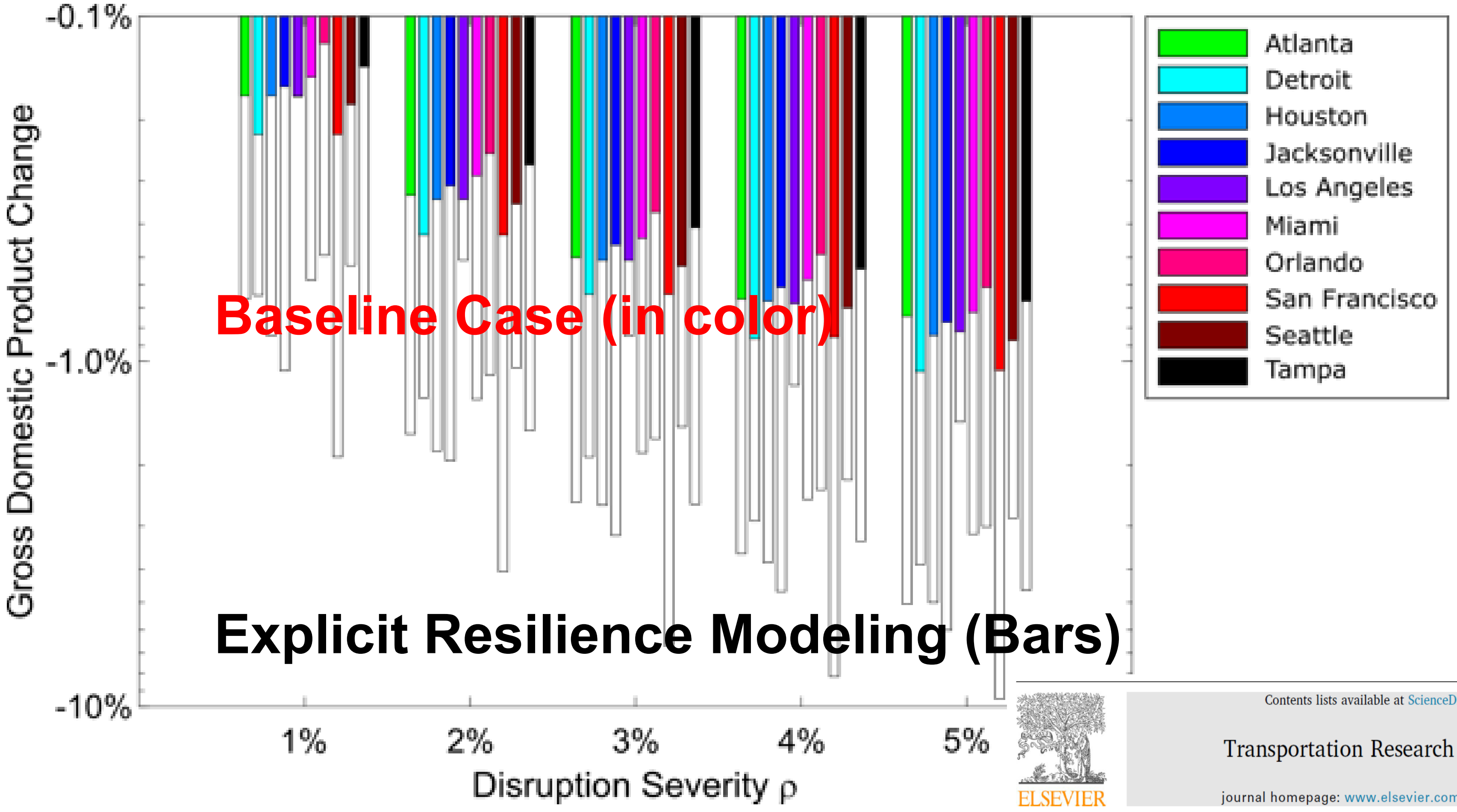
SCIENCE ADVANCES | RESEARCH ARTICLE

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
ELSEVIER

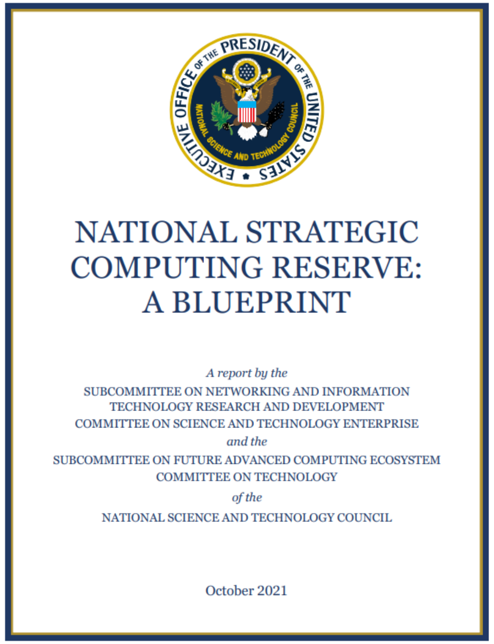
Lack of resilience in transportation networks: Economic implications

