APPLIED RESEARCH LABORATORY FOR
INTELLIGENCE
AND SECURITY

The Uncompromised Delivery and Sustainment of the Navy's Digital Engineering

Thomas Hedberg (thedberg@arlis.umd.edu)
Timothy Sprock (tsprock@arlis.umd.edu)

Disclaimer

Any opinions, findings, conclusions, or recommendations expressed in this publication do not necessarily reflect the views of the Department of Defense (DoD). Additionally, neither the DoD nor any of its employees make any warranty, expressed or implied, nor assume any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, product, or process included in this publication.

Certain commercial entities, equipment, or materials may be identified in this document to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by the ARLIS, the University of Maryland, or the DoD, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

BLUF

Cyber risks evolved quickly and caught many off guard. Supply chain is facing a similar watershed moment and we may already be playing catch-up to mitigate risks and build resilience.

While we need new methodologies for designing and controlling resilient supply chains, we first need a better understanding and specification of what they need to be resilient to.

UNCLASSIFIED // APPROVED FOR PUBLIC RELEASE

What's the problem?

- Typical production & logistics trade-space: Cost, quality, and schedule
- Risk is a function of threats, vulnerabilities, and consequences
  - Threat of compromise (e.g., vendors delivering out-of-spec parts, counterfeits) or disruption (e.g., labor strike, weather)
- How do we properly consider risk when designing a supply chain?
  - How do we incorporate the ecosystem that our supply chain(s) live and operate in?
  - How do we design supply chains to be resilient to the unknown unknowns? In particular, advanced persistent threats?

Doesn't SCRM handle this?

- Originated from efforts to apply business risk management methods and culture to the supply chain.
- Focuses on financial risk and is managed as a part of supplier management.
- The effectiveness of risk management regimes depends not only on how we define and measure risk, but also how we look for them.
  - Typical SCRM and vulnerability literature consider "business-as-usual" risks, large-scale disruptions (hurricanes), and "terrorism"; but fail to consider advanced, persistent threats – this is where the cyber & supply chain communities diverge significantly
  - In cyber – detecting behaviors (threats) beats zero-days (vulnerabilities)

"Diet of Poisoned Fruit“ – Richard Danzig

Global, interconnected supply chains may draw an analogy to the "Diet of Poisoned Fruit" (cyber systems)

- Global scale supply chains -- Enable innovation; cheaper, quicker, and "more" of complex products; global integration & purchasing power.
  - Global supply chains have effectively become absolutely essential to maintaining the lifestyle of Americans and enabling the development and production of critical economic and national security capabilities.
  - Magnify impacts of disruptions (shipping, weather, disaster), create opportunities for theft and loss of innovation & intellectual property; interdependence creates challenges and opportunities for geo-economic coercion.
- "[Supply chain] is adversarial, contested, and crowded territory. Our adversaries (criminals, malevolent groups, numerous opposing states) co-evolve with us."
- "It's much more fluid, egalitarian, distributed, and dynamic than technologies/systems encountered during the last half-century"

Danzig (2014) “Surviving on a Diet of Poisoned Fruit: Reducing the National Security Risks of America’s Cyber Dependencies”. Center for New American Security.

