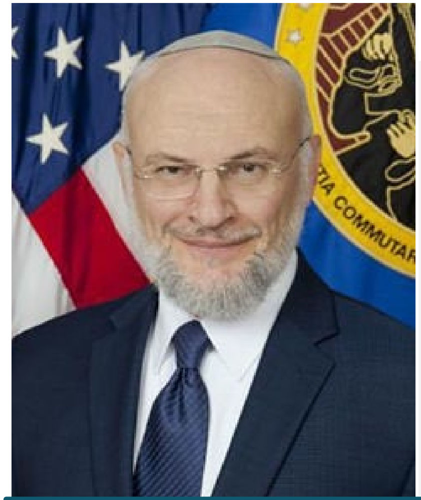
WELCOME



SERC Talks: “Cyber Resilience: Technical Concept or Vague Desiderata?”

April 6, 2022 | 1:00 PM ET

Dr. Alexander Kott | CONTACT

Chief Scientist, U.S. Army Research Laboratory; Army Senior Research Scientist (ST) for Cyber Resilience

CYBER RESILIENCE

- □ Today’s session will be recorded.
- □ An archive of today’s talk will be available at: www.sercuarc.org/serc-talks/ as well as on the SERC YouTube channel.
- □ Use the Q&A box to queue up questions, reserving the chat box for comments, and questions will be answered during the last 5-10 minutes of the session.
- □ If you are connected via the dial-in information only, please email questions or comments to SERCtalks@stevens.edu.
- □ Any issues? Use the chat feature for any technical difficulties or other comments, or email SERCtalks@stevens.edu.

SYSTEMS ENGINEERING RESEARCH CENTER

SERC TALKS

SERC Talks: "Cyber Resilience: Technical Concept or Vague Desiderata?"

SERC TALKS

Dr. Alexander Kott
Chief Scientist, U.S. Army Research Laboratory;
Army Senior Research Scientist (ST) for Cyber Resilience
U.S. Army

CYBER RESILIENCE

Dr. Peter Beling, SERC Research Council Member; Professor and Associate Director, Intelligent Systems Lab, Hume Center for National Security and Technology; Professor, Grado Department of Industrial and Systems Engineering at Virginia Tech

DISCLAIMER

The Systems Engineering Research Center (SERC) is a federally funded University Affiliated Research Center managed by Stevens Institute of Technology.

Any views, opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the United States Department of Defense, OUSD (R&E), nor the SERC.

No Warranty. This SERC - Stevens Institute of Technology Material is furnished on an “as-is” basis. SERC and Stevens Institute of Technology makes no warranties of any kind, either expressed or implied, as to any matter including, but not limited to, warranty of fitness for purpose or merchantability, exclusivity, or results obtained from use of the material. SERC and Stevens Institute of Technology does not make any warranty of any kind with respect to freedom from patent, trademark, or copyright infringement.

This material has been approved for public release and unlimited distribution.

U.S. ARMY COMBAT CAPABILITIES DEVELOPMENT COMMAND – ARMY RESEARCH LABORATORY

Cyber Resilience: a Technical Concept or Vague Desiderata?

Alexander Kott, PhD
Chief Scientist, ARL
ST, Cyber Resilience

6 April 2022

INTRODUCING MYSELF

2008-today:

- **Cyber resilience**
- **Cyber-physical, SCADA, IoT**
- **Cyber modeling and wargaming**
- **Autonomous Intelligent Agents in cyber warfare**
- **Technological forecasting**

Two current roles:

- **Chief Scientist of ARL**
- **ST for Cyber Resilience**

A FEW REFERENCES UPFRONT

- **A. Kott and I. Linkov, "To Improve Cyber Resilience, Measure It," in Computer, vol. 54, no. 2, pp. 80-85, Feb. 2021**

- **Kott, A., & Linkov, I. (Eds.). (2019). Cyber resilience of systems and networks (pp. 381-401). New York, NY: Springer International Publishing.**

Why Cyber Resilience?

Resilience vs Risk and Security

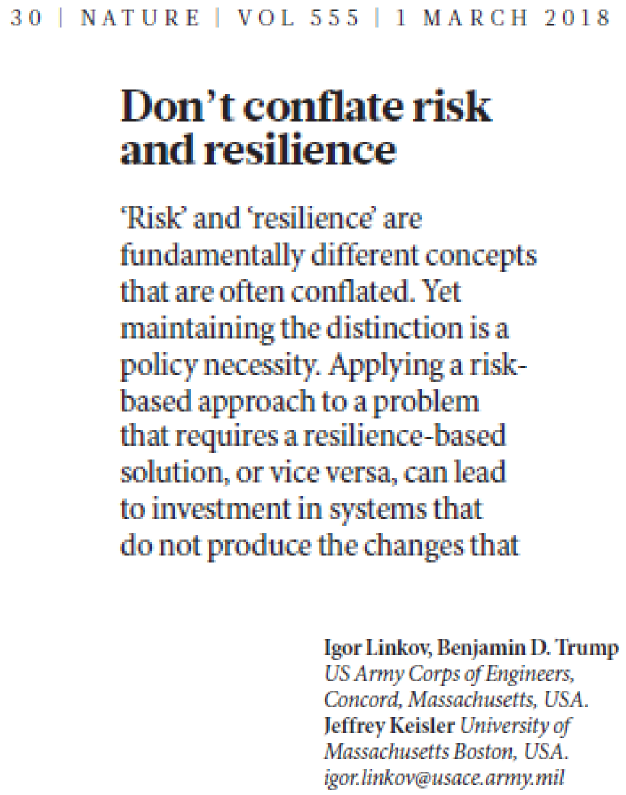
Risk -- “a situation involving exposure to danger [threat].”

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

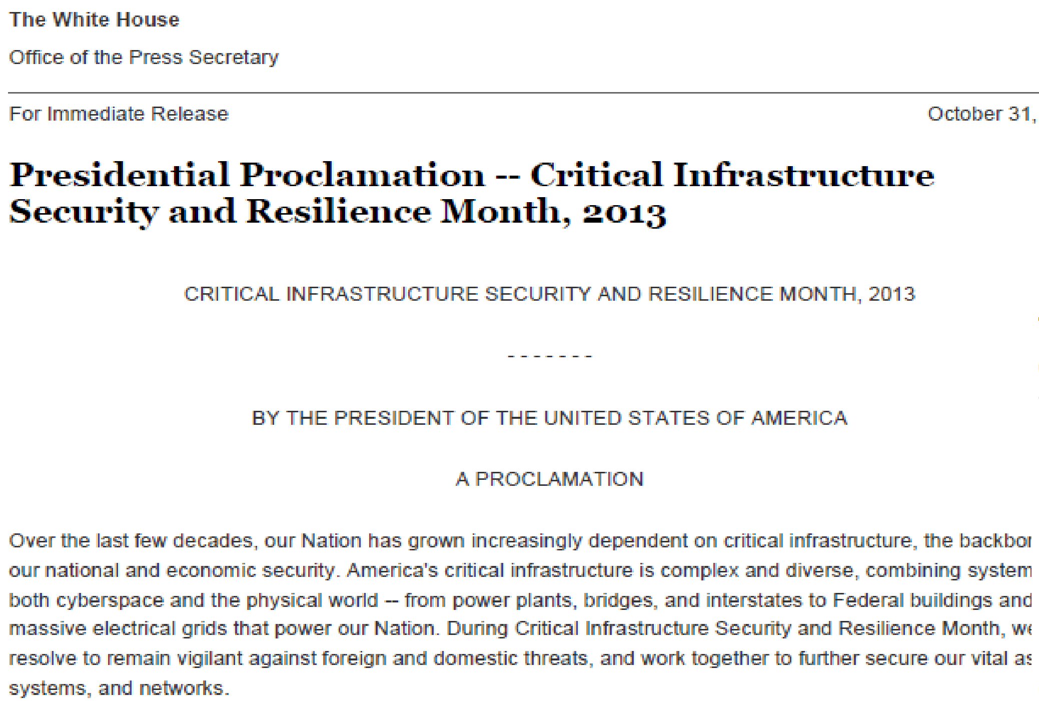
Courtesy of Dr. I. Linkov, Army ERDC

MANY DEFINITIONS OF CYBER RESILIENCE

- “The ability of systems to resist, absorb, and recover from or adapt to an adverse occurrence during operation….” [DoD 2014]
- Focus is on what happens after the compromise (“adverse occurrence”)
- Too often (misleadingly) used interchangeably with cyber security
- Cyber survivability is closely related to cyber resilience (worth separate discussion)

Calls for Resilience

“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 October 31, 2013

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

CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE MONTH, 2013

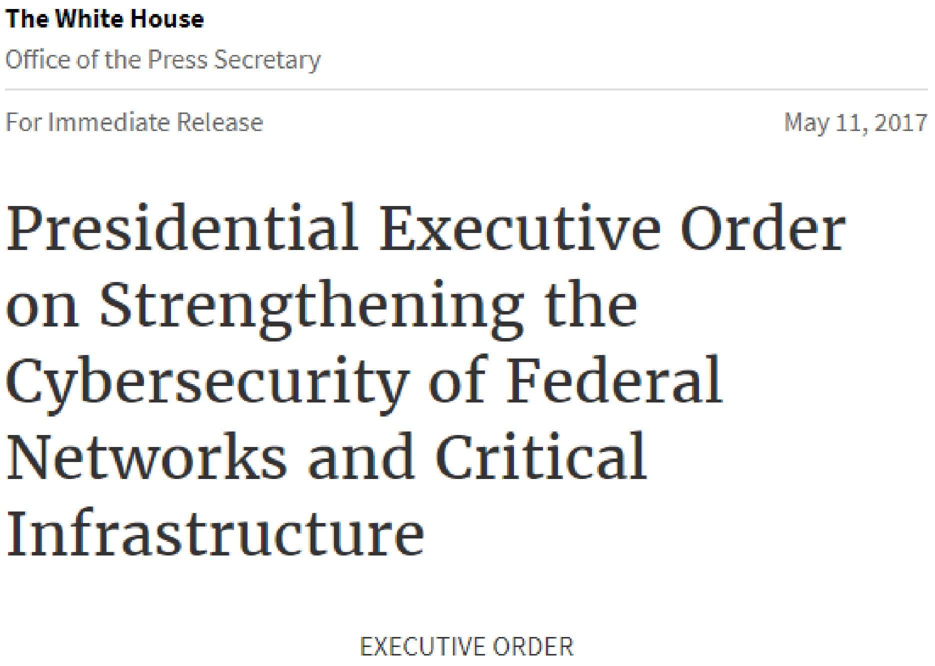
- - - - - - -

BY THE PRESIDENT OF THE UNITED STATES OF AMERICA

A PROCLAMATION

Over the last few decades, our Nation has grown increasingly dependent on critical infrastructure, the backbor our national and economic security. America's critical infrastructure is complex and diverse, combining system both cyberspace and the physical world -- from power plants, bridges, and interstates to Federal buildings and massive electrical grids that power our Nation. During Critical Infrastructure Security and Resilience Month, we resolve to remain vigilant against foreign and domestic threats, and work together to further secure our vital as 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**.