112 COMPUTER PUBLISHED BY THE IEEE COMPUTER SOCIETY

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



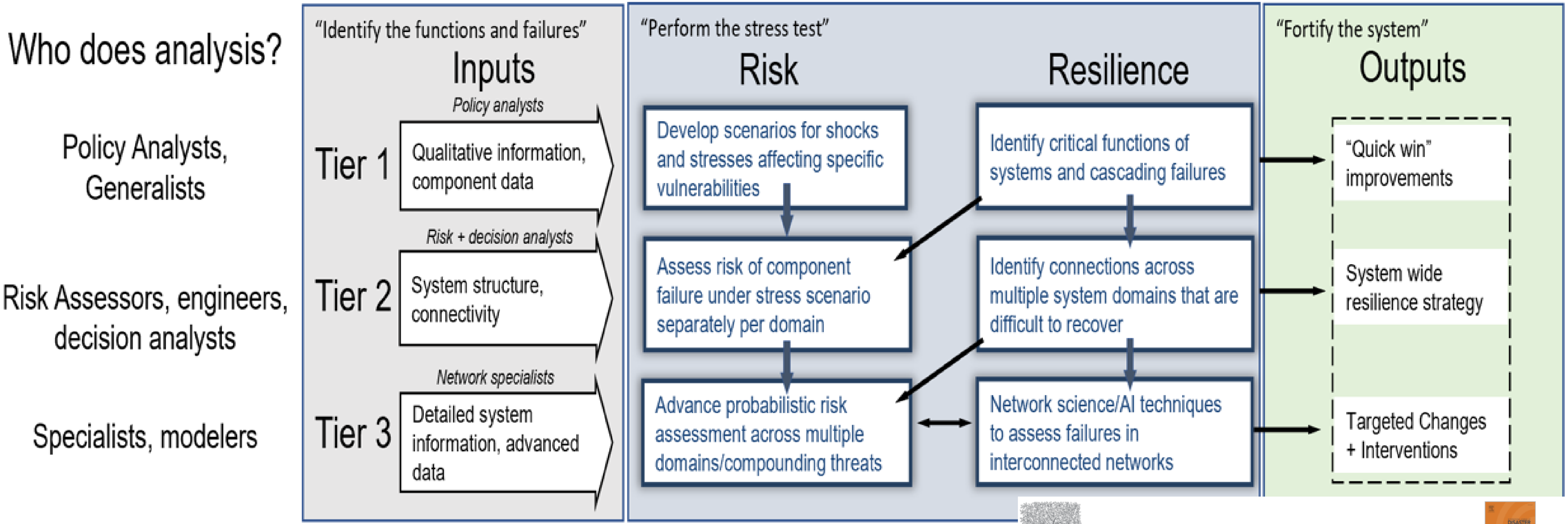
NATIONAL STRATEGIC COMPUTING RESERVE: A BLUEPRINT

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

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

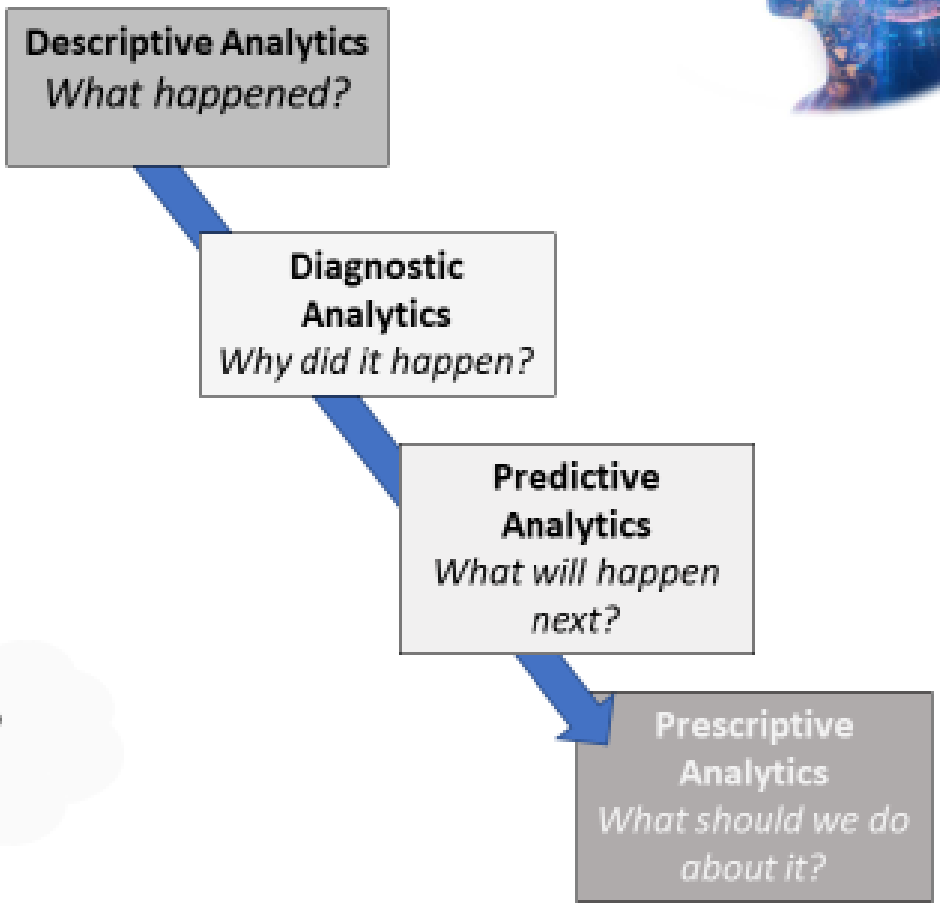
Tier 3: Asset-level data-driven analysis