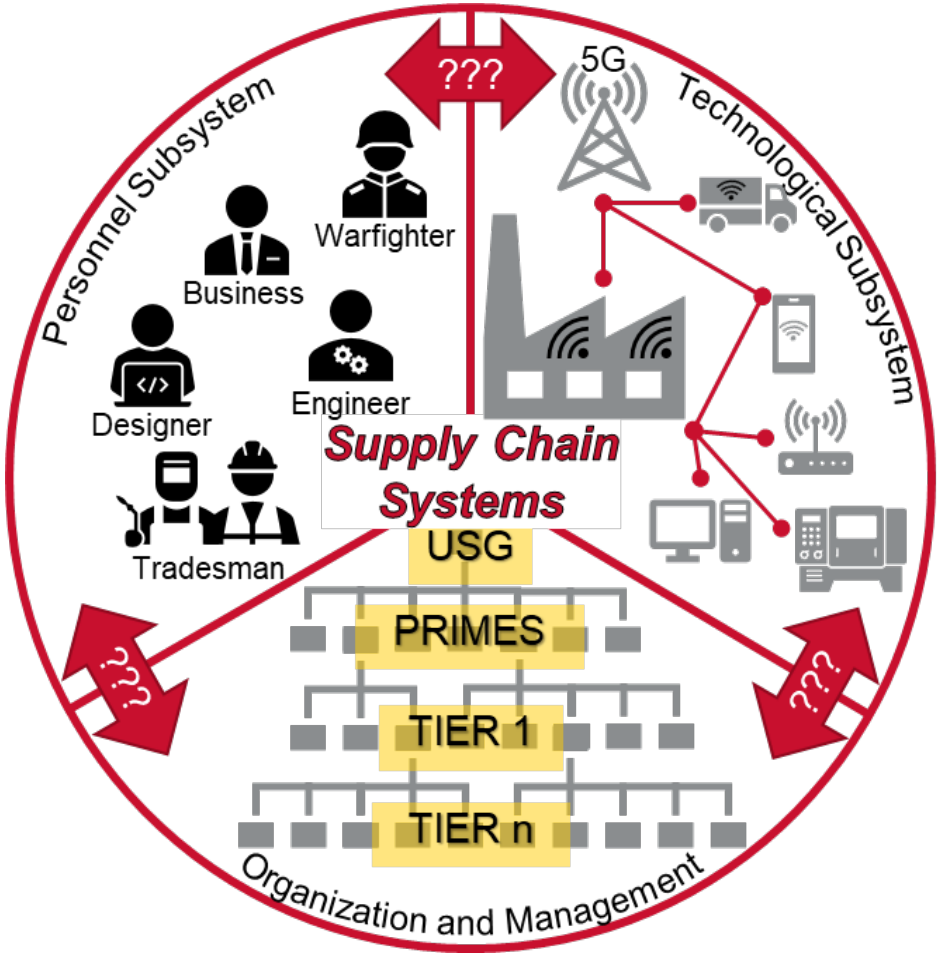
UNCLASSIFIED // APPROVED FOR PUBLIC RELEASE

But what if ….?

- You wanted to design the system to work when you needed it most?
- You needed to expect and prevent Murphy's Law?

Acquisition and Industrial Security

Uncompromised Delivery and Sustainment of Systems, Capabilities, and Workforces



SUPPLY CHAINS ARE SOCIOTECHNICAL SYSTEMS

Objective:

- Provide a capability for identifying and explaining what technologies and supply chains are too critical for the U.S. to lose --- but also, to determine what we can let go
- Conduct applied S&T research to gain and maintain engagement advantages through all-source intelligence collecting, decision making, and executing at the intersection of humans and information

Thrust Areas:

- **Technical Information Assurance:** mitigating risks to linking everything together for ensuring uncompromisable digital transformations and information systems
- **Continuous IT/OT Validation:** standards-based sensing and monitoring of IT/OT capabilities for anomaly detection and risk mitigation
- **Resilient, Trustworthy Supply Chains:** ensuring operational control through integrated, uncompromisable logistics and decision making

