University of Pittsburgh.
Cyber Energy Center

Transforming Cybersecurity Workshop

Workshop summary

September 30, 2025

Acknowledgements

This was supported by Pitt Cyber and the Cyber Energy Center. We are grateful to all the speakers and participants.

Summary

The Transforming Cybersecurity Workshop brought together nearly 50 experts from government, industry, academia, and research institutions to examine the evolving cyber threat landscape and explore strategies to build resilience across interconnected systems, including critical infrastructure. Cybersecurity risk is fundamentally about decision-making under uncertainty. Risk decisions are multidisciplinary, reflecting threats to outcomes we value, such as confidentiality, integrity, availability, and the long-term safety of critical systems

A central theme was the importance of moving beyond siloed approaches to adopt an ecosystem perspective. Cyber threats do not respect sector or agency boundaries, and vulnerabilities often emerge at the "seams" where responsibility is diffuse. Engaging multi-sector stakeholders is essential to make progress. Participants highlighted the need to align policies, standards, and practices across sectors and to better define roles and responsibilities among organizations and authorities. Emerging challenges—such as those posed by connected vehicles, supply chain dependencies, and cyber-physical systems—illustrated the risks of fragmented accountability and insufficient visibility.

Another key insight was the need to rebalance effort toward the "left of boom," shifting resources from incident response toward prevention, education, policy modernization, and anticipatory strategies. Today's practices still rely heavily on patching and post-hoc protections, but systemic risks demand more proactive approaches. Formal methods, combined with policy incentives and cultural change in organizations, could help shift toward prevention. Yet there are challenges in defining "certified" software. Additionally, while full formal verification is costly and hard to scale, partial certification and formal methods can reduce ambiguity and enforce essential properties.

Overall, the workshop stressed that meaningful transformation in cybersecurity requires sustained collaboration, integrated approaches, and a commitment to aligning incentives across the ecosystem. Advancing education, fostering innovation, and investing in cross-sector policy solutions will be critical to staying ahead of adversaries and ensuring resilience in an increasingly digital and interconnected world. There was strong agreement that collaboration is essential across sectors. Participants recommended that the group sustain momentum by reconvening regularly, publishing action steps, and initiating joint projects. Building a trusted

mechanism for data sharing, aligning incentives, and involving a wider set of stakeholders—such as utilities, regulators, and industry associations—were also highlighted as essential next steps.

Key takeaways

- Effective cybersecurity requires ecosystem-level governance, harmonized standards, and investment in prevention.
- Periods of change present opportunities to reframe public–private partnerships and strengthen resilience.
- Future priorities: reduce uncertainties, engineer adaptive systems, and train the next generation in specification and formal proof.
    - Insurance and warranties may become embedded in software products.
    - More emphasis is needed on proactive "left of boom" approaches rather than post-incident response.
    - Continuous adaptation, testing, and education are essential for resilient systems.
- Certification can provide value, but only if designed as a living process—continuous, context-sensitive, and backed by aligned incentives and accountability.

Next steps

- Dan Cole and Erica Owen will schedule a follow-up lunch in both Fall 2025 and Spring 2026
- The first lunch is scheduled for noon on Friday November 7, 2025 at University of Pittsburgh Benedum Hall Room 1145. RSVP to follow.
- One achievement of this workshop was to discuss problem and highlight challenges and opportunities. In Sumer 2026, we plan to host a follow-up workshop that features discussions of specific policy-technology gaps.
- More broadly, we invite those interested to reach out to other potential interested parties, including for instance additional sectors and stakeholders (e.g., utilities under NERC CIP, regulators, industry associations)
- We invite folks to stay connected through Cyber Energy Center monthly seminars. Seminar information can be found on our website.

APPENDIX: SUMMARY BY PANEL

Cheri Caddy Keynote: Transforming Cybersecurity

Cheri Caddy emphasized that cybersecurity is a "team sport" and warned against siloed approaches that leave gaps at the seams of responsibility. She highlighted the risks of siloed policies and fragmented accountability, particularly in areas like connected vehicles and energy systems where IT and OT converge. She called for greater investment "left of boom" in prevention, education, and cyber-informed engineering, along with clearer governance structures and regulatory harmonization. Caddy highlighted the need to integrate cybersecurity into engineering education and to build global standards that can keep pace with rapid technological change.

- Ecosystem focus:
  - Cyber issues cut across all sectors; no single-sector problems.
  - Overcoming "stovepipes" in government, industry, and academia is essential to bring diverse stakeholders together.
  - Governance structures must account for interdependencies (e.g., energy, connected vehicles).
- Roles and responsibilities:
  - IT and OT operators often assume the other is responsible, leaving gaps.
  - Shared responsibility and clearer frameworks are needed to manage distributed risk.
- Prioritize "Left of boom" investment:
  - Most resources are spent on response (right of boom) rather than prevention.
  - Greater emphasis needed on awareness, education, design, and infrastructure resilience.
  - Cyber-informed engineering (CIE) integrates security into design for long-lived systems.
- Risk reallocation:
  - Shifts in public–private partnerships are changing who bears responsibility for risk.
  - Regulatory harmonization is critical: vendors serving multiple sectors face inconsistent requirements.
  - Global standards and stronger technical benchmarks are needed.
- Education and workforce:
  - Expand cybersecurity education in engineering and professional programs.
  - Integrated degrees, mandatory training in service academies, and certification updates (ABET, PE, ROTC) can build capacity.