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.

Digital Twin

CYBERTRUST

COMPUTER 0018-9162/20©2020IEEE
PUBLISHED BY THE IEEE COMPUTER SOCIETY SEPTEMBER 2020

Cybertrust: From Explainable to Actionable and Interpretable Artificial Intelligence

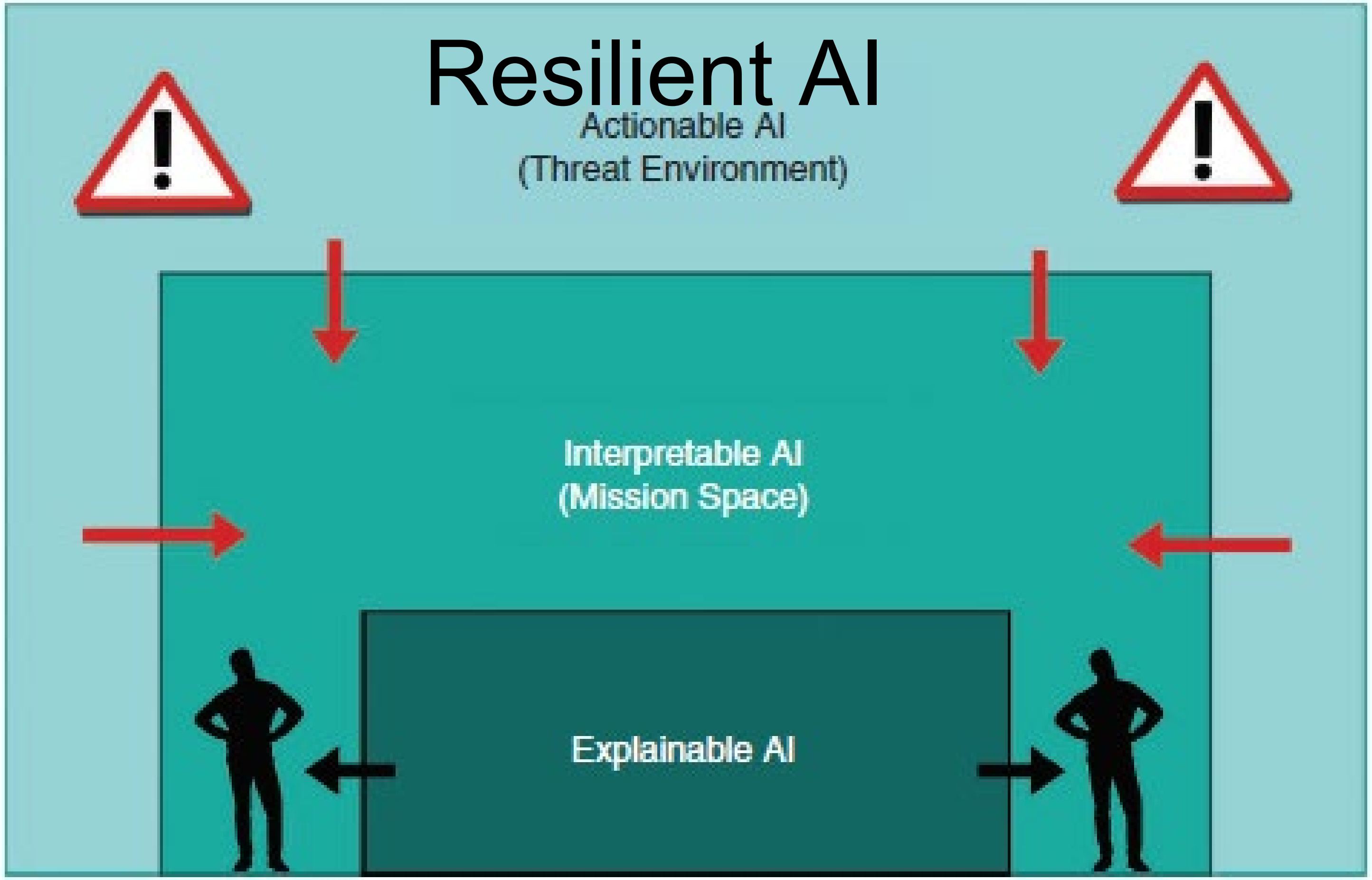
Igor Linkov, Stephanie Galaitsi, and Benjamin D. Trump, U.S. Army Corps of Engineers