APPLIED RESEARCH LABORATORY FOR INTELLIGENCE AND SECURITY

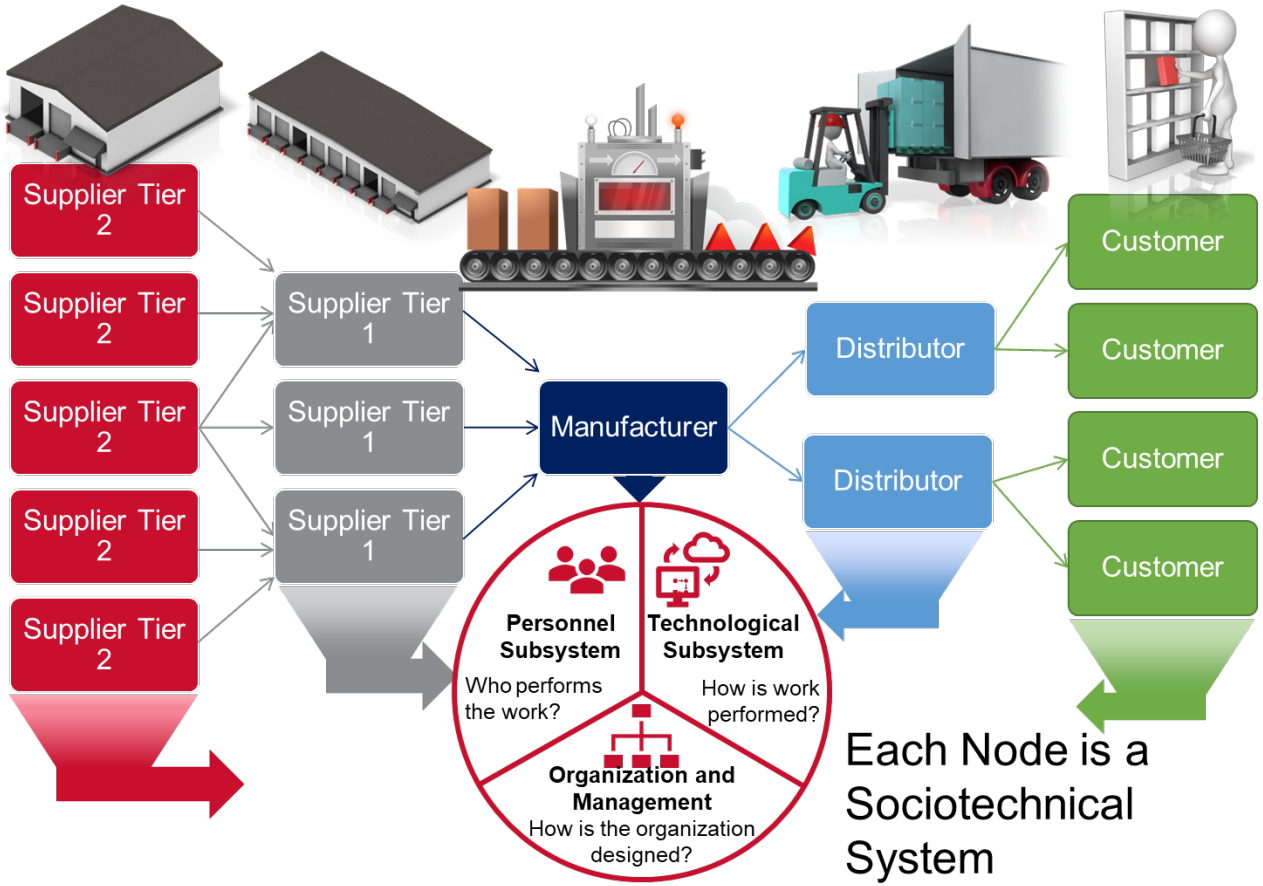
UNIVERSITY OF MARYLAND

2023/07/19

Acquisition and Industrial Security

Supply Chain Resilience:

- Node-level
- Sector-level
- Network-level
- End-to-end
- Full-lifecycle



Each Node is a Sociotechnical System

IT/OT Validation

- Interface between humans, digital, and physical world
- Root of data and control

What is to be made? How to make it?

Information Flows

What was made? How was it made?