Greg Shannon Keynote: New Horizons in Cybersecurity and Risk

The presentation by Greg Shannon highlighted the imperative of using formal methods to address complex cyber risks, especially those affecting national critical infrastructure. Major cyber events are estimated to potentially cause billions in losses, even though cyber/software disasters have yet to rise to that level. The presentation framed cybersecurity challenges within four questions related to risk decisions, emphasizing that risk decisions are multidisciplinary and hinge on what outcomes we value (safety, availability, integrity, confidentiality, and long-term system resilience): What do we value? What are the options? What are the outcomes? and, What are the uncertainties? A gap in knowledge is how to reason about software, especially given uncertainties across areas like provenance, capabilities, correctness, vulnerabilities, and dependencies; yet there is a critical need to understand software behavior, which underpins many important activities. The presentation argued that formal methods, which formally analyze whole systems to prove properties, can reduce uncertainties and shift the focus from traditional post-hoc responses to preventive defense, allowing for the unambiguous specification of system properties, more rigorous risk prioritization, and supporting the development of partially certified software.

- Risk decisions are multidisciplinary and hinge on what outcomes we value (confidentiality, integrity, availability, and long-term system resilience).
- Certified software: full formal verification is costly and hard to scale; partial certification and formal methods can reduce ambiguity and enforce essential properties.
- Uncertainties in software and systems:
    - Provenance & pedigree — Where the software came from, who developed it, and whether the supply chain is trustworthy.
    - Capabilities — What the system is able (or not able) to do in practice.
    - Correctness — Whether the software functions as intended.
    - Specification — How well requirements are defined, clear, and complete.
    - Vulnerability — Known or unknown weaknesses in the system.
    - Exploitability — How easily vulnerabilities can be used by attackers.
    - Dependencies — Reliance on third-party code, libraries, or systems outside one's control.
- Current practice relies on post-hoc protections (patching, mitigation, recovery), but systemic risks require more proactive approaches.

- Formal methods can help move from reactive to preventive security—clarifying assumptions, supporting compliance, and adapting long-lived systems.
- Policy and organizational change are needed: align incentives, address workflow barriers, and strengthen standards while avoiding "moral hazard" in certification.

Panel: Perspectives on Risk

Panelists: Sarah Scheffler (chair) Derek Brown, Mark Hairston, Jim Gillespie

The risk panel highlighted the complexity of defining, prioritizing, and managing cyber risk across sectors. Participants noted that organizations often underestimate exposures due to blind spots in legacy systems, supply chains, and third-party IT providers. Risk modeling remains uneven: while compliance frameworks can establish baselines, they often fail to capture systemic or cascading risks. Insurance was seen as both a driver of better practices—by incentivizing basic controls—and a source of distortion, as exclusions and shifting market dynamics can discourage long-term investment. Panelists agreed that effective risk management requires moving beyond high-level modeling to continuous testing, cross-department engagement, and closer alignment between technical realities, business processes, and policy incentives.

- Cyber risk extends beyond technology; it includes industrial operations, business software, third-party providers, environmental factors, and human safety.
- Legacy systems remain vulnerable: older operational technology requires remediation, segmentation, and continuous monitoring.
- Insurance as a driver and a challenge:
    - Cyber is now one of the largest business exposures, with average costs often unsustainable.
    - Basic controls significantly reduce risk, but compliance alone does not equal security.
    - Exclusions in policies (e.g., "acts of war") create uncertainty and may limit coverage.
- Slow adaptation: both government and industry move cautiously, leaving gaps between evolving threats and implemented protections.
- Risk modeling and testing: high-level models are useful but insufficient; real progress comes from testing attack surfaces and simulating cascading failures.
- Supply chains and dependent businesses create systemic risks where one failure cascades into many.
- Emerging technologies:
    - AI introduces new opportunities (threat detection, code review) but also risks (data misuse, unanticipated vulnerabilities).
    - Quantum computing may disrupt encryption standards.

- Organizational dynamics:
  - Cybersecurity is not just a technical problem—it requires understanding workflows, business priorities, and building relationships across departments.
  - Misaligned incentives or reliance on insurance alone can lead to underinvestment in real protections.

Panel: Certification and Policy

Speakers: Cheri Caddy (chair), Chad Heitzenrater, Zia Hydari, Sam Perl

The certification and policy panel explored what it means to certify in a dynamic cyber environment and who should bear responsibility for doing so. Participants agreed that certifications can provide value but risk becoming static and ineffective if treated as one-time snapshots. Instead, certification must be a continuous process, balancing cost and rigor while adapting to evolving threats. The discussion also underscored collective action challenges: government is uniquely positioned to set baseline expectations, but effective certification requires aligned incentives, trusted auditors, and accountability mechanisms. Questions of liability—especially in the context of AI-generated software and open-source tools—emerged as unresolved but increasingly urgent.