Jeffrey M. Keisler, University of Massachusetts

Alexander Kott, U.S. Army Futures Command

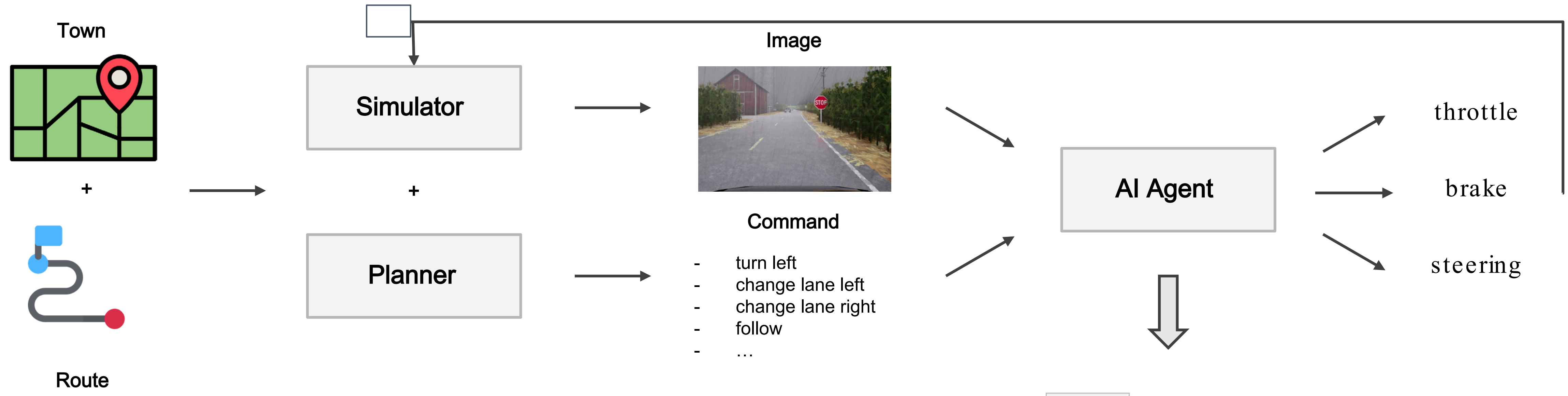
TABLE 1. The typology of human-AI assessments of decision strategy.

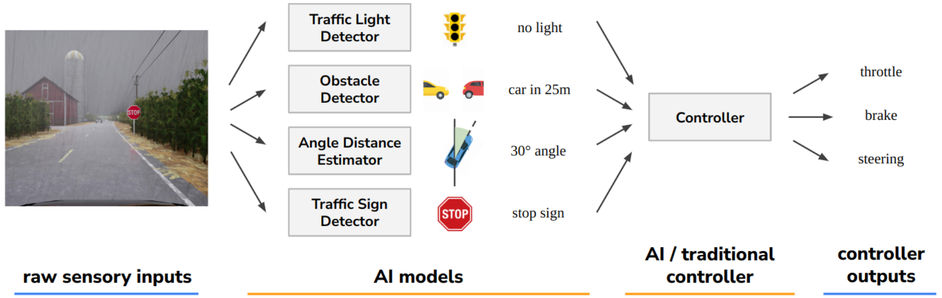
		AI	
		Yes	No
Human	Yes	Agreement	Disagreement
	No	Disagreement	Agreement