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

Courtesy of Dr. I. Linkov, Army ERDC

FOCUSING THE SCOPE

- **Focus on tactical mobile assets: autonomous assets, manned platforms, networks of mobile formations, forward command posts**

- **Relatively disadvantaged assets: partly dated, COTS-based, modest SWAP**

- **Close proximity to adversarial elements –> ease of access, penetration**

- **Probability of physical capture by the adversary**

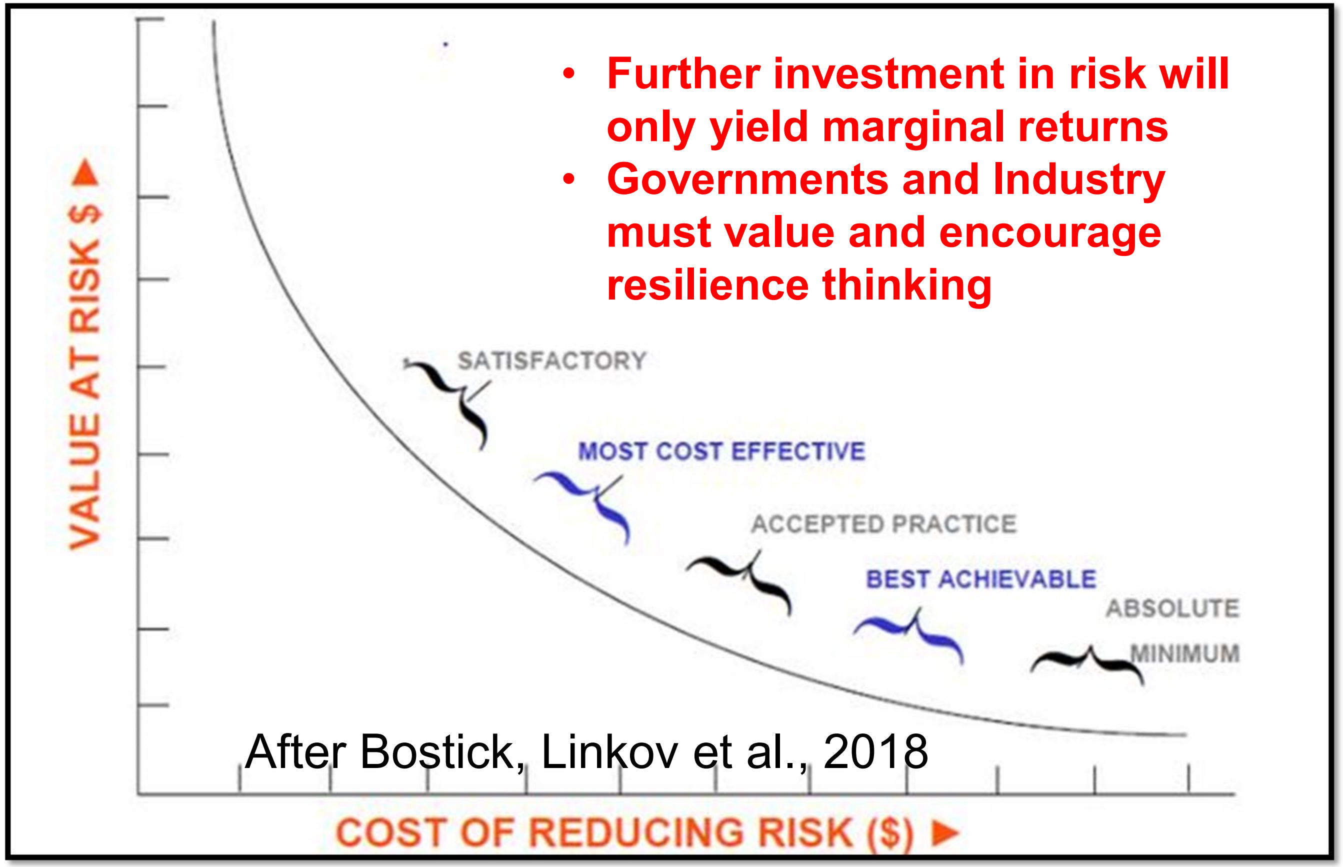
- **Lack of local, on-board cyber defenders**

- **Highly contested networking, intermittent connectivity, need to avoid emissions -> lack of centralized monitoring and response**

IN THIS CONTEXT, CYBER RESILIENCE IS ESPECIALLY IMPORTANT

- **Likelihood of compromise is significant**
- **Taking a (partly) compromised system out of the fight is often not an option**
- **Recovery by on-board personnel is unlikely**
- **Many assets are unmanned – no on-board personnel**
- **Remote monitoring and recovery is constrained by contested comms**
- **Built-in autonomous defense and recovery is critical**

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

Courtesy of Dr. I. Linkov, Army ERDC

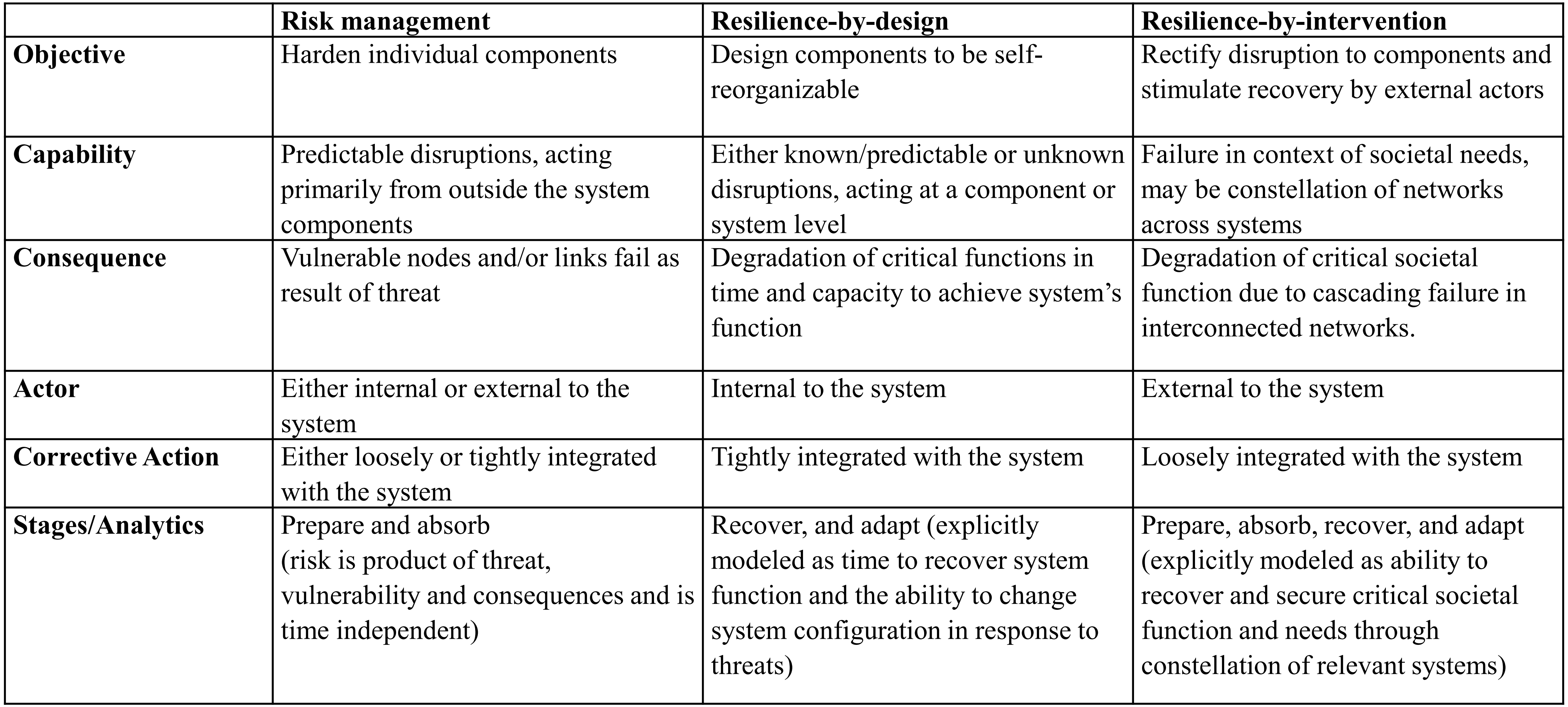
ACHIEVING RESILIENCE: AN EMERGING DIFFERENTIATION

- **“Resilience by Design (RBD” is a rising term.**
- **Other kinds of resilience? Resilience by Intervention (RBI)**
- **Two dimensions: integration and authority**
- **RBD:**
  - Tight integration
  - Internal authority
  - Example: vehicle protected by on-board autonomous resilience agent
  - Advantage: immediate response, even when external access is impeded
  - Disadvantage: additional capabilities not available if needed

- **RBI:**
  - External agent, not inherent to the system
  - External authority
  - Example: vehicle protected by external monitoring and response center
  - Advantage: effective and modulated use of resources
  - Disadvantage: response may be delayed, especially if access is impeded

Kott, A., Golan, M. S., Trump, B. D., & Linkov, I. (2021). Cyber Resilience: by Design or by Intervention?. *Computer*, *54*(8), 112-117.
Ligo, A. K., Kott, A., & Linkov, I. (2021). Autonomous Cyberdefense Introduces Risk: Can We Manage the Risk?. *Computer*, *54*(10), 106-110.