- Meaning of certification:
  - Multiple interpretations exist—certifying processes vs. certifying outcomes.
  - Risk reduction value depends on the standard used; must go beyond "check-the-box" compliance.
  - Trade-offs between cost, intensity of verification, and usefulness.
- Challenges with static certification:
  - Certifications are snapshots in time; adversaries adapt quickly.
  - Processes can become stagnant if not updated continuously.
  - Need for dynamic or continuous certification models that reflect real-world change.
- Policy and incentive alignment:
  - Policies should create clear, unambiguous expectations while avoiding ambiguity that weakens enforcement.
  - Incentives must fall on those with the ability to address risks.
  - Risk of moral hazard: certifiers themselves need oversight.
- Scaling certification:
  - Difficult for smaller organizations to meet requirements without external support.
  - Automation and AI may eventually assist, but current systems are trained on insecure code.
  - SaaS and cloud services offer potential platforms for scalable certification.
- Liability and safe harbor:
  - Growing debate over where liability should lie—vendors, users, or intermediaries.
  - Software often licensed rather than sold, creating accountability gaps.

    - Safe harbor provisions may provide protection but also risk undermining responsibility.
- Ecosystem implications:
    - Defense and critical infrastructure face "structured insecurity" due to reliance on diverse suppliers.
    - Effective certification requires investment in training, infrastructure, and processes across the supply chain.
    - Certification must keep pace with emerging technologies (e.g., AI-written software, quantum computing).

Rob Cunningham Interactive Discussion: Designing the Future of Cybersecurity

In the interactive discussion, participants identified key gaps and opportunities for advancing cybersecurity. They emphasized the need for better data on adversaries, supply chain maturity, and the effectiveness of controls, along with improved frameworks for risk modeling, secure engineering, and workforce training. Policy priorities included harmonized standards across sectors, clear minimum requirements, updated liability laws, and mechanisms for safe information sharing. Looking ahead, participants underscored the importance of universities, labs, federal agencies, and industry each playing distinct but complementary roles, and recommended starting with small, concrete steps to build momentum and trust across stakeholders.

- Data Needs
    - More granular intelligence on adversaries: who they are, where they operate, and attack methods.
    - Supply chain visibility and maturity assessments of vendors/technologies.
    - Metrics to measure likelihood and impact of incidents (e.g., costs of losses, insurance vs. control investments).
    - Real-world evidence: attack vectors, system-level risks, failure modes, downstream impacts.
    - Usage data on how organizations and individuals interact with technology.
    - Information that links attack success or failure to impact and usage of different controls and tools
- Frameworks and Tools
    - Stronger methods for risk quantification and effective assessment.
    - Tools for mapping system-level risks across interconnected infrastructures.
    - Better integration of formal methods and model-based approaches into practice.
    - Automation, scalable solutions, and continuous monitoring to address dynamic threats.
    - Practical guidance on bridging IT/OT environments and ensuring interoperability.

- Laws, Regulations, and Policies
  - Harmonization of regulatory regimes across sectors (avoiding fragmented requirements).
  - Standards that are practical, enforceable, and adaptable to fast-changing threats.
  - Clarification of liability and responsibility for cyber failures.
  - Policies to support information sharing and reduce barriers to cross-sector collaboration.
  - Consideration of economic levers (e.g., insurance, incentives) to encourage proactive investment.

Welcome to the

TRANSFORMING CYBERSECURITY WORKSHOP

Hosted by

PITT CYBER & CYBER ENERGY CENTER

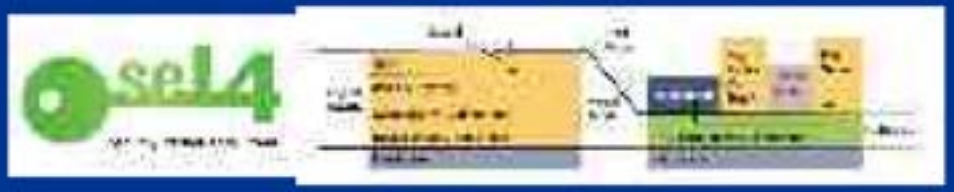
Welcome & Thank you for Coming

Daniel G. Cole, dgcole@pitt.edu
Erica Owen, ericaowen@pitt.edu

Cyber Energy Center,
cyberenergy@pitt.edu
Pitt Cyber, cyber@pitt.edu

University of Pittsburgh.
Cyber Energy Center

This workshop arose from asking the question,
"What if we could change cyber risk by orders of magnitude?"



University of Pittsburgh
Cyber Energy Center

The goal of this workshop is to explore how technological innovation, policy development, and better risk modeling can be used to develop new strategies that reduce cyber risks and enhance resilience.

University of Pittsburgh.