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





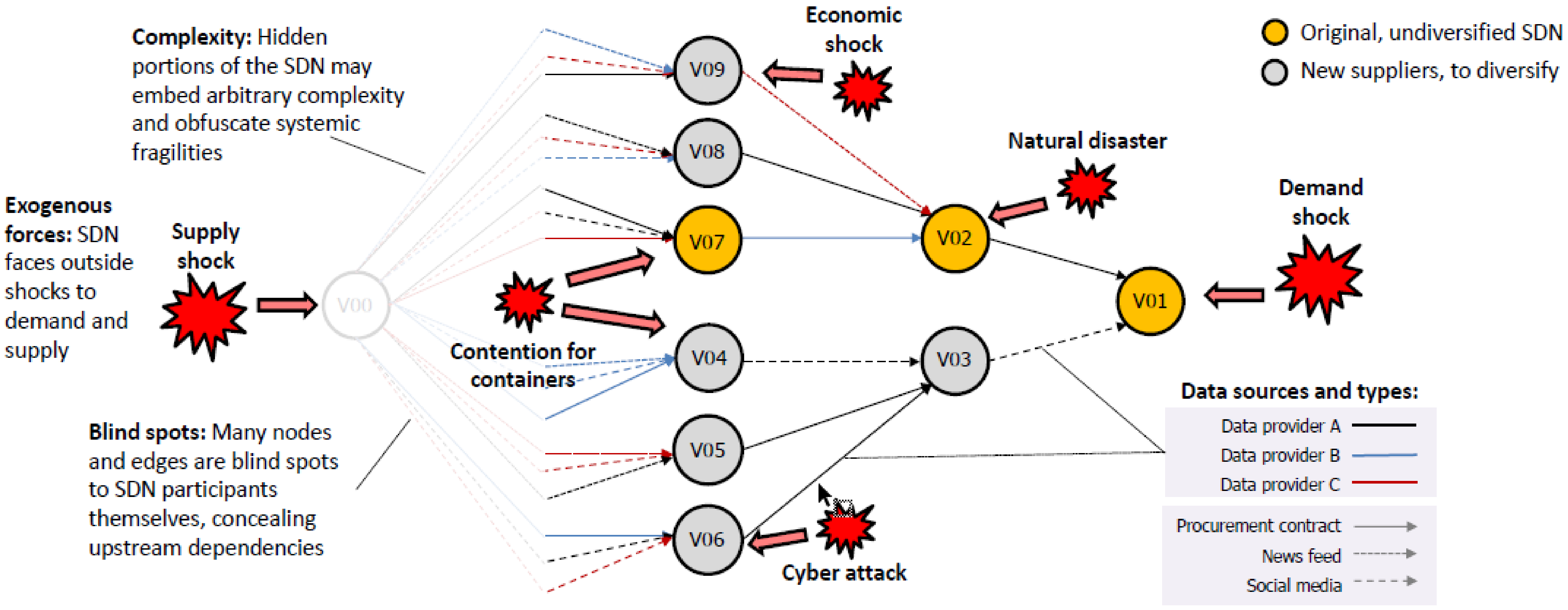
Disruption → image noise, image rotations, stickers, …

Efficiency → “**driving performance**” **System level property**

Resilience → change in “**driving performance**” relative to disruptions

Supply-and-Demand Networks – challenges

SDNs operate as engines for strategic surprise – many critical vulnerabilities emerge only at the system level