Comparison of risk management approaches (i.e., cybersecurity), RbD and RbI for cyber systems



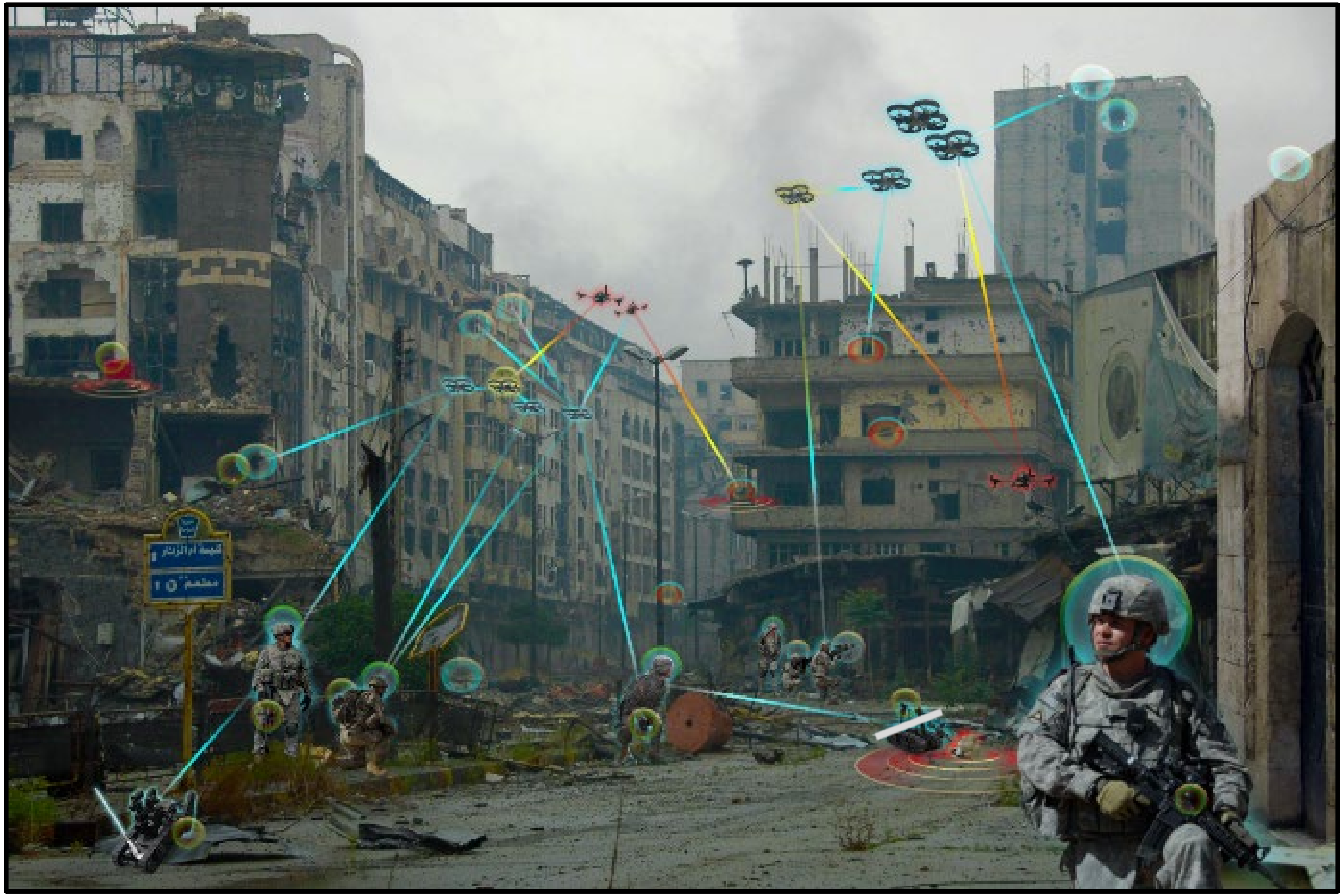
	Risk management	**Resilience-by-design**	**Resilience-by-intervention**
Objective	Harden individual components	Design components to be self-reorganizable	Rectify disruption to components and stimulate recovery by external actors
Capability	Predictable disruptions, acting primarily from outside the system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

After Kott, A.
et al. 2021

Courtesy of Dr. I. Linkov, Army ERDC

Autonomous Intelligent Agents for Cyber Resilience

A WORLD OF UBIQUITOUS AGENTS

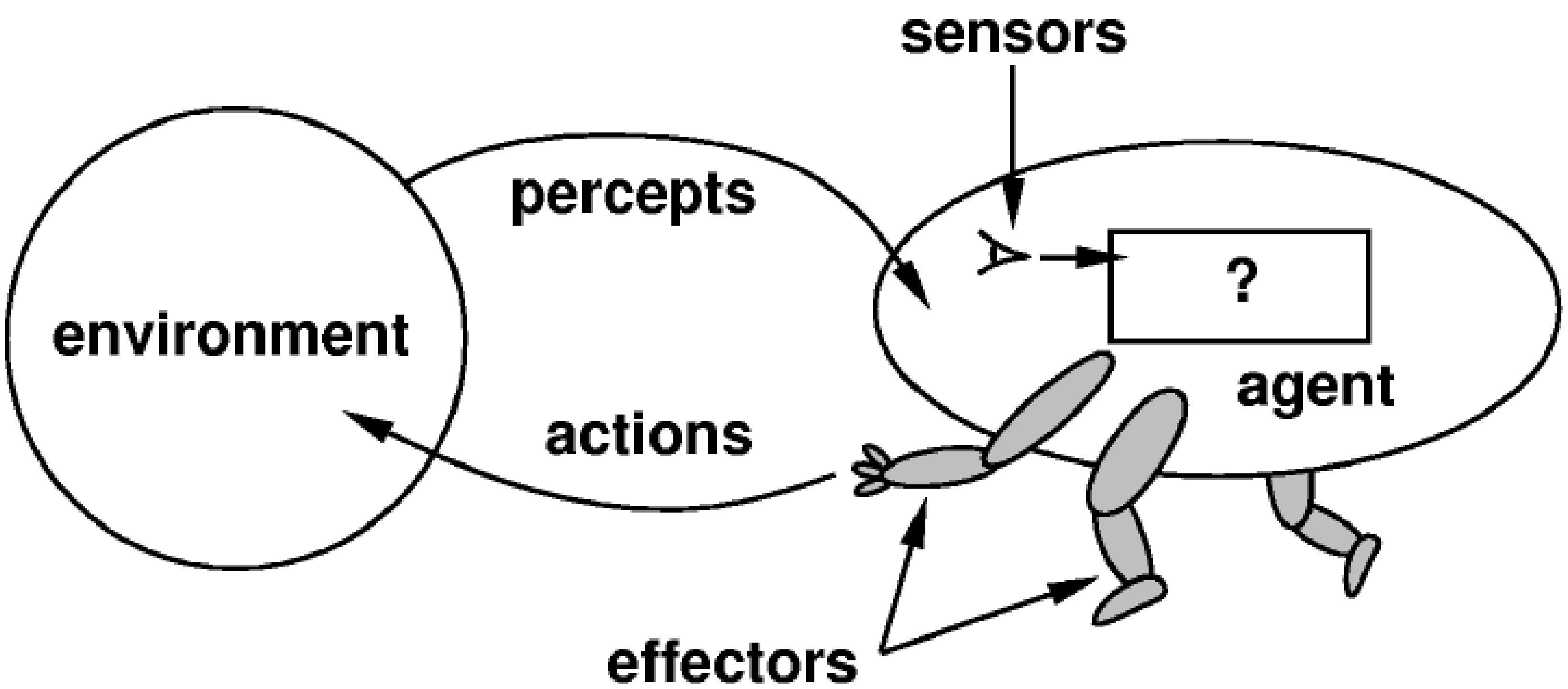


MOTIVATION FOR AUTONOMOUS INTELLIGENT CYBER-DEFENSE AGENTS

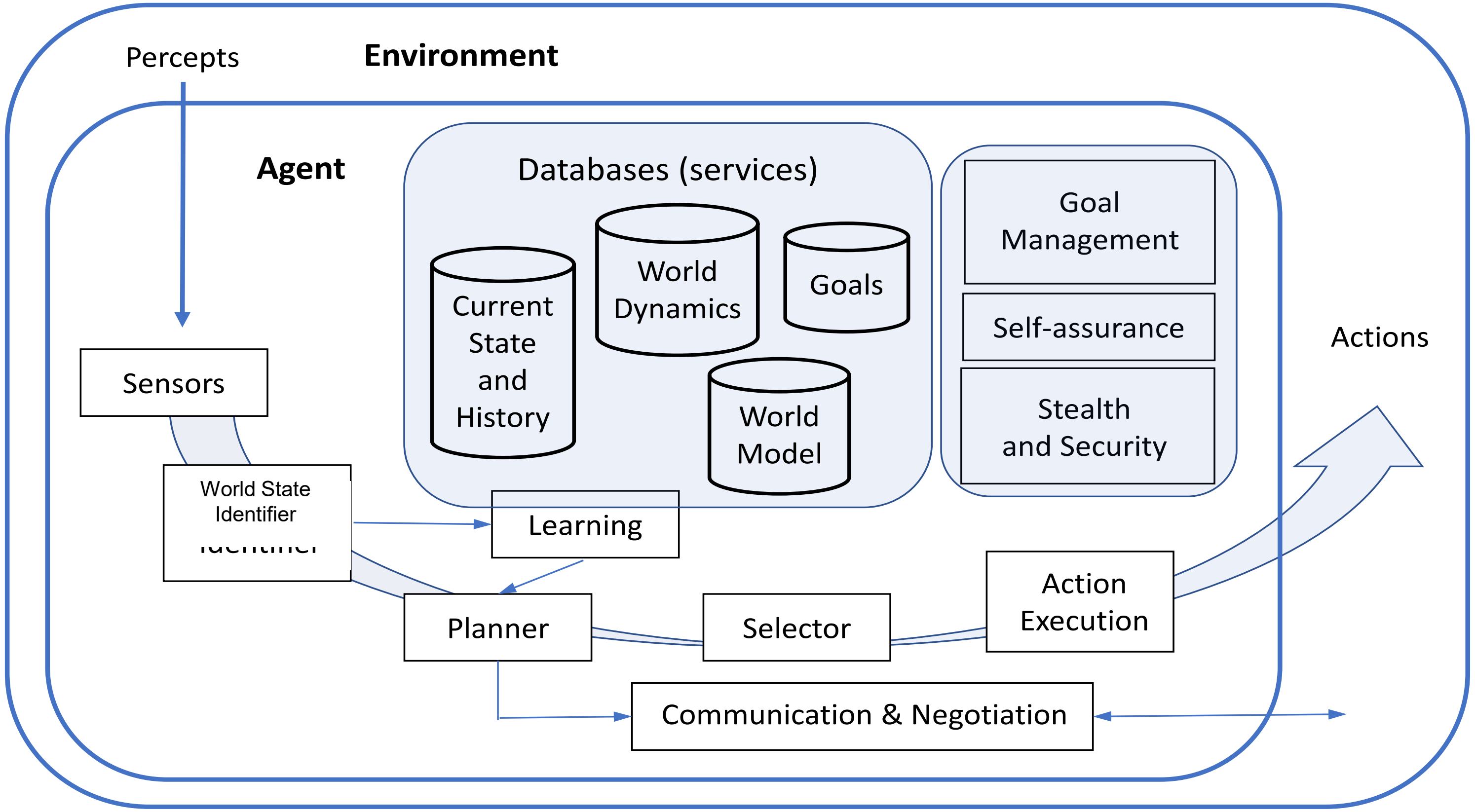
- **Growing focus on AI, autonomy, and issues of human trust in AI**
- **Cyber is exceptionally ripe for strong AI; autonomous yet human-managed agents for cyber operation**
- **Malware is growing in autonomy and sophistication**
- **Current manual and semi-manual approaches grossly inadequate**
- **Needed are autonomous agents that:**
  - actively and stealthily patrol the friendly network
  - detect and react to hostile activities far faster than human reaction time
  - detect the enemy agents while remaining concealed,
  - destroy or degrade the enemy agents (malware)
  - do so mostly autonomously, without support or guidance of a human expert

Kott, A., & Theron, P. (2020). Doers, not watchers: Intelligent autonomous agents are a path to cyber resilience. IEEE Security & Privacy, 18(3), 62-66

GENERALIZED INTELLIGENT AGENT



AUTONOMOUS AGENT FIGHTING FOR RESILIENCE



- Complex planning
- Responses and ramifications
- Stealthy execution

Kott, A. and Theron, P., 2020. Doers, Not Watchers: Intelligent Autonomous Agents Are a Path to Cyber Resilience. *IEEE Security & Privacy*, *18*(3), pp.62-66

A working group and a conference: https://www.aica2021.org/

LIMITED CONTROL

- **Provisions are made to enable a remote or local human controller to observe, direct and modify the actions of the agent.**

- **However, human control is often impossible.**

- **The agent has to plan, analyze and perform most or all of its actions autonomously.**

- **Provisions are made for the agent to collaborate with other agents**

- **However, when the communications are impaired or observed by the enemy, the agent operates alone.**

ACCEPTANCE AND MANAGEMENT OF RISK

The concept of AICA always raises questions regarding the risks of cyber autonomy. The agent has to take destructive actions, such as deleting or quarantining certain software, autonomously.