Technical Information Assurance

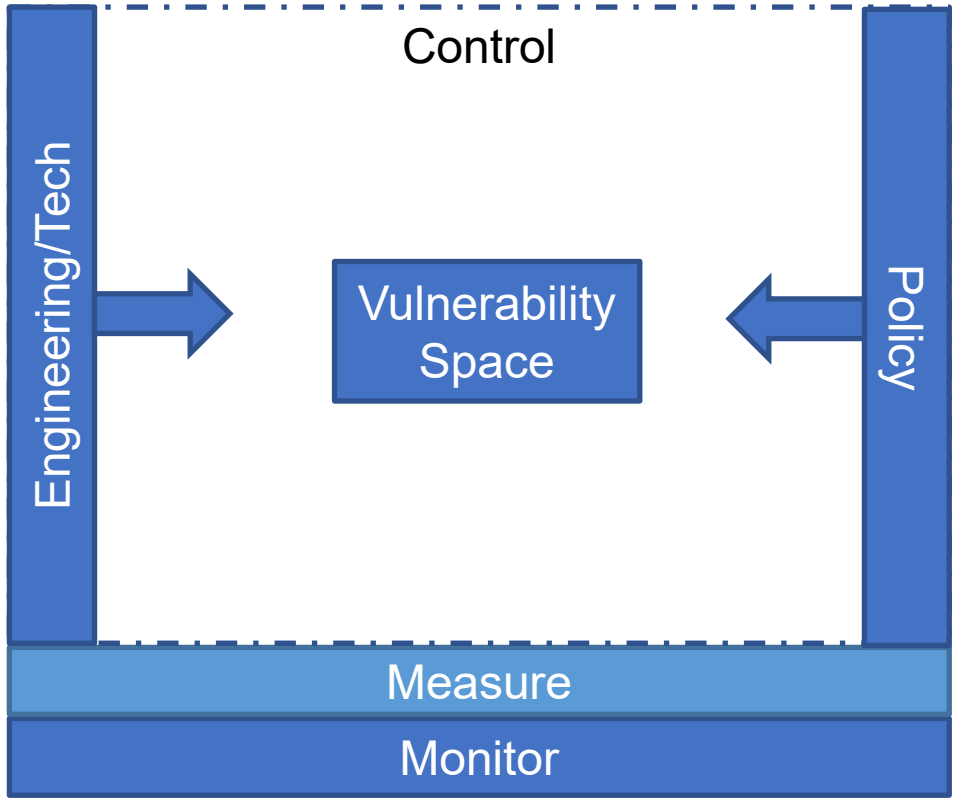
- Digital Engineering
- Digital Twin
- …

2023/07/19

A Brief Aside on Digital Engineering

- Concerted DoD-wide push to deploy digital engineering to solve cost, quality, & schedule issues.
- From an information assurance perspective, it becomes tightly intertwined with cyber security concerns

A type of information assurance problem where characteristics of the data and process enable semantic/behavioral security to be built into the information system.



- Cybersecurity
- Confidential Computing
- Out-of-band measures
  - Humans-in-the-loop
  - Federated authentication
  - Data zones
- Strategy of Abnegation
  - Forgoing “nice-to-have” features of DE ecosystem to balance risk exposure

Challenge: decision-makers aren’t trained, motivated, and authorized to make trade-offs between risk and other factors

UNCLASSIFIED // APPROVED FOR PUBLIC RELEASE

Supply Chain Gets Attention from USG

Emphasis on bolstering our supply chains and recognition that our supply chains are vulnerable

- Supply chain is mentioned in both the 2022 National Defense and National Security Strategies
- Executive Order (E.O.) 14017 on America's Supply Chains.

  "The COVID-19 pandemic exposed structural weaknesses in the U.S. domestic industrial base and critical supply chains – the result of decades of preferencing underinvestment, outsourcing, and offshoring over long-term security, sustainability, and resilience. From the beginning of his Administration, President Biden prioritized strengthening critical supply chains and revitalizing the U.S. industrial base."

Needed Supply Chain Capabilities

- What are the analytical capabilities we need to identify and mitigate risks in our current and future supply chains?
  - Remediating vulnerabilities isn't the right approach. Typical SCRM approaches are just whack-a-mole. Rather it's important to improve our ability to detect and respond to threats to the system and also increase the system's ability to cope with disruptions/compromises (resilience).
- Measure, Monitor, & Control Supply Chains
  - Cyber-analogy: detecting behaviors beats plugging zero-days
    - Plugging zero-days <=> mitigating vulnerabilities in tech, people, policy

UNCLASSIFIED // APPROVED FOR PUBLIC RELEASE

Measure, Monitor, & Control Supply Chains

Ambitious Goal: An ensemble of supply chain and economic models that would enable an assessment of supply chain vulnerability, resilience, and capacity for adaptation.