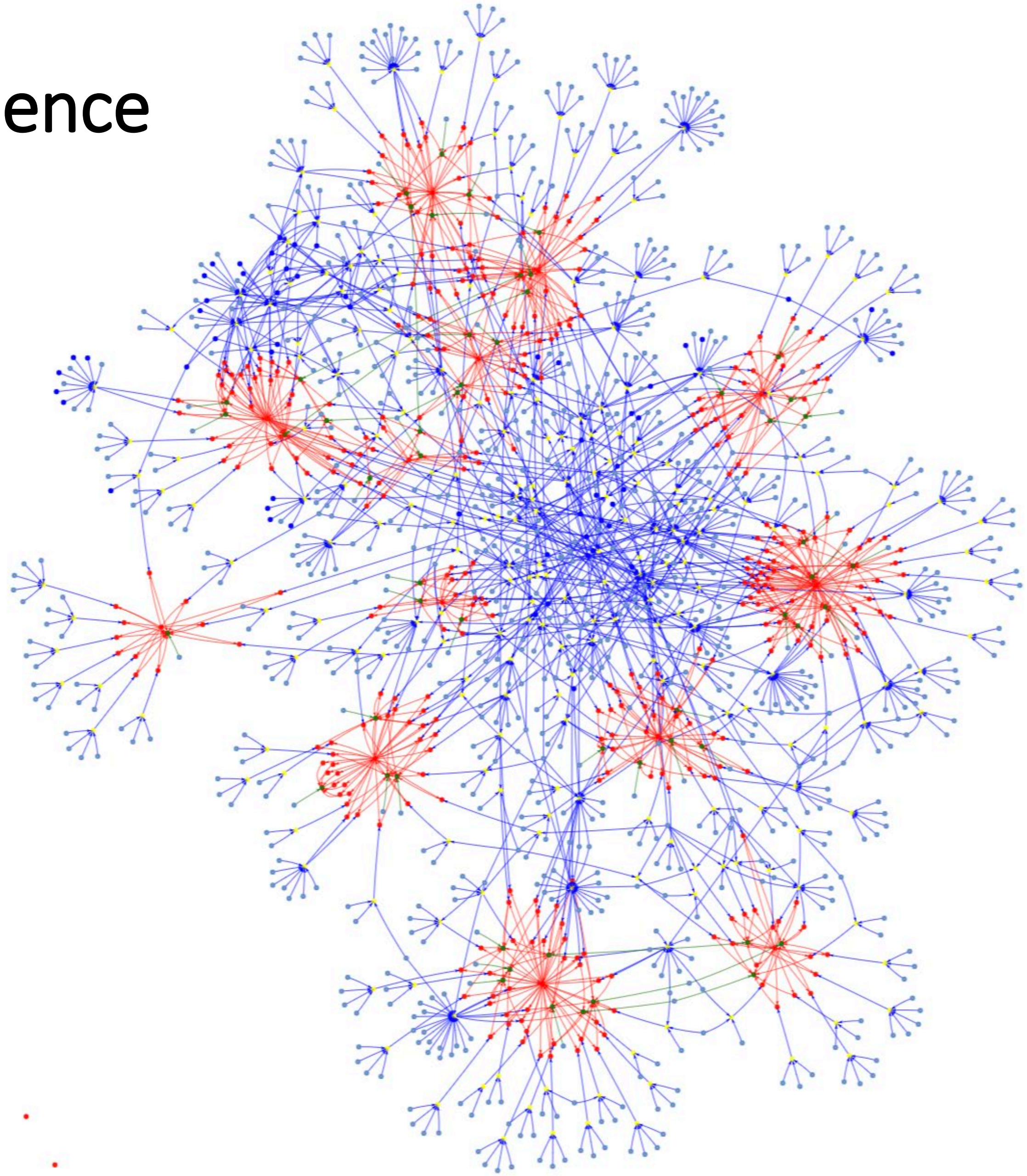


Generative AI and Resilience

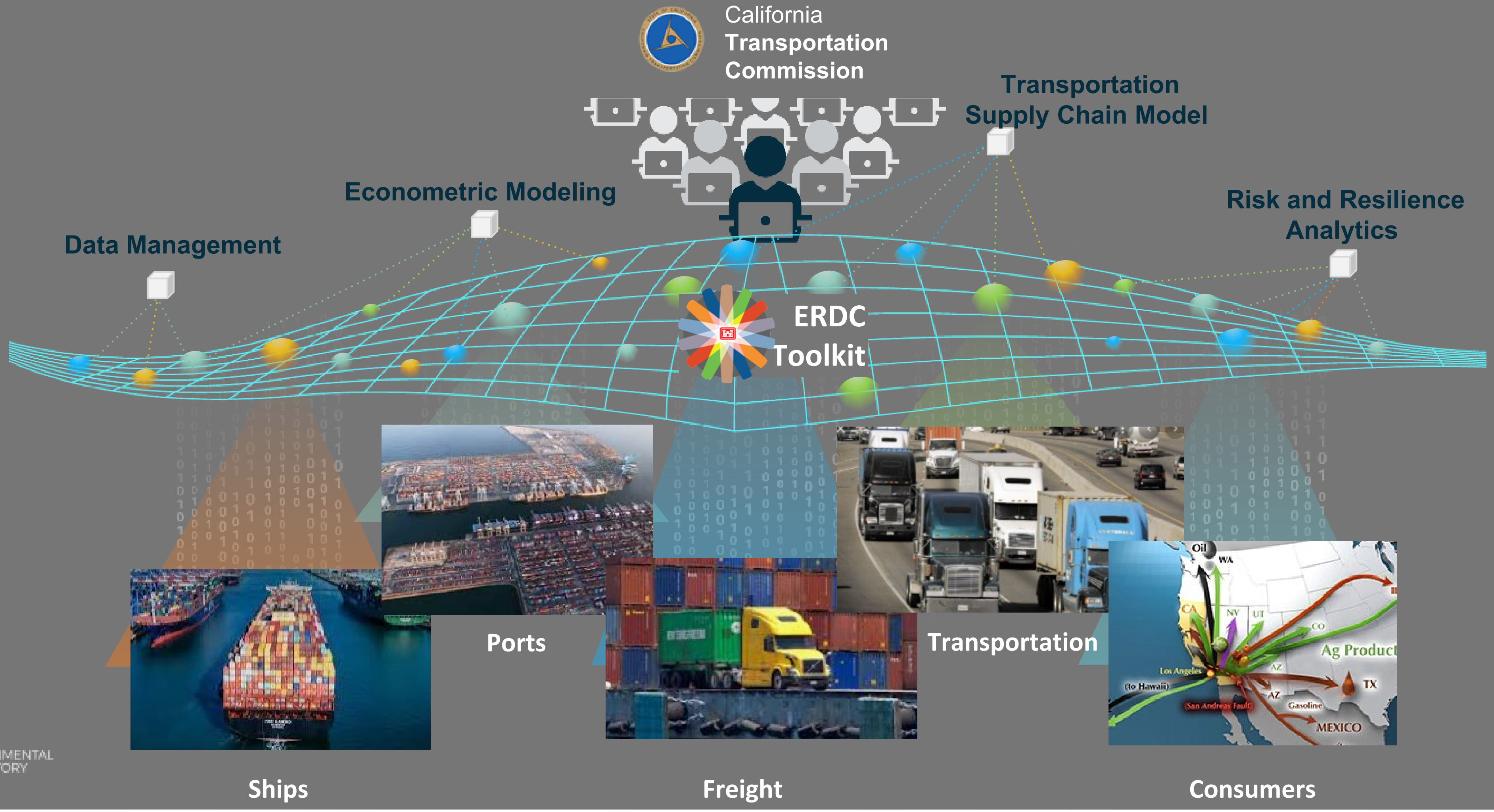
DARPA surrogate data to build supply demand network