- **We can mitigate some risks, to an extent,**
  - destructive actions are controlled by the rules of engagement,
  - allowed only on the computer where the agent resides.
- **We have to accept the residual risks because alternatives are even worse**
  - in general, actions cannot be guaranteed to preserve availability or integrity of the functions and data of friendly computers.
  - this risk, in a military environment, has to be balanced against the death or destruction caused by the enemy if the agent’s action is not taken.

Ligo, A. K., Kott, A., & Linkov, I. (2021). Autonomous Cyberdefense Introduces Risk: Can We Manage the Risk?. *Computer*, *54*(10), 106-110.

WHERE WE ARE: AUTONOMOUS AGENTS FOR CYBER RESILIENCE

- **Autonomous intelligent cyber-defense agents are a promising class**
- **S&T organizations pursue various approaches to autonomous cyber agents**
- **Growing body of technical literature**
- **Initial architectural recommendations**
- **International NATO-focused working group, https://www.aica-iwg.org/**
- **Tri-Service Tech Exchange on Autonomous Cyber Defense**

Please do contact me: alexander.kott1.civ@army.mil

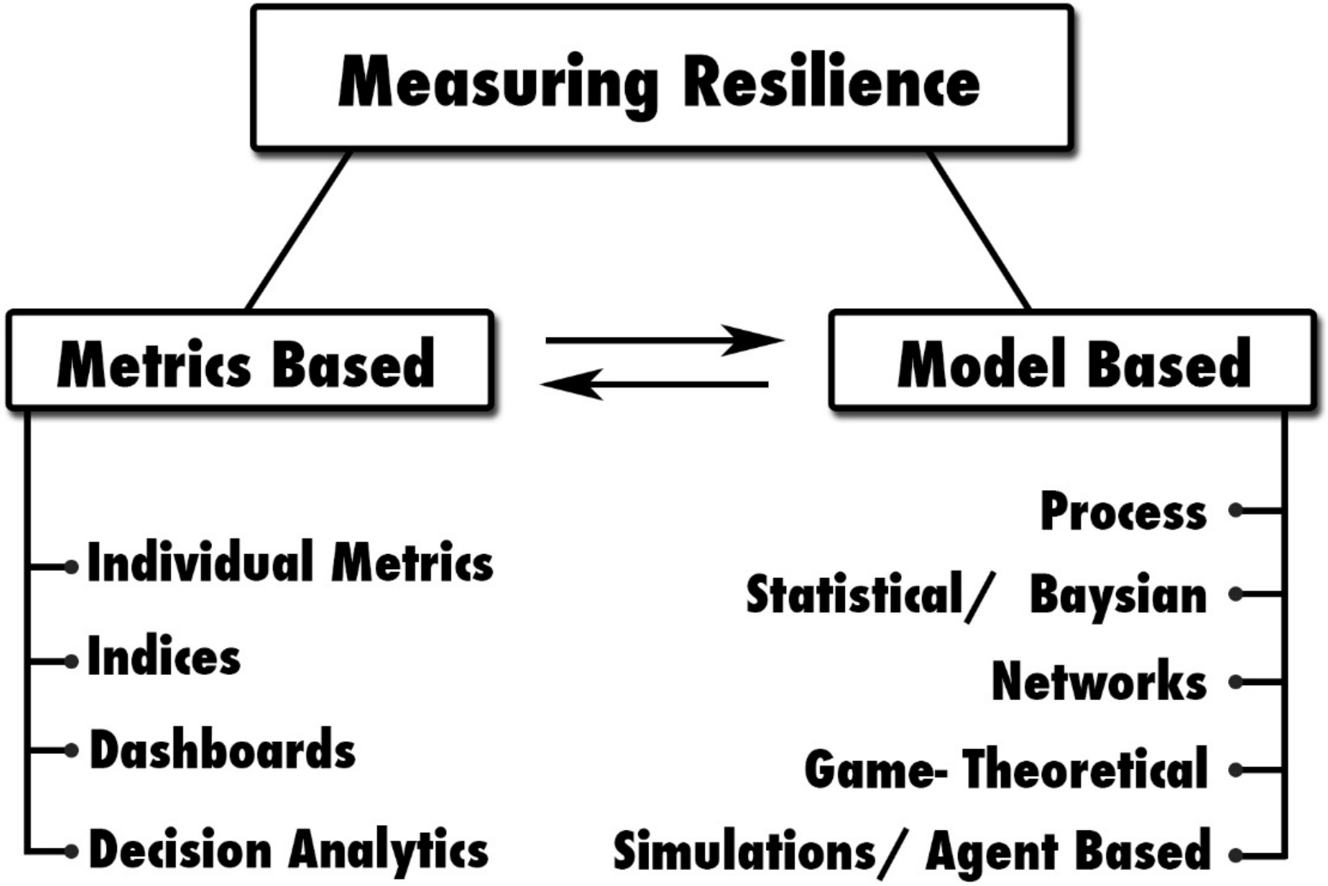
Kott, A., & Theron, P. (2020). Doers, not watchers: Intelligent autonomous agents are a path to cyber resilience. IEEE Security & Privacy, 18(3), 62-66

How Good is Your Cyber Resilience

WHY MEASURE CYBER RESILIENCE?

- You cannot improve what you cannot measure
- All sciences and engineering blossomed only when measurements tools appeared
- Analogy: indicator diagram. James Watt found it so important for development of steam engines, it so crucial to improving his steam engines, he kept it secret
- We need tools for measuring cyber resilience: rigorous, repeatable, and statistically meaningful
- Red teams and qualitative assessments are important. But no substitute for high throughput automated testing, for multiple operational and threat scenarios
- Growing number of cyber defense features and mechanism increase uncertainty of their efficacy – they might decrease resilience, not increase

How to Quantify Resilience?



Measuring Resilience

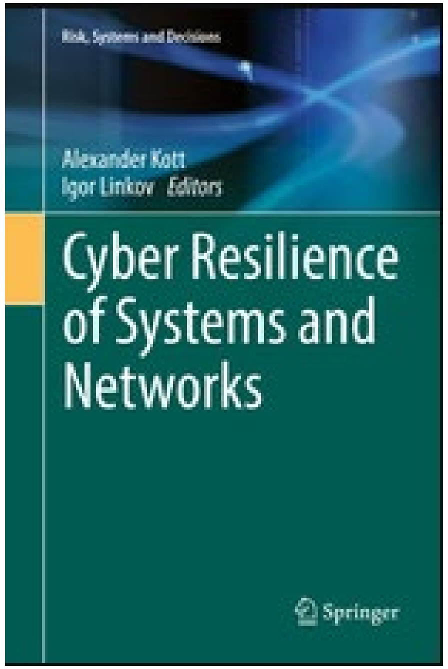
Metrics Based

- Individual Metrics
- Indices
- Dashboards
- Decision Analytics

Model Based

- Process
- Statistical/ Baysian
- Networks
- Game- Theoretical
- Simulations/ Agent Based

Kott, A., & Linkov, I. (Eds.). (2019). *Cyber resilience of systems and networks* (pp. 381-401). New York, NY: Springer International Publishing.