Measure:

- Supply chain illumination
- What's the "weather balloon" for supply chains?
- Formal definitions of risk, vulnerability, and resilience

Monitor:

Behavioral Models and Dynamics

- Rigorous, computational models drawn from multiple domains
  - How do you model what the supply chain is supposed to be doing?
  - Understand network effects, causality, interdependence, and cascade
- Anomaly detection
  - How do you detect when it's not doing what it's supposed to?
  - SIEM approaches for supply chain

Control:

- Graceful Extensibility and Sustained Adaptability as engineering and policy approaches to resilience
  - Can US economy and supply chains "push through" adversity? To what extent and long? Can it adapt to conditions? COVID pandemic gives us some clues
- Innovation, collaboration, and contracting
  - Game theoretic approaches to incentive structures
- Risk Assessment: Aggregation, interdependence, disaggregation, & preferences
  - Decision-makers must be trained, motivated, and authorized to make trade-offs between risk and other metrics

UNCLASSIFIED // APPROVED FOR PUBLIC RELEASE

Supply Chain Illumination

- Illumination is already getting a big push in the DoD
  - "The lack of visibility into defense supply chains makes easy targets for adversaries seeking to insert undetected risks into supply chains" https://warontherocks.com/2023/06/in-the-dark-how-the-pentagons-limited-supplier-visibility-risks-u-s-national-security/
- Venture capital is masking ownership, particularly foreign ownership, and making illumination difficult and CFIUS review ineffective
  - "When the Invisible Hand turns into a Sleight of Hand: Understanding How Venture Capital is used to Create Vulnerabilities in the Supply Chain" (https://www.dni.gov/files/NCSC/documents/supplychain/Final%20VC.pdf)
  - "Foreign Shell Companies Trying to Infiltrate US Defense Industry, Top Weapons Buyer Says" https://www.military.com/daily-news/2020/05/01/foreign-shell-companies-trying-infiltrate-us-defense-industry-top-weapons-buyer-says.html
- Digital twins aren't necessarily the solution
  - Information assurance and AI trustworthiness challenges
- What and where should be measured?
  - Supply chain metrics are often aggregated, low granularity, and infrequently reported; and thus lagging indicators. What and where should be measured? What are the best leading, real-time indicators? And how can that data be gathered and leveraged in near real-time?
  - Illuminating relationships and network structure is challenging and just the start

UNCLASSIFIED // APPROVED FOR PUBLIC RELEASE

Resilient, Trustworthy Supply Chains

Four concepts for resilience (Woods, 2015):

- Resilience as rebound
  - How do systems recover from surprises?
- Resilience as robustness
  - Increase set of surprises that the system can absorb.
- Resilience as graceful extensibility (degradation) <=> Anti-fragility
  - Opposite of brittleness (fragility)
  - How do systems stretch to handle surprises?
- Resilience as sustained adaptability
  - "ability to continue to adapt to changing environments, stakeholders, demands, contexts, and constraints"
  - Avoiding or delaying "decompensation": exhausting the capacity to deploy and mobilize responses as disturbances grow and cascade

https://maritimesafetyinnovationlab.org/wp-content/uploads/2021/06/4sensesofresiliencepublic.pdf

Defining Vulnerability

- **Centers of Gravity**: Primary sources of moral or physical strength, power and resistance.
- **Critical Capabilities**: Primary abilities which merits a Center of Gravity to be identified as such in the context of a given scenario, situation or mission.
- **Critical Requirements**: Essential conditions, resources and means for a critical capability to be fully operative.
- **Critical Vulnerabilities**: Critical requirements or components thereof which are deficient, or vulnerable to neutralization, interdiction or attack (moral/physical harm) in a manner achieving decisive results - the smaller the resources and effort applied and the smaller the risk and cost, the better.

Strange, Joe. (1996) “CENTERS OF GRAVITY & CRITICAL VULNERABILITIES: Building on the Clausewitzian Foundation So That We Can All Speak the Same Language”. Marine Corps War College. https://jfsc.ndu.edu/Portals/72/Documents/JC2IOS/Additional_Reading/3B_COG_and_Critical_Vulnerabilities.pdf

Design for Robustness

Typical approaches from supply chain literature include:

- Hold more inventory,
- Select more reliable, but more expensive, suppliers
- Invest in fostering additional capacity for critical capabilities,
- Invest in process/resource flexibility,
- Invest to improve reliability of existing capacity & suppliers

Beyond Robustness: Lessons from Other Disciplines

- What can we learn from the internet?
  - Resilience is due to geographical and functional redundancies, but also, can be attributed to timely measurements used for real-time control.
- What can we learn from cyber-security?
  - SIEM for Supply Chain: How do we monitor and measure the network to detect anomalies? And respond more quickly?
- What can we learn from financial and social networks?
  - How to describe, predict, and control contagion in the network – prevent cascading failures?
- What can we learn from safety-critical systems?
  - Formal verification of “cannot fail” or proof that your systems are “safe”, i.e., availability, confidentiality, integrity
- How do you define a critical capability?
  - How can we ensure sufficient capacity and redundancy for each critical capability? How can we identify critical technologies and capabilities, or entire supply chains?