Cyber Energy Center

Time	Duration	Description	Speakers
8:30am	30 min	Gathering w/ Continental Breakfast	
9:00am	15 min	Welcome, Introductions, and Overview	Dan Cole, Pitt Erica Owen, Pitt
9:15am	60 min	Keynote: Transforming Cybersecurity	Cheri Caddy, McCrary Institute
10:15am	30 min	**Break**	
10:45am	60 min	Keynote: New Horizons in Cybersecurity and Risk	Greg Shannon, INL
11:45am	60 min	**Lunch**	
12:45pm	60 min	Panel #1: Perspectives on Risk	Derek Brown, EQT Jim Gillespie, GrayMatter Mark Hairston, Seubert & Associates Sarah Scheffler*, CMU
1:45pm	15 min	**Break**	
2:00pm	60 min	Panel #2: Certification and Policy	Chad Heitzenrater, RAND Pgh Zya Hydari, Pitt Sam Perl, CMU SEI Cheri Caddy*, McCrary Institute
3:00pm	15 min	**Break**	
3:15pm	60 min	Interactive Discussion: Designing the Future of Cybersecurity	Rob Cunningham*, Pitt
4:30pm		**Adjourn**	**Designates Discussion Chair*

Transforming Cybersecurity

Cheri Caddy
Senior Cybersecurity Fellow, McCrary Institute for Cybersecurity & Critical Infrastructure at Auburn University;
former Deputy Assistant National Cyber Director for Research & Technology, the White House

University of Pittsburgh.
Cyber Energy Center

TRANSFORMING CYBERSECURITY

CHERI CADDY

SENIOR CYBERSECURITY FELLOW, MCCRARY INSTITUTE FOR CYBERSECURITY & CRITICAL INFRASTRUCTURE AT AUBURN UNIVERSITY

FORMER DEPUTY ASSISTANT NATIONAL CYBER DIRECTOR FOR RESEARCH & TECHNOLOGY, THE WHITE HOUSE

TOPICS

- About
- The Challenge of Transformation in Cyber
- Ecosystem Focus
- Left of Boom
- Risk Reallocation
- Outlook

ECOSYSTEM FOCUS

- Stakeholders, Authorities, and Policy
- Cyber-Physical Systems
- An Example: Connected Vehicles