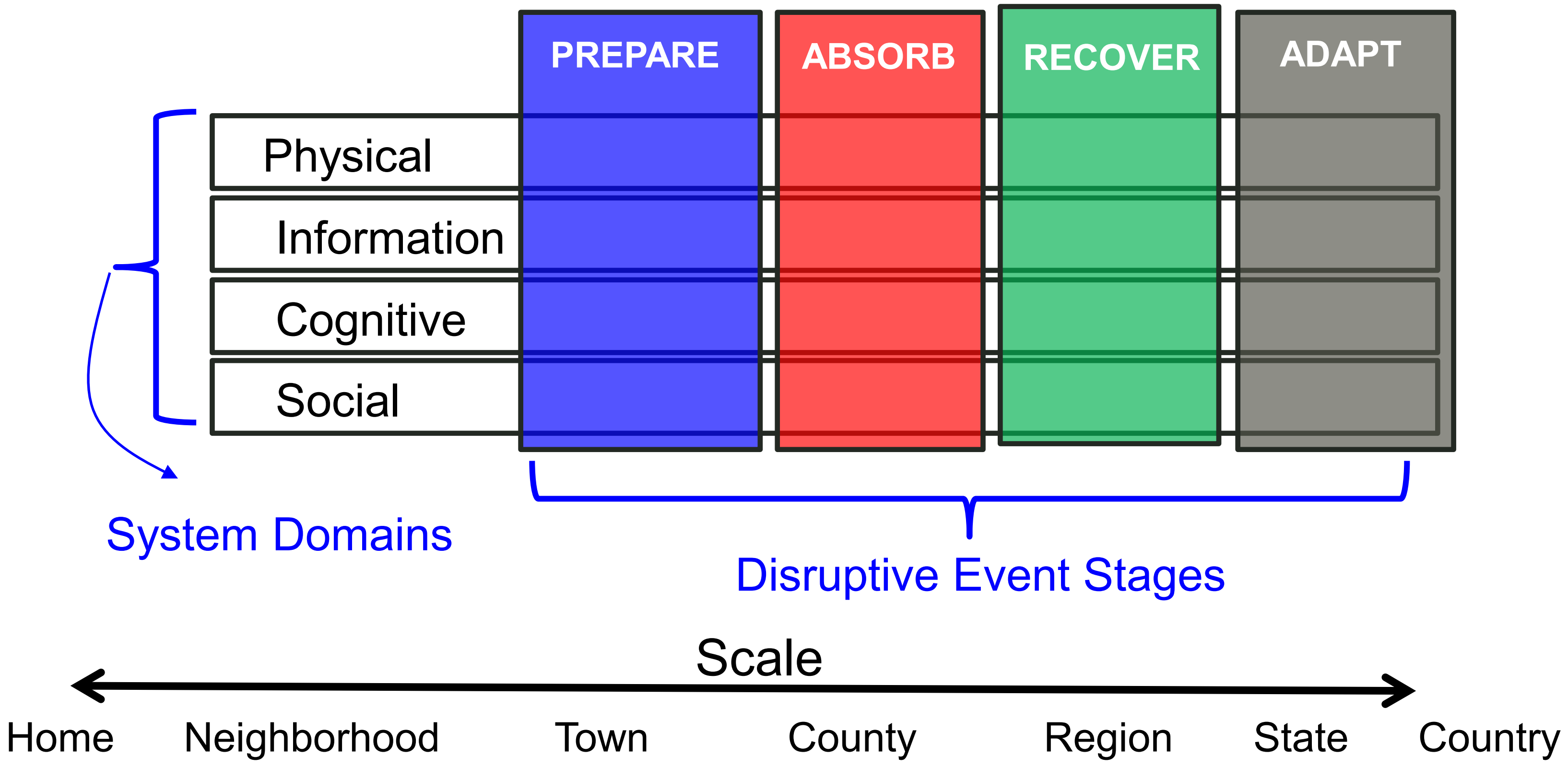
Risk, Systems and Decisions

Alexander Kott
Igor Linkov *Editors*

Cyber Resilience of Systems and Networks

Springer

Resilience Matrix



PREPARE

ABSORB

RECOVER

ADAPT

Physical

Information

Cognitive

Social

System Domains

Disruptive Event Stages

Scale

Home

Neighborhood

Town

County

Region

State

Country

Courtesy of Dr. I. Linkov, Army ERDC

RESILIENCE MATRIX: CYBER

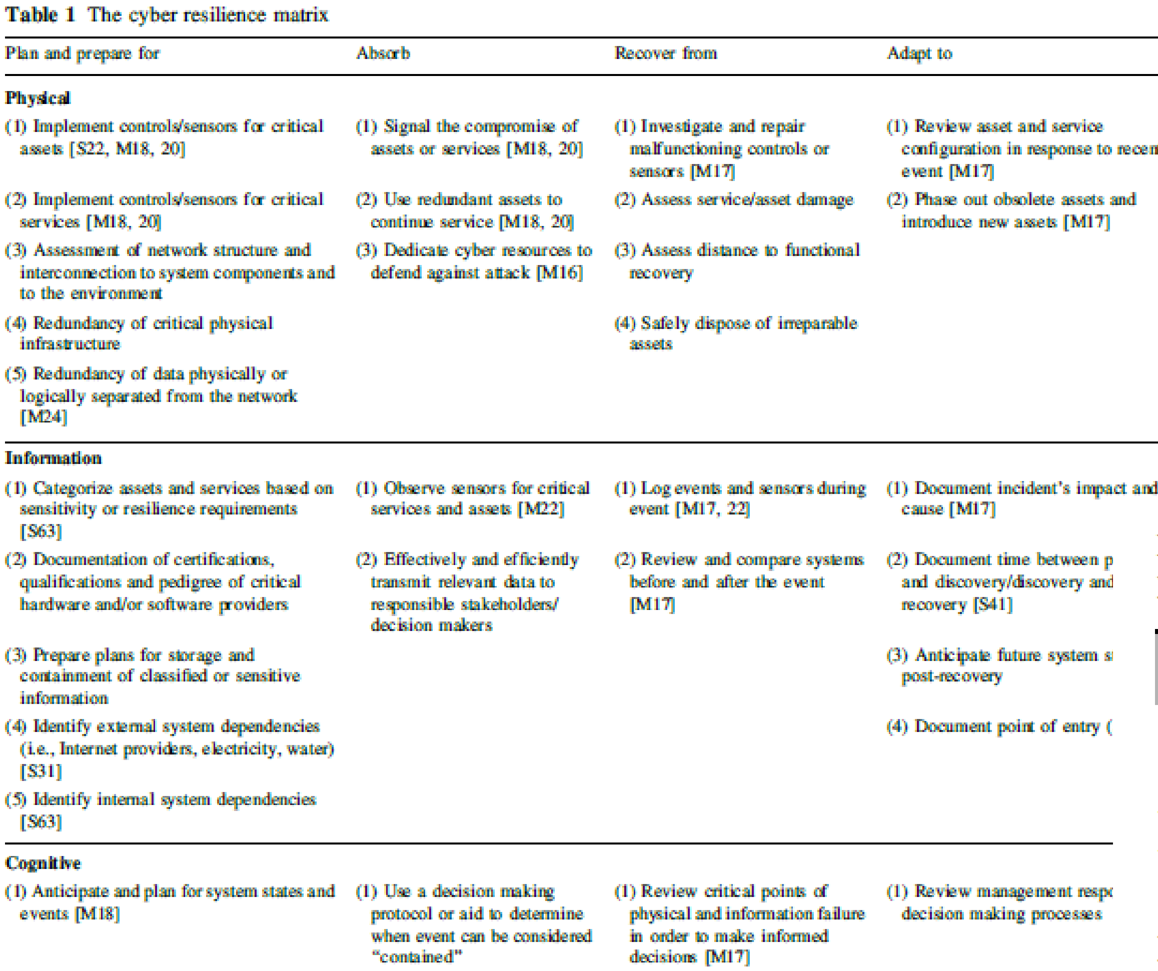
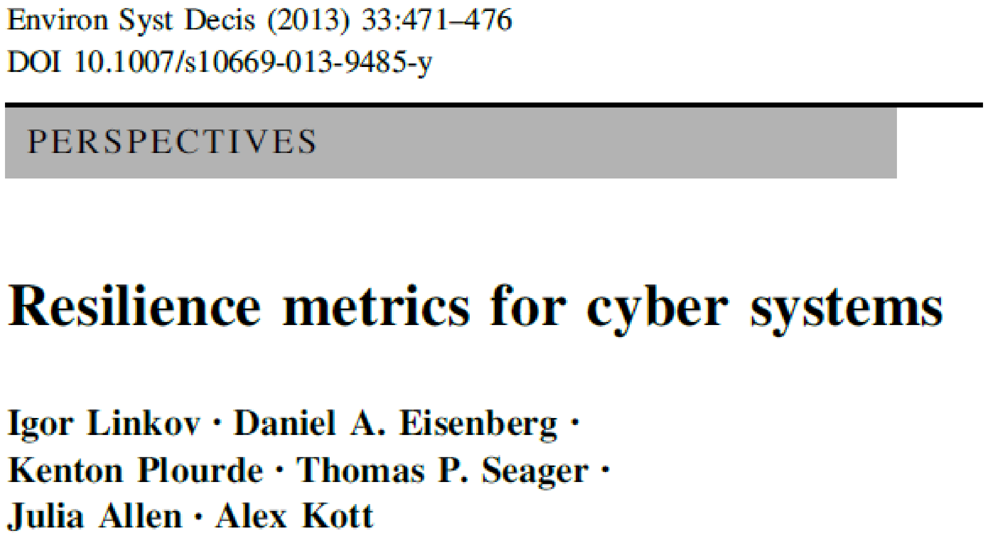


Table 1 The cyber resilience matrix

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 p and discovery/discovery and recovery [S41]
(3) Prepare plans for storage and containment of classified or sensitive information			(3) Anticipate future system s post-recovery
(4) Identify external system dependencies (i.e., Internet providers, electricity, water) [S31]			(4) Document point of entry (
(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 critical points of physical and information failure in order to make informed decisions [M17]	(1) Review management respo decision making processes



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

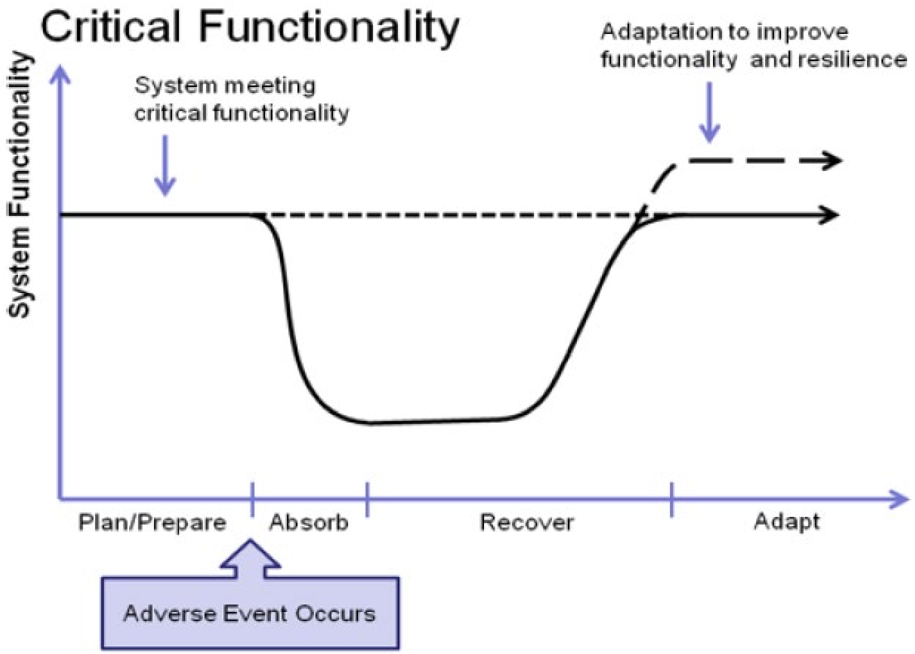
PERSPECTIVES

Resilience metrics for cyber systems

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

ONE COMMON IDEA – "AREA UNDER THE CURVE"

- **Focuses on cumulative loss of functionality, capability, productivity, etc.**
- **Explored since 1980s**
- **In multiple domains: ecology, biology, sociology, psychology, urban planning…**