Importance of Socio-technical Solutions

- Massive introduction of complexity / technology while not understanding risks and safeguards seems to be part of the problem
- People aren't trained to make risk trade-offs
- Policy that is reactive and generally poor at spelling out intent and goals; organizational/control structures poorly incentive collaboration
- The solution space requires leveraging the strengths of people, policy, & technology to shore up each's deficiencies

Beyond Robustness: Socio-technical Solutions

Humans must be part of the solution

- Develop stress testing framework for supply chains leveraging human-machine teaming.
- Develop and deploy contract vehicles for supply chain coordination, in particular addressing system risk.
- Develop design methods, organizational policies, and software to enable socio-technical integration and coordination at an operational level.

Closing Thoughts

- There's some baseline stuff that we have to do well. Then there's harder stuff ... then there's the unknown unknowns.

- IP theft is a problem for competitiveness. OCONUS supply chains are vulnerable to disruption and compromise from passive and active threats. CONUS IT systems (including critical infrastructure) are under threat from APTs and smaller actors. To what degree are our CONUS supply chains threatened?

Acknowledgment

This material is based upon work supported by the Office of Naval Research (ONR) under Contract No. HQ0034-18-D-0005, Delivery Order No. N00014-23-F-1001.

Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of ONR.

Thank you! Questions?

Contact Information

- Thomas Hedberg (thedberg@arlis.umd.edu)
- Timothy Sprock (tsprock@arlis.umd.edu)

Related Efforts

- DARPA Resilient Supply-Demand Networks (RSDN) *active*
  - SDN stress-testing and fragility-mitigation simulator
- DARPA Complex Adaptive System Composition and Design Environment (CASCADE)
  - Develop and/or exploit innovative approaches in mathematical abstraction and composition for the design of dynamic, adaptive and resilient systems with unified understanding of system structures, behaviors and interactions across multiple spatiotemporal scales
- DARPA Advanced Vehicle Make (AVM) Instant Foundry Adaptive through Bits (iFAB) (iFAB)
  - Develop an information architecture to enable rapidly-configurable, distributed, digital manufacturing.
- DARPA LogX
  - The goal of the LogX program is to develop and demonstrate software for real-time logistics and supply chain system situational awareness (diagnosis), future state prediction (prognosis) and resilience at unprecedented scale and speed.
- Supply Chain Risk Analysis Management Solution (SCRAMS)
  - https://www.navysbir.com/n16_3/N163-D02.htm

Additional S&T Needs

Simultaneously address these meta-research questions:

- How to mature research into industrial practice?
- How to adopt successful risk mitigation and resiliency practices from one industry to another?
- How to accommodate imprecise measurements, messy relationships, and fuzzy preferences of finicky humans?