Synthetic, plausible supply chain:

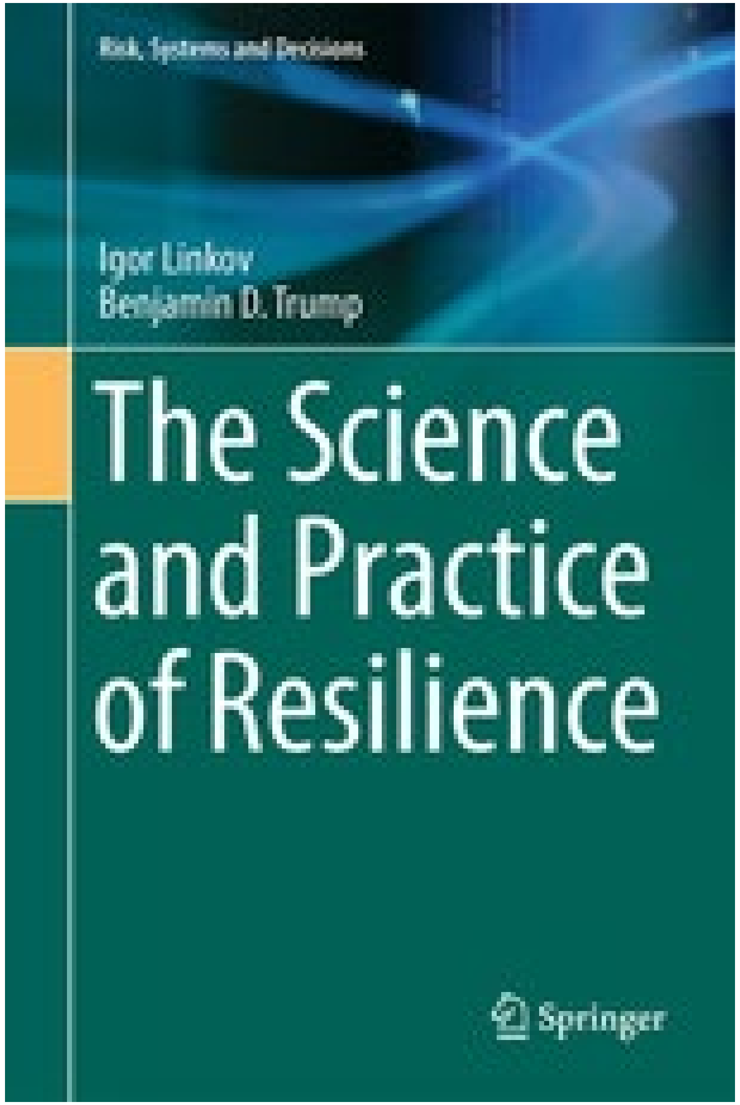
- Current DARPA surrogate SDN is limited in scope
- Leveraged *LLMs* to build out SDNs
- Demonstrates how LLMs can be used for imputation when data is unavailable