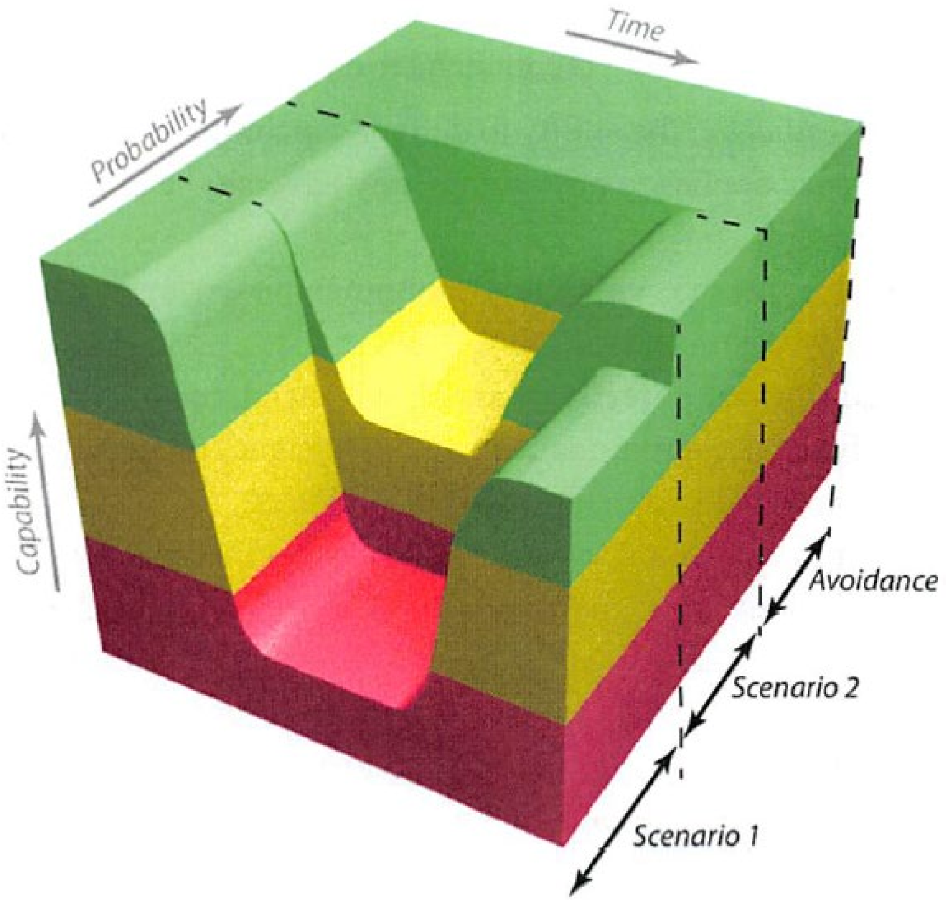


Hosseini, S., Barker, K., & Ramirez-Marquez, J. E. (2016). A review of definitions and measures of system resilience. Reliability Engineering & System Safety, 145, 47-61.

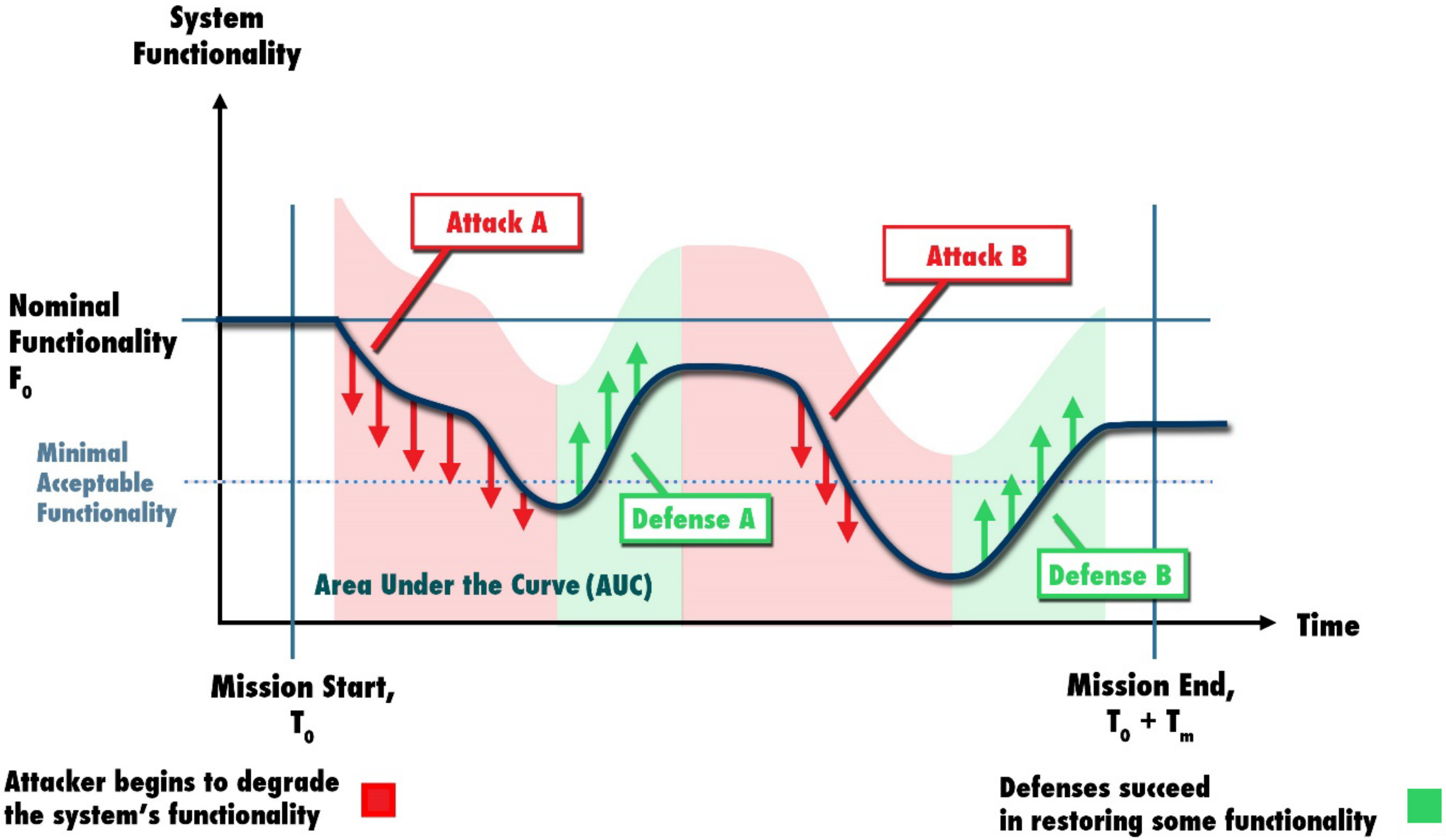
MANY VARIATIONS ON THE MAIN IDEA

"We evaluated 23 candidate metrics against 19 evaluation criteria. From this analysis we conclude that the best single metric for resiliency in the expected availability of the required capability."

J. S. Brtis, "How to think about resilience in a DoD context," MITRE CORP, Colorado Springs (CO), 2016.



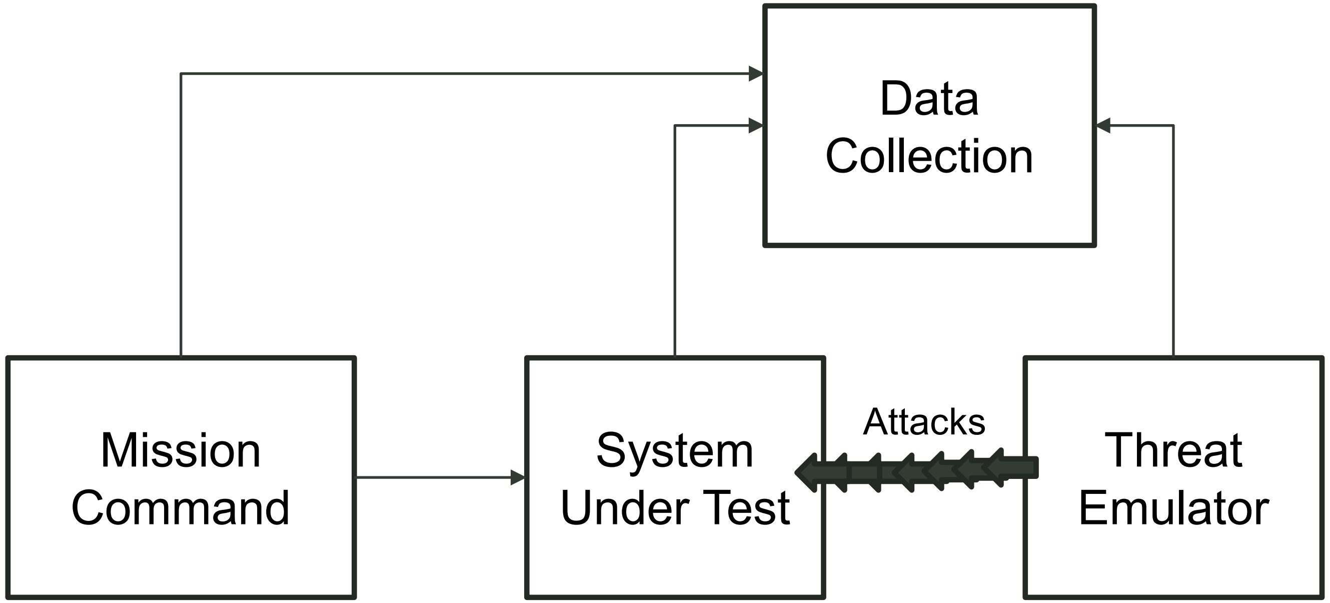
CONTINUOUS ATTACK AND DEFENSE



A. Kott and I. Linkov, "To Improve Cyber Resilience, Measure It," in *Computer*, vol. 54, no. 2, pp. 80-85, Feb. 2021

HOW THE MEASURING MIGHT BE DONE?

- **Execute a representative mission (e.g., 30min duration recon)**
- **Apply cyber "pressure" via an Automated Red Team**
- **Record mission functionality over time**
- **Repeat N times (e.g., 10), suitably randomized**
- **Compute the resilience (single number or statistical distribution, TBD)**



ALL MEASURES HAVE DEFICIENCIES AND CONCERNS

- Qualitative assessments [e.g., I. Linkov, D. A. Eisenberg, K. Plourde, T. P. Seager, J. Allen, and A. Kott, "Resilience metrics for cyber systems," Environ. Syst. Decis., vol. 33, no. 4, pp. 471–476, 2013.]. Concerns: subjectivity, inconsistency
- Probabilistic expert estimates [e.g., D. W. Hubbard and R. Seiersen, How to Measure Anything in Cybersecurity Risk. Hoboken, NJ, USA: Wiley, 2016]. Concerns: subjectivity, inconsistency
- Modeling / Simulation [e.g., A. Kott, J. Ludwig, and M. Lange, "Assessing mission impact of cyberattacks: Toward a model-driven paradigm," IEEE Secur. Privacy, vol. 15, no. 5, pp. 65–74, Jan. 2017.] Concerns: expensive, difficult validation, limited coverage
- Wargaming [e.g., E. J. M. Colbert, A. Kott, and L. P. Knachel, "The game-theoretic model and experimental investigation of cyber wargaming," J. Def. Model. Simul., vol. 17, no. 1, pp. 21–38, 2020.]. Concerns: subjectivity, expense, repeatability.
- Red Teaming, Pen-Testing. Concerns: expense, repeatability, consistency
- "Basic AUC". Concerns: defining functionality, capability; temporal changes in functionality; temporal changes in attacks
- AUC w/ Mission Accomplishment. Concerns: defining mission accomplishment.
- AUC w/ Adversary Effort instead of Time. Concerns: measuring adversary effort.