Relevant Quotes from Danzig

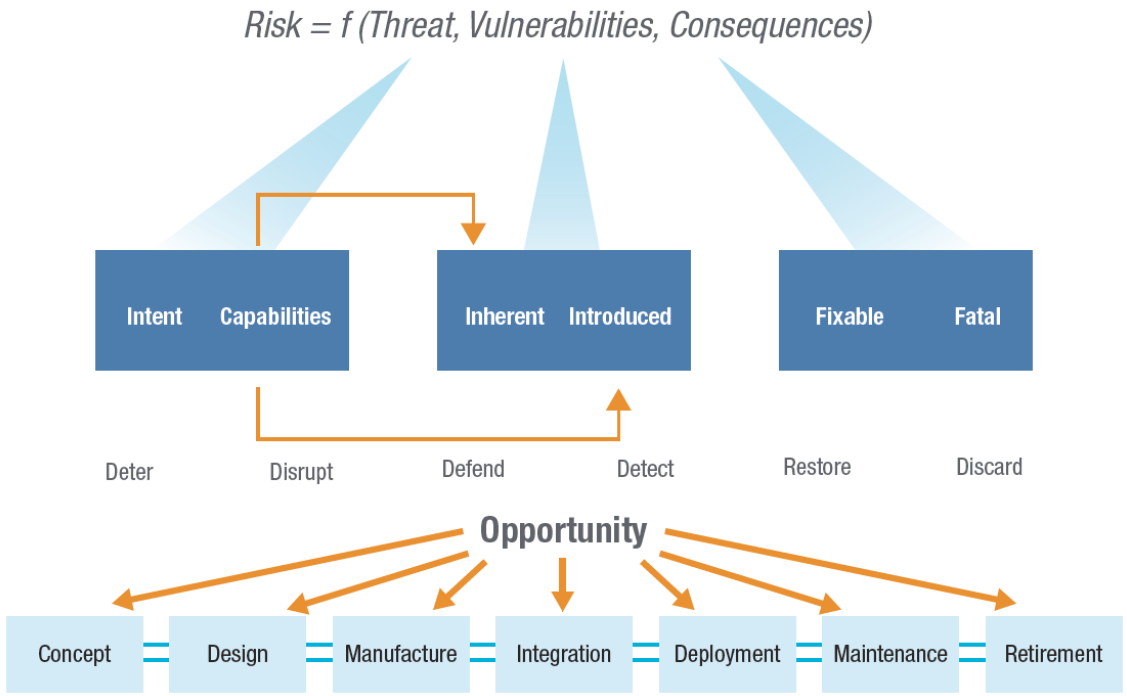
- "In sum, strategies for cybersecurity can reasonably aim to reduce and manage risks by improving security capabilities and practices.
- But cybersecurity risks cannot be completely or assuredly eradicated. Successful strategies must proceed from the premise that cyberspace is continuously contested territory in which we can control memory and operating capabilities some of the time but cannot be assured of complete control all of the time or even of any control at any particular time.
- Policymakers must make a judgment about when to intervene and when to allow market forces to determine exposure to this risk. They must also judge how much they are willing to sacrifice efficiency and effectiveness in cyber systems to enhance security."

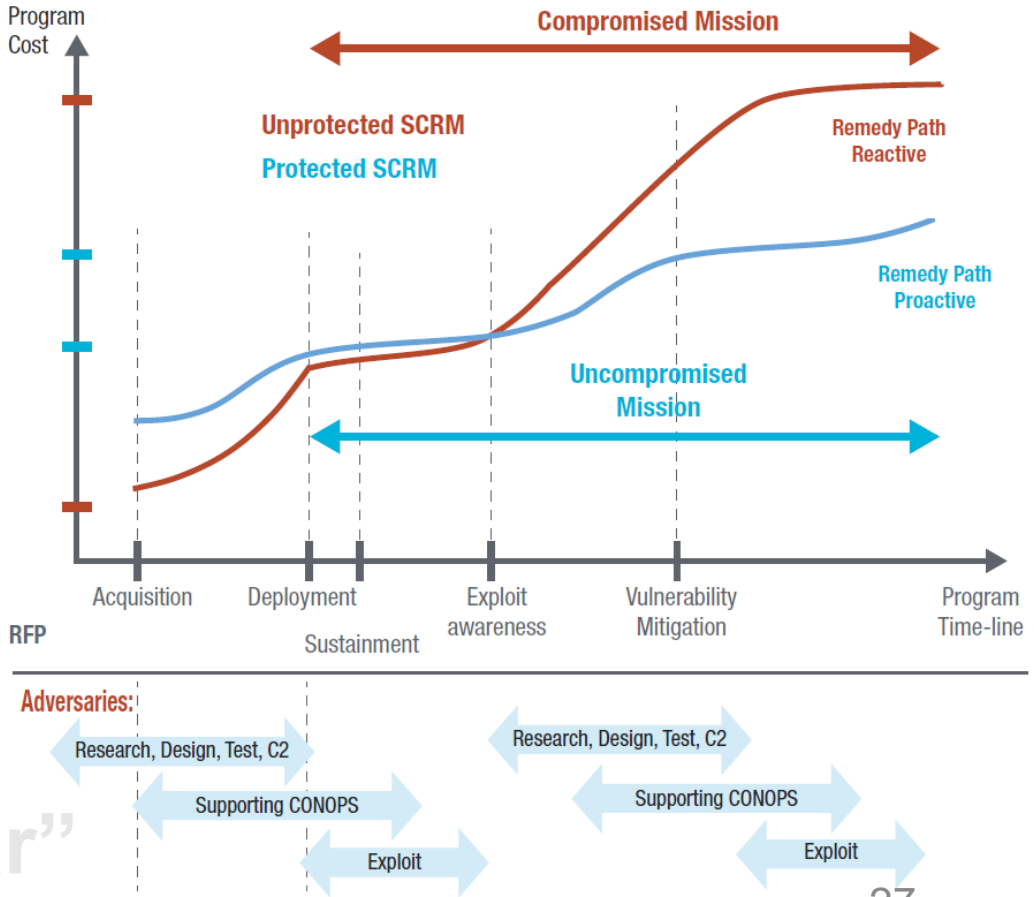
  - Richard Danzig – "Surviving on a diet of Poisoned Fruit"

Deliver Uncompromised!

For mission owners, the primary goal of DoD must be to deliver warfighting capabilities to Operating Forces without their critical information and/or technology being wittingly or unwittingly lost, stolen, denied, degraded or inappropriately given away or sold.

--- William Stephens, (Ret.) Director of Counterintelligence, DCSA





"Make Security a Fourth Pillar"

Nissen, C., Gronager, J., Metzger, R., & Rishikof, H. (2018). *Deliver Uncompromised: A Strategy for Supply Chain Security and Resilience in Response to the Changing Character of War*. The MITRE Corporation.

UNCLASSIFIED // APPROVED FOR PUBLIC RELEASE

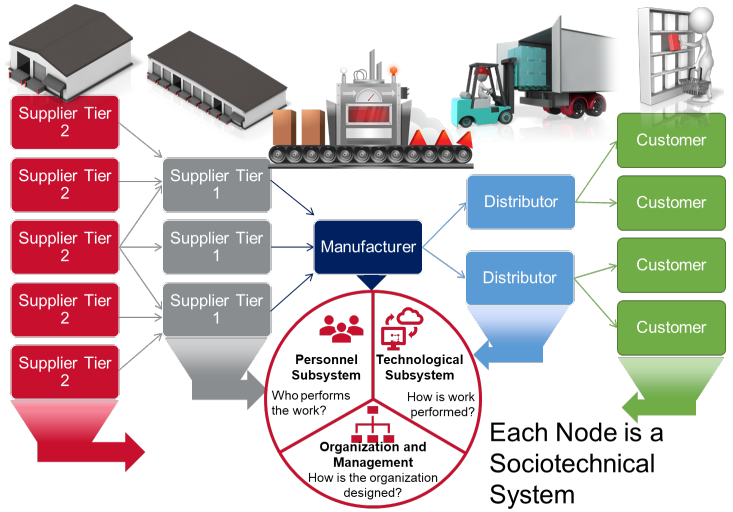
The Uncompromised Delivery and Sustainment of the Navy's Digital Engineering

- **Quarterly/Monthly Accomplishments**
  - Draft of Intellectual Property Exfil summary
  - RISC Interns: supply chain vulnerability vignettes
  - Scoping workshop with retired Navy leadership yielded new insights of where to track root cause.

- **(I) Issues, (C) Concerns, (D) Decisions**
  - (I) Classification/CUI determination for summary and analysis reports. We don't have OCA and CUI is vague.
  - (C) Hiring has been slower than expected. Limiting throughput on surveys and compendium type deliverables
  - (D) Limitation of funds letter.

- **Award Self-Assessment**
  - Proceeding cautiously regarding CUI / aggregation challenges.
  - Re-planning workshops CDRL execution.
  - Supply chain vulnerability research is getting a new perspective; re: Danzig's poisoned fruit and graceful extensibility

Supply Chain Resilience Requires Sociotechnical Solutions



- **Plans/Tasks for next Quarter/Month**
  - *Complete draft of DE strategy study*
  - *Navy Digital Engineering COI/workshop*
  - *Draft: IP Exfil w/ MITRE ATTA&CK framework*

PI: Thomas Hedberg
(thedberg@arlis.umd.edu)
Co-PI: Timothy Sprock
(tsprock@arlis.umd.edu)