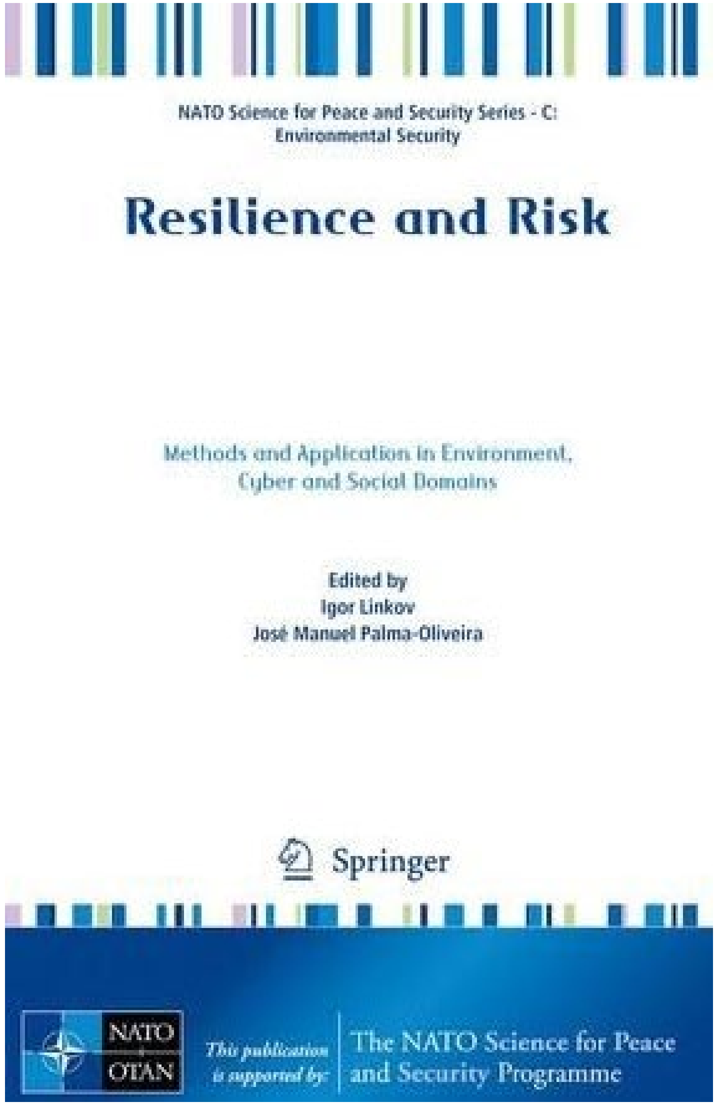


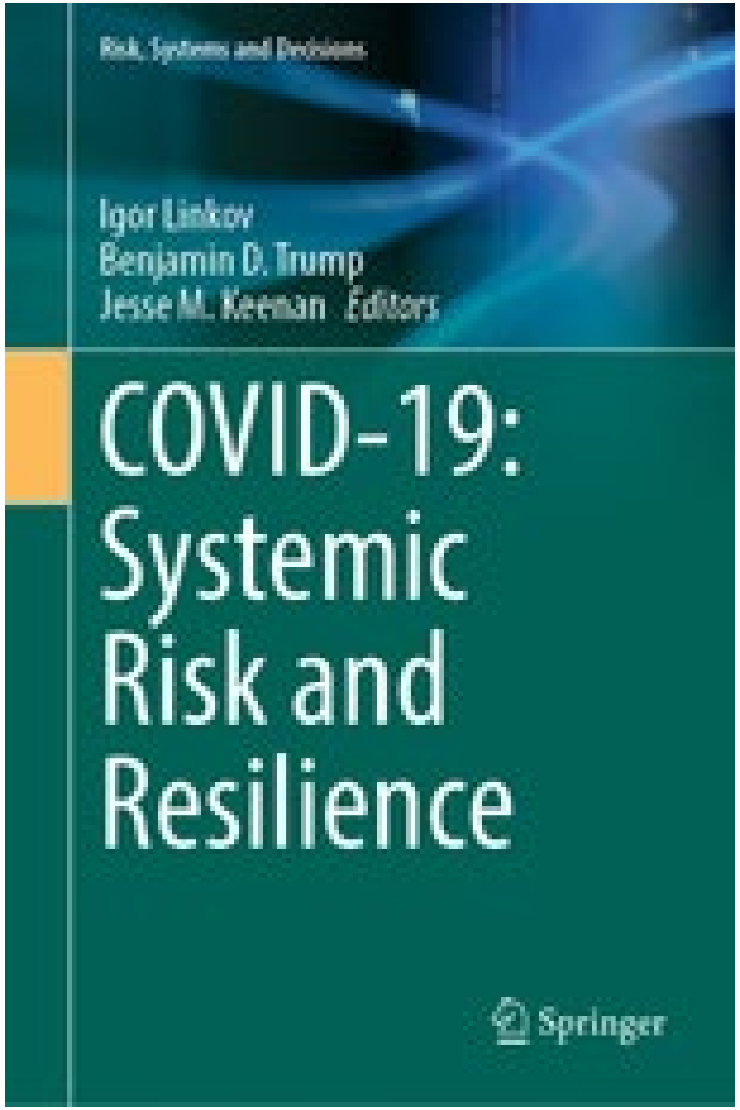
AI-Driven Resilience in CA Transportation Networks



EL 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