RESEARCH QUESTIONS – IS THIS A GOOD MEASURE?

- **Repeatability: for a given system and measurement tools, do repeated series of measurements yield approximately the same value of resilience?**

- **Consistency with respect to missions: do similar (but not identical) missions yield reasonably similar values of the resilience quantity?**

- **Monotonicity with respect to defenses: do significantly stronger on-board cyber-defenses yield a higher value of *R*?**

- **Monotonicity with respect to attacks: do significantly stronger cyber-attacks yield a lower value of *R*?**

A. Kott and I. Linkov, "To Improve Cyber Resilience, Measure It,"
in *Computer*, vol. 54, no. 2, pp. 80-85, Feb. 2021

BUT WHAT WOULD ONE DO WITH SUCH MEASURES?

- **Assess benefit of a cyber defense mechanism. An additional cyber defense mechanism is not always helpful. It may even introduce new vulnerabilities. Cyber resilience measurement will tell whether an additional complication and expense are worthwhile.**

- **Determination of whether a system meets a required value of cyber resilience.**

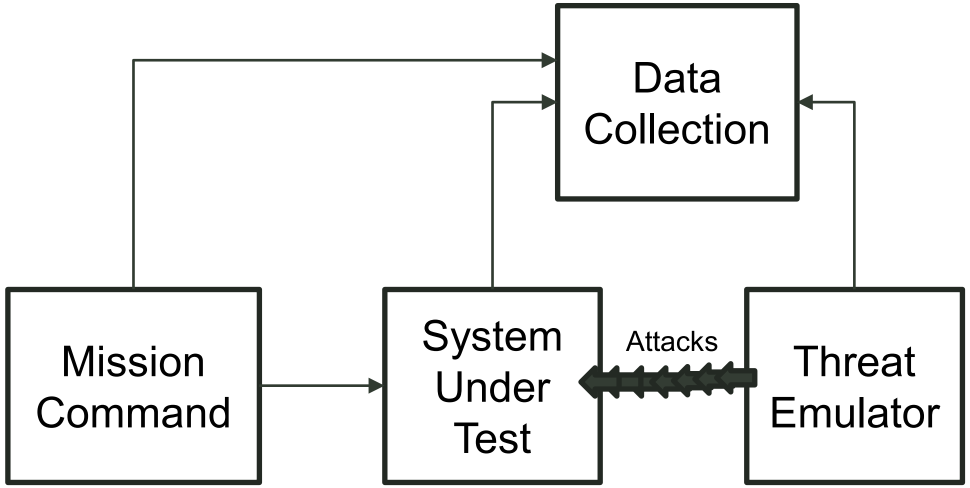
- **Help designers or operators to estimate the likelihood of a mission's success, or suitability of a system for performing a particular mission.**

- **Comparative evaluation of two systems with respect to their cyber resilience.**

- **Validation of a simulation model of a system with respect to its cyber resilience.**

WHERE WE ARE NOW

- A moderately-funded 2-year exploratory project
- Initial table-top exercises
- Investigating / procuring 3 potential systems, surrogates of manned/unmanned vehicles
- The “vehicle” is being equipped with autonomous cyber defense system (limited prototype)
- An academic partner developing a threat emulator, to issue randomized sequences of attacks
- Developing data collection mechanism
- Investigating mathematical approaches to deal with expected limitations of experimental data



Mathematical Modeling of Cyber Resilience

Initial parsimonious model:

$$\frac{dF}{dt} = (F_0 - F(t))E_b(t)A_b(t) - F(t)E_m(t)A_m(t)$$

$$\text{Malware:} \quad \mathcal{M}(t) = E_m(t)\,\overbrace{A_m(t)}^{\text{Activity}}$$

$$\text{Bonware:} \quad \mathcal{B}(t) = \underbrace{E_b(t)}_{\text{Effectiveness}}\,A_b(t)$$

Assuming constant malware/bonware model:

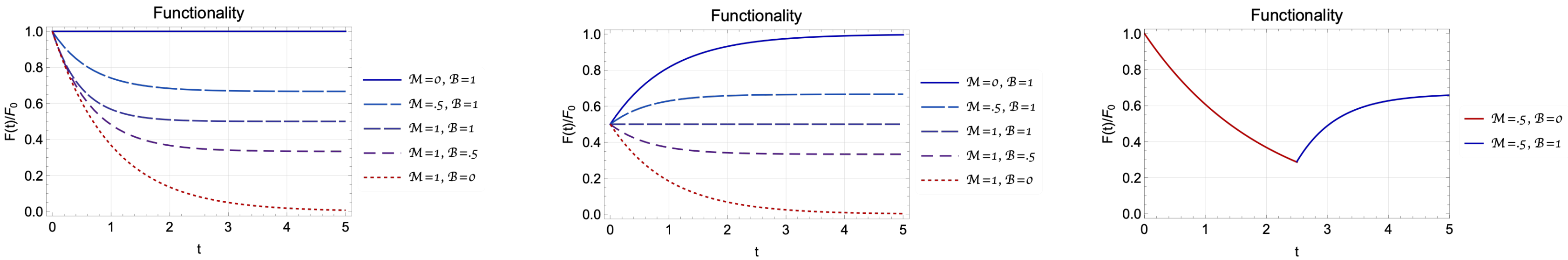
$$\mathcal{Q} = \mathcal{M} + \mathcal{B}$$

$$\frac{dF}{dt} + \mathcal{Q}F(t) = F_0\mathcal{B}$$

$$F(t) = \left[F(0) - \frac{F_0\mathcal{B}}{\mathcal{Q}}\right]e^{-\mathcal{Q}t} + \frac{F_0\mathcal{B}}{\mathcal{Q}}$$

Mathematical Modeling of Cyber Resilience

The model exhibits qualitative behaviors consistent with resilience literature and offers conceptual insights that might inform future resilience measurements approaches.



$$\text{Initial Conditions:} \; F(0) \in \{1.0, 0.5, 0.0\}$$

$$\text{Malware:} \; \mathcal{M} \in \{0.0, 0.5, 1.0\}$$

$$\text{Bonware:} \; \mathcal{B} \in \{1.0, 0.5, 0.0\}$$

Mathematical Modeling of Cyber Resilience

Initial parsimonious model:

$$\frac{dF}{dt} = (F_0 - F(t))E_b(t)A_b(t) - F(t)E_m(t)A_m(t)$$

$$\text{Malware:} \quad \mathcal{M}(t) = E_m(t)\,\overbrace{A_m(t)}^{\text{Activity}}$$

$$\text{Bonware:} \quad \mathcal{B}(t) = \underbrace{E_b(t)}_{\text{Effectiveness}}\,A_b(t)$$

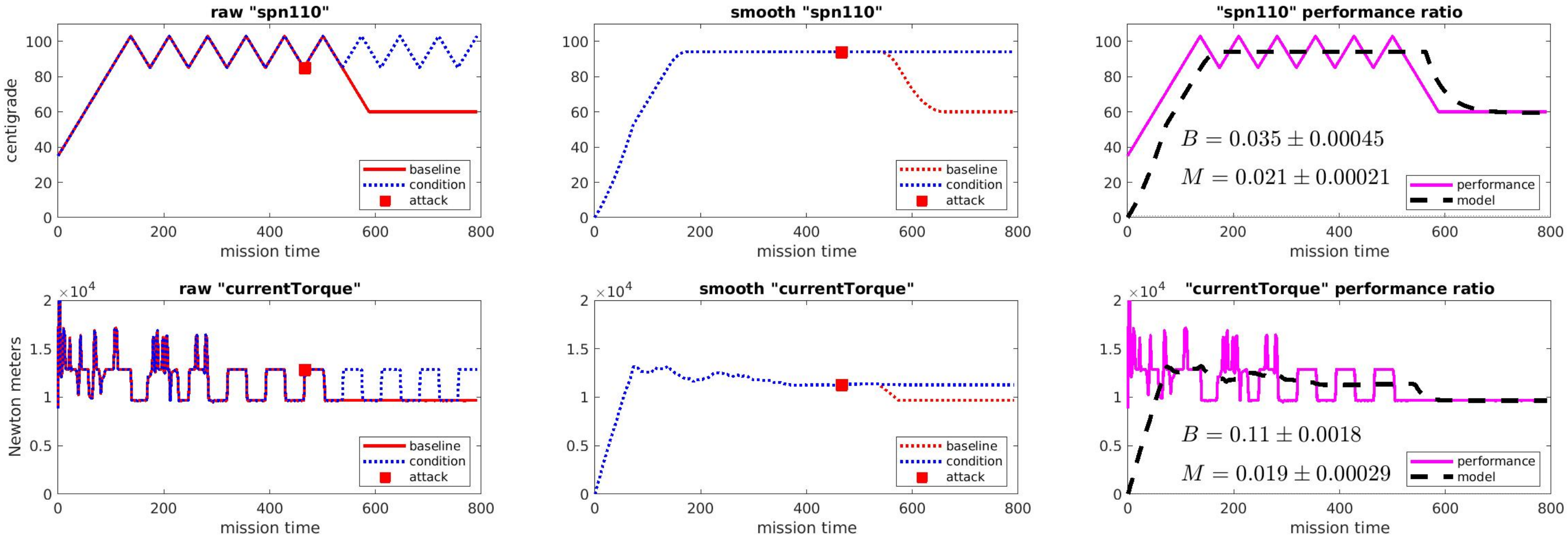
Assuming constant malware/bonware model:

$$\mathcal{Q} = \mathcal{M} + \mathcal{B}$$

$$\frac{dF}{dt} + \mathcal{Q}F(t) = F_0\mathcal{B}$$

The model parameters can be estimated using standard techniques including MCMC. Even with few free parameters, the initial model exhibits good fit to preliminary data.

Using the simulation platform, data were generated under baseline and attack scenarios. Their ratio is our performance measure. An attack was simulated starting at *t* = 467.