CYBER ROLES & RESPONSIBILITIES

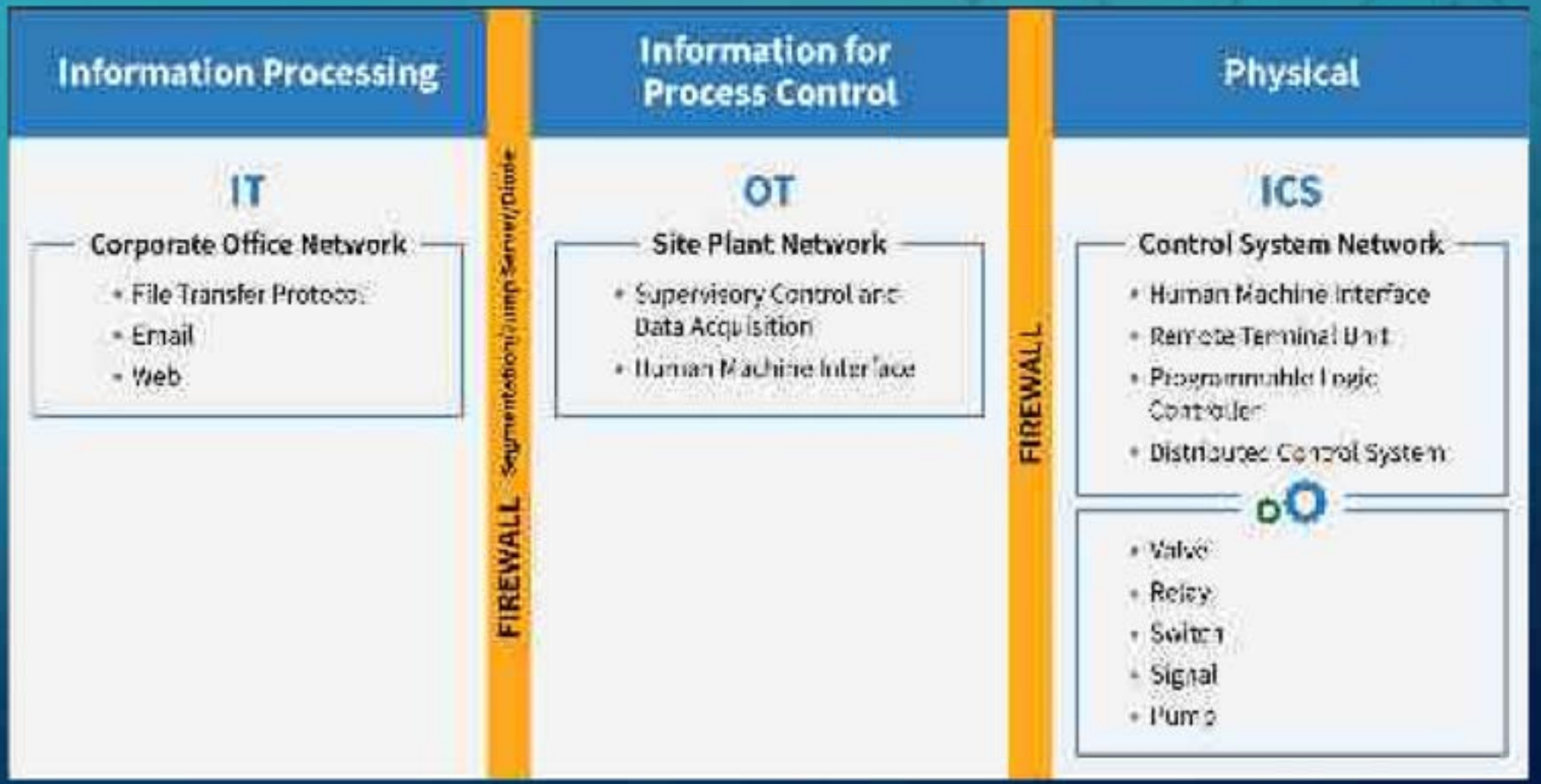
- National Security Memo 22

https://bidenwhitehouse.archives.gov/briefing-room/presidential-actions/2024/04/30/national-security-memorandum-on-critical-infrastructure-security-and-resilience/ /

EXAMPLE - ENERGY SECTOR INTERDEPENDENCIES

Securing Cyber Assets: Addressing Urgent Cyber Threats to Critical Infrastructure - NIAC

CYBER-PHYSICAL SYSTEMS - IT VS. OT NETWORKS



IT VS. OT/INDUSTRIAL CONTROL SYSTEMS RISKS AND THREATS

	IT	OT & ICS
Operators	CIO, CISO, Analysts	Plant Manager, Control Engineer, COO
Business Priority	Confidentiality	Availability
Major Focus	Data Integrity	Zero Downtime for Control Processes
Protection Targets	Windows Computers, Servers	Industrial Components (PLCs, HMIs)
Environmental Conditions	Air-conditioned	Harsh Environments (extreme temperatures, vibrations, shocks)
Lifecycle	Software Updated Continuously	Firmware in place for decades

IT Threat Emphasis	OT Threat Emphasis
• Unauthorized information disclosure • Unauthorized data alteration • Impaired data availability	• Injury & environmental disaster • Damaged equipment & physical process downtime • Unauthorized information disclosure

INTERDEPENDENCES EXAMPLE– CONNECTED VEHICLES

IT-OT converged endpoint device

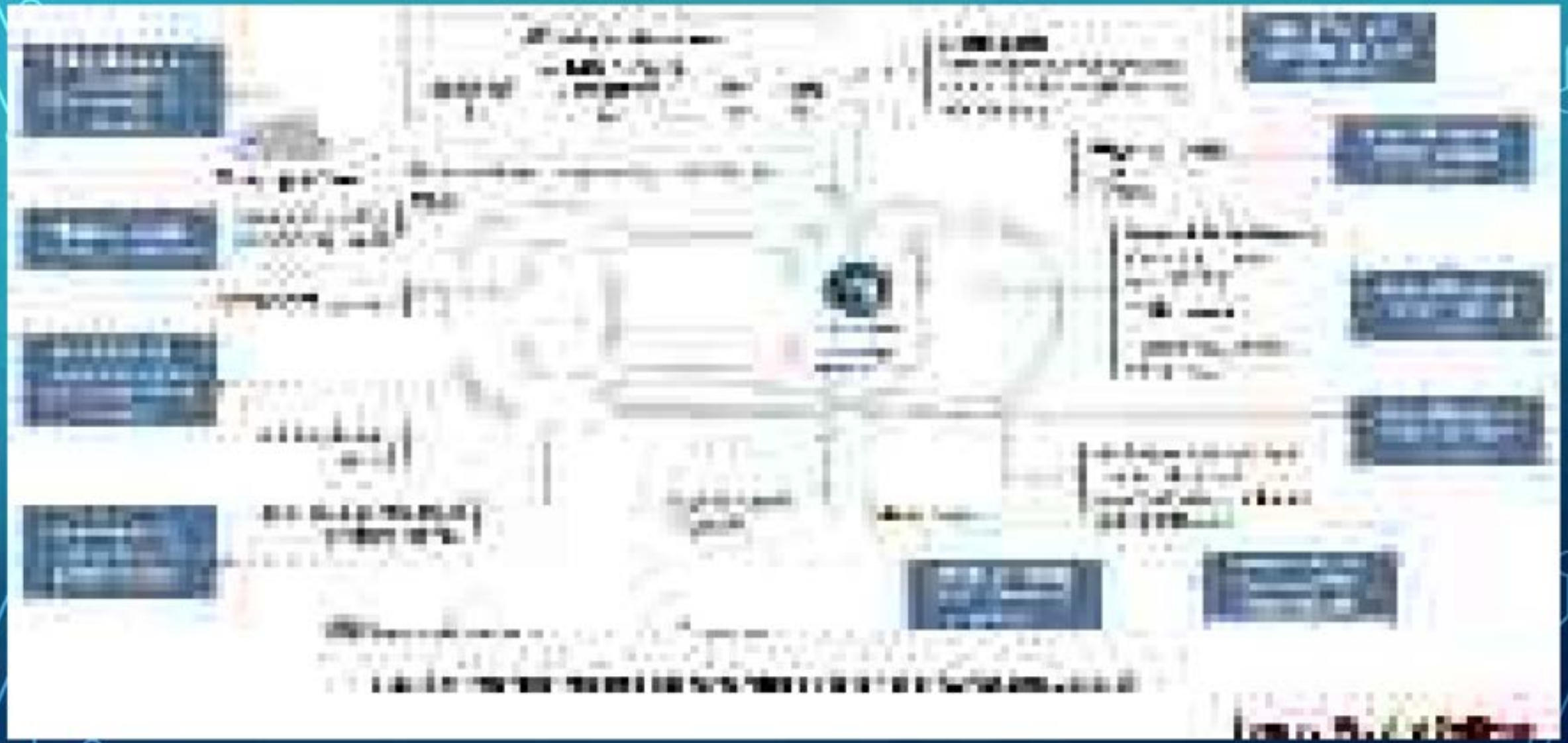
Sectors Implicated:

- Energy
- Transportation
- Critical Manufacturing
- IT
- Communications
- Financial Services

Technologies:

- WiFi
- Bluetooth
- Cloud
- AI/ML

CYBERSECURITY VULNERABILITIES AND CONNECTED VEHICLES



https://www.frost.com/growth-opportunity-news/new-opportunities-and-vehicle-architectures-how-upcoming-cybersecurity-regulations-will-transform-the-connected-car-ecosystem/

(U) VEHICLE DATA IS GROWING & GRANULAR

Vehicle data

- Vehicle information
  - Fuel data
  - Tire pressure
  - Maintenance events
  - Mileage
  - Visual image/video data
- External information
  - Road and weather conditions
  - Surrounding vehicle detection
  - Lane crossing
  - Visual image data

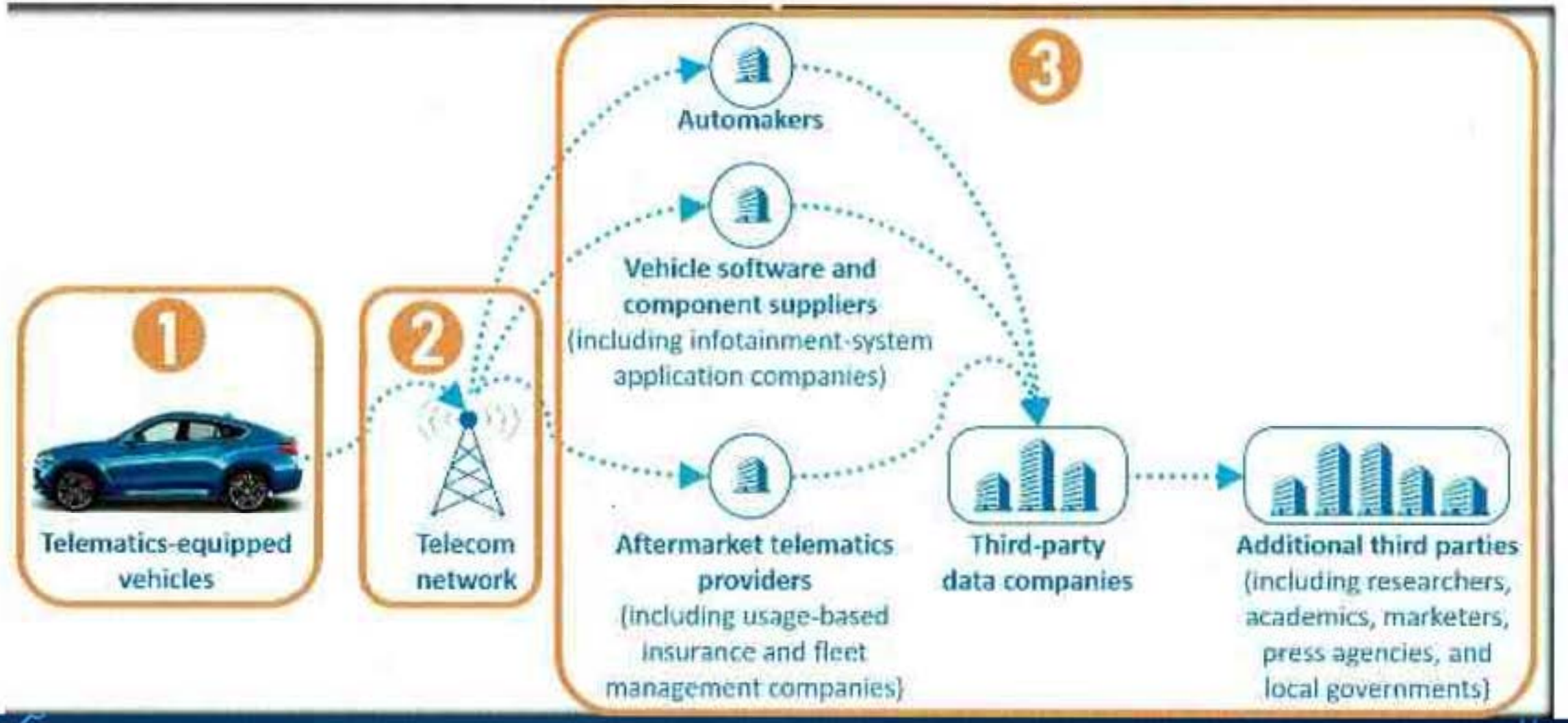
User-generated vehicle data

- Vehicle performance
  - Home address
  - Work address
  - Most visited restaurants, convenience, and other businesses
- Driving behavior
  - Speed
  - Acceleration and braking patterns
  - Seatbelt usage
  - Driving performance
  - Eye-tracking and head movement detection

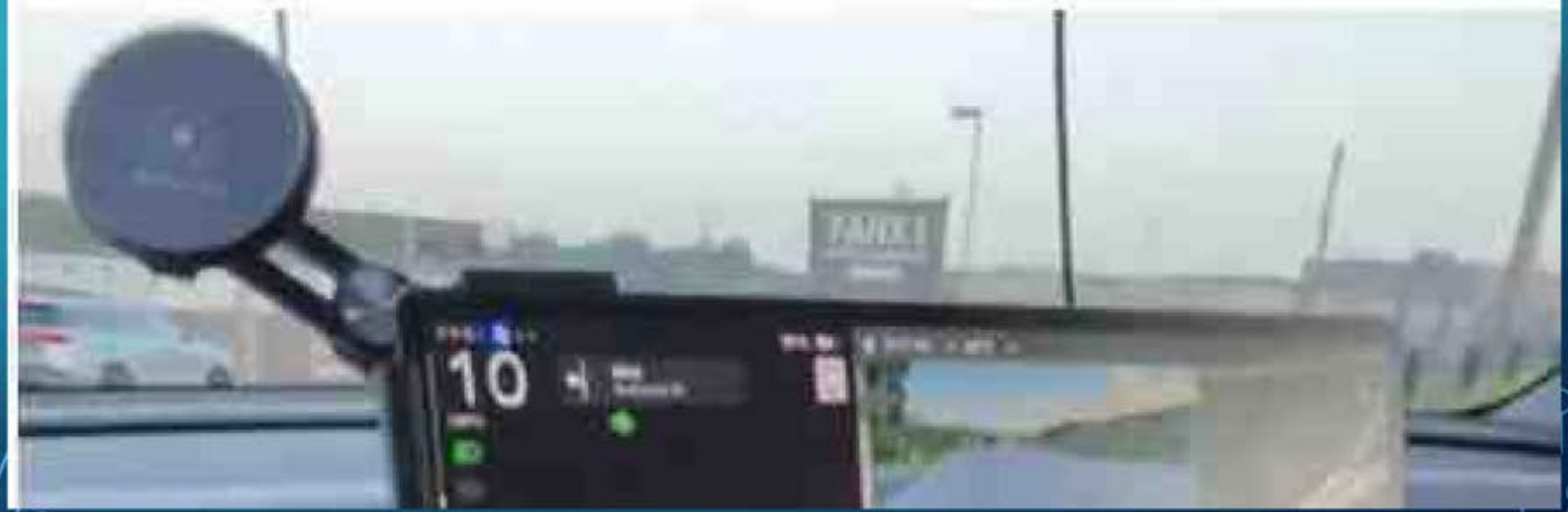
User-generated data

- Personal information
  - Name and birthdate
  - Driver's license
  - Family and close acquaintances
  - Text messages and emails
  - Body weight
  - Music preferences
  - Any data contained in third-party applications connected to vehicle
- Financial information
  - Credit card information

(U) VEHICLE TELEMATICS DATA FLOW



US intel agency revlewing Grok vldeo filmed during man's commute to secure NSA facility



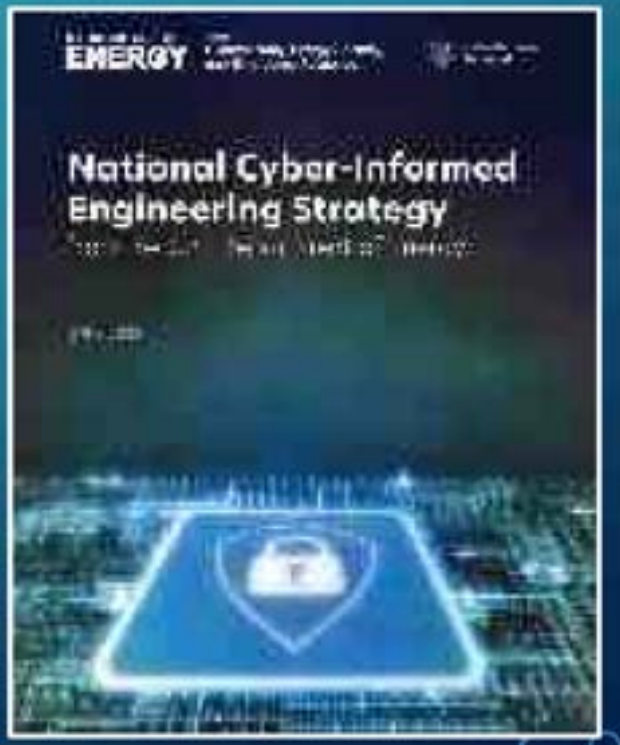
LEFT OF BOOM

- Security by Design
- Cyber-Informed Engineering

CIE AND THE SYSTEMS ENGINEERING LIFECYCLE

NATIONAL CYBER-INFORMED ENGINEERING STRATEGY

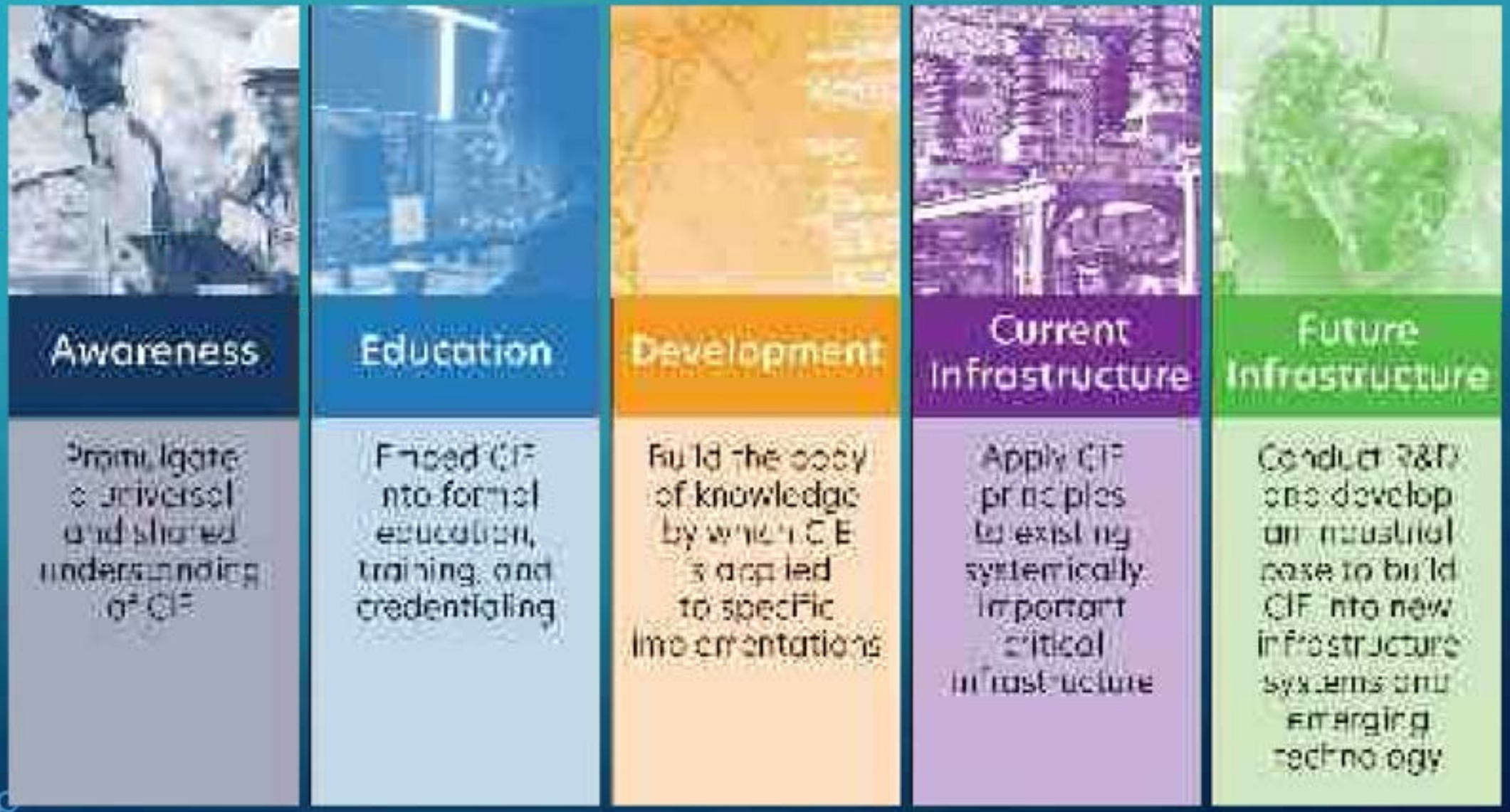
- Directed by Congress in the 2020 National Defense Authorization Act
- Five integrated pillars incorporate CIE as a common practice for engineers and engineering technicians
- Drives collective action among diverse stakeholders



Cyber-Informed Engineering

- Uses **design decisions and engineering controls** to eliminate or mitigate avenues for cyber-enabled attack
- Aims to **"engineer out" cyber risk** throughout the design and operation lifecycle, rather than add cyber controls after the fact
- Focused on **engineers and technicians**, CIE provides framework for cyber education, awareness, and accountability
- Creates a **culture of security** aligned with the existing industry safety culture

PILLARS OF THE CYBER-INFORMED ENGINEERING STRATEGY



RISK REALLOCATION

- Changes in Public-Private Partnerships in Cybersecurity
- Future of Cybersecurity Regulations and Standards