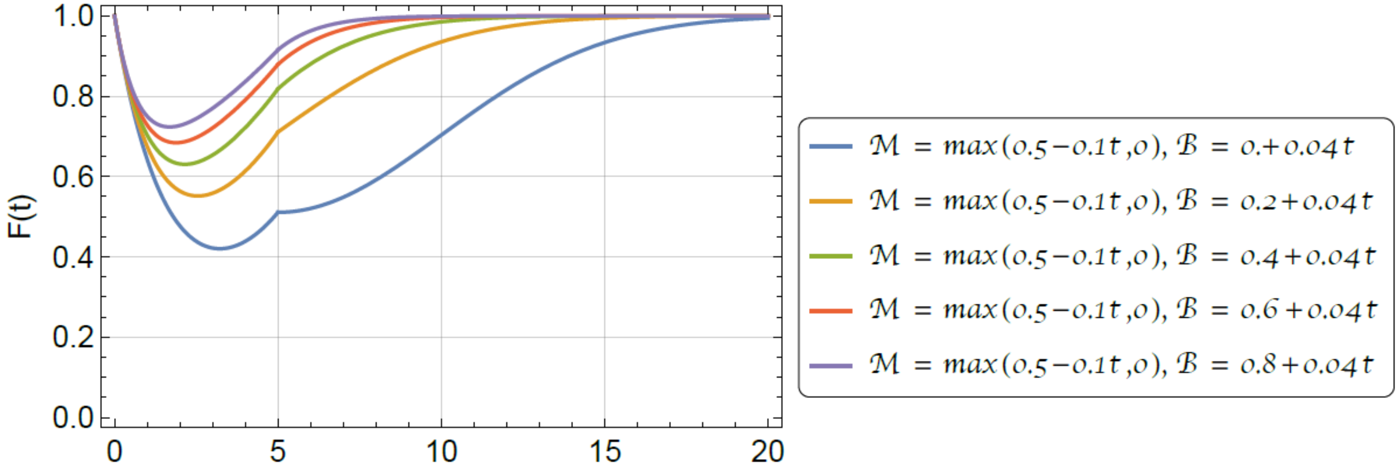


Linear Time-dependent Model for Malware and Bonware

A linear model for malware and bonware

$$\mathcal{M}(t) = \nu - \mu t,$$
$$\mathcal{B}(t) = \alpha - \beta t,$$
$$\mathcal{Q}(t) = \lambda - \omega t,$$
$$\lambda = \alpha + \nu,$$
$$\omega = \beta + \mu.$$

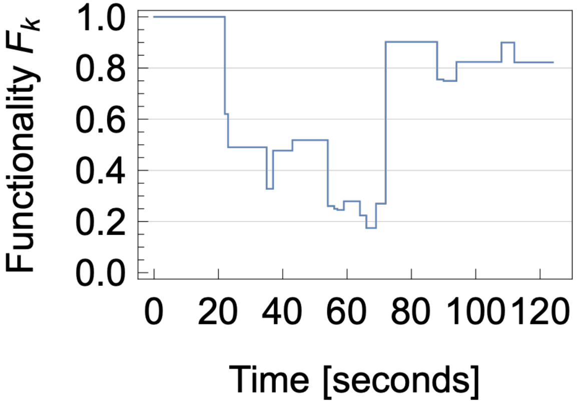
$$\frac{dF}{dt} + (\lambda - \omega t)F(t) = F_0(\alpha - \beta t)$$

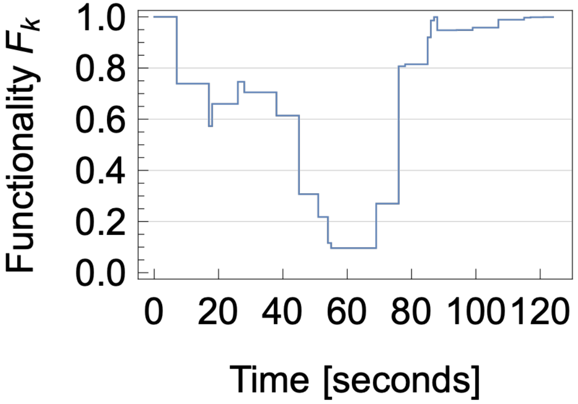


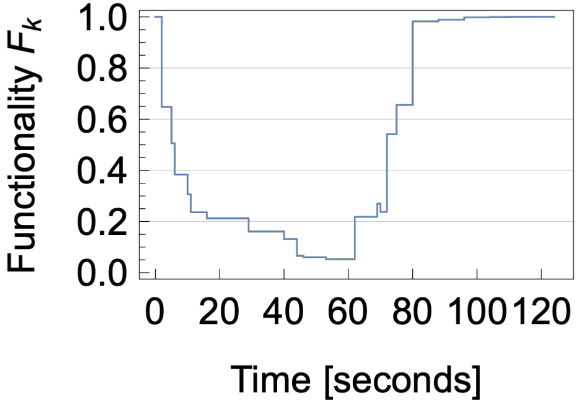
A time-dependent model allows for more complex behaviors. As malware effectiveness decreases and bonware's increases, functionality trend reversal can be modeled.

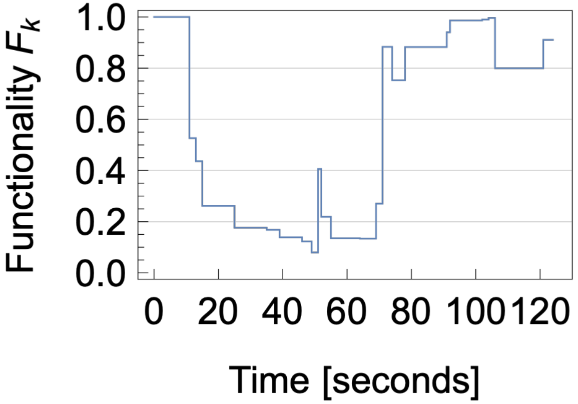
Notional Data and Realizations Generated

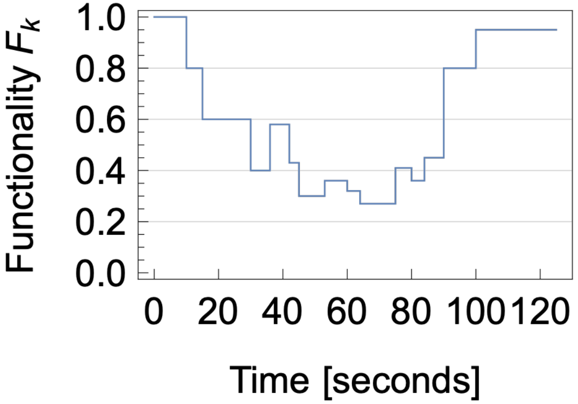
Which is a plot of the data?

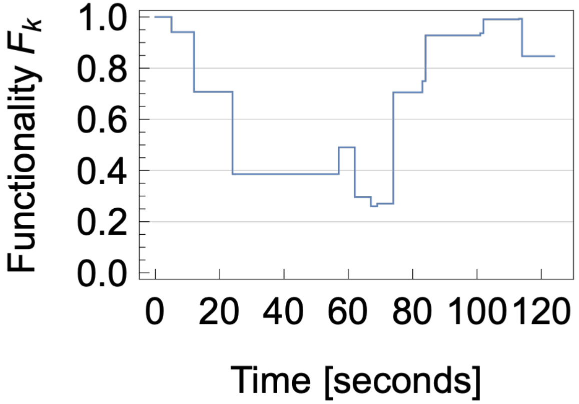












GENERAL LESSONS LEARNED SO FAR

- **Articles (subjects) of tests are not readily available**
  - Must be instrumented to allow observation of internal cyber events and states
  - Must allow sufficient variety of mission scenarios
  - Must be affordable, and allow for affordable tests
  - Even simulators / emulators are not readily available
  - Wish: a system under development should meet requirements of testability for cyber resilience

- **Mission scenarios are not obvious**
  - Realistic yet executable for testing purposes
  - Diverse yet representative
  - With non-ambiguous mission accomplishment
  - User-adaptable
  - Affordable
  - Defensible even when no 2 SMEs agree

- **Defining threats, attacks: capabilities, intensity, techniques**
  - Much of the same as above

ILLUSTRATIVE EXAMPLES

- **Modest changes in environment, execution may bring disproportional impact**
  - Example: routes with different maximum grade may change impact of a cyber attack drastically
- **Omitting a physical phenomenon hide a major cyber impact**
  - Example: A simulator does not include fuel consumption – fails to portray a massive cyber impact
- **Physical robustness may be conflated with cyber resilience**
  - Example: a highly robust physical subsystem may negate a cyber attack

REFERENCES

- A. Kott and I. Linkov, "To Improve Cyber Resilience, Measure It," in Computer, vol. 54, no. 2, pp. 80-85, Feb. 2021
- Kott, A., & Linkov, I. (Eds.). (2019). Cyber resilience of systems and networks (pp. 381-401). New York, NY: Springer International Publishing.
- Hosseini, S., Barker, K., & Ramirez-Marquez, J. E. (2016). A review of definitions and measures of system resilience. Reliability Engineering & System Safety, 145, 47-61.
- J. S. Brtis, "How to think about resilience in a DoD context," MITRE CORP, Colorado Springs (CO), 2016.
- I. Linkov, D. A. Eisenberg, K. Plourde, T. P. Seager, J. Allen, and A. Kott, “Resilience metrics for cyber systems,” Environ. Syst. Decis., vol. 33, no. 4, pp. 471–476, 2013
- D. W. Hubbard and R. Seiersen, How to Measure Anything in Cybersecurity Risk. Hoboken, NJ, USA: Wiley, 2016
- A. Kott, J. Ludwig, and M. Lange, “Assessing mission impact of cyberattacks: Toward a model-driven paradigm,” IEEE Secur. Privacy, vol. 15, no. 5, pp. 65–74, Jan. 2017
- E. J. M. Colbert, A. Kott, and L. P. Knachel, “The game-theoretic model and experimental investigation of cyber wargaming,” J. Def. Model. Simul., vol. 17, no. 1, pp. 21–38, 2020
- Colbert, E. J., & Kott, A. (Eds.). (2016). Cyber-security of SCADA and other industrial control systems (Vol. 66). Springer.
- Kott, A. (2018). Intelligent autonomous agents are key to cyber defense of the future army networks. The Cyber Defense Review, 3(3), 57-70.
- Kott, A., & Theron, P. (2020). Doers, not watchers: Intelligent autonomous agents are a path to cyber resilience. IEEE Security & Privacy, 18(3), 62-66.
- Kott, A., Théron, P., Drašar, M., Dushku, E., LeBlanc, B., Losiewicz, P., ... & Rzadca, K. (2018). Autonomous intelligent cyber-defense agent (aica) reference architecture. release 2.0. arXiv preprint arXiv:1803.10664.
- Aaron C. Madewell, Paul C. Johnson, Quantifying the Operational Resilience of Systems Operating in Cyberspace, MORS Journal 2021

QUESTIONS AND DISCUSSION

UPCOMING TALKS

SERC TALKS

Ms. Melinda K. Reed

Director, Resilient Systems, Office of the Under Secretary of Defense for Research and Engineering within the Office of Strategic Technology Protection and Exploitation

Wednesday, June 15, 2022 | 1PM ET

"Cyber Resilience" Series Moderator:

Dr. Peter Beling, SERC Research Council member, Virginia Tech

CONTACT

Webinar Coordinator: Ms. Mimi Marcus, Stevens Institute of Technology – mmarcus@stevens.edu

Please visit the SERC Talks page to register and for more information and updates.

SERC TALKS

SYSTEMS ENGINEERING RESEARCH CENTER

THANK YOU FOR JOINING US!

Please check back on the SERC website for today’s recording and future SERC Talks information.

www.sercuarc.org/contact-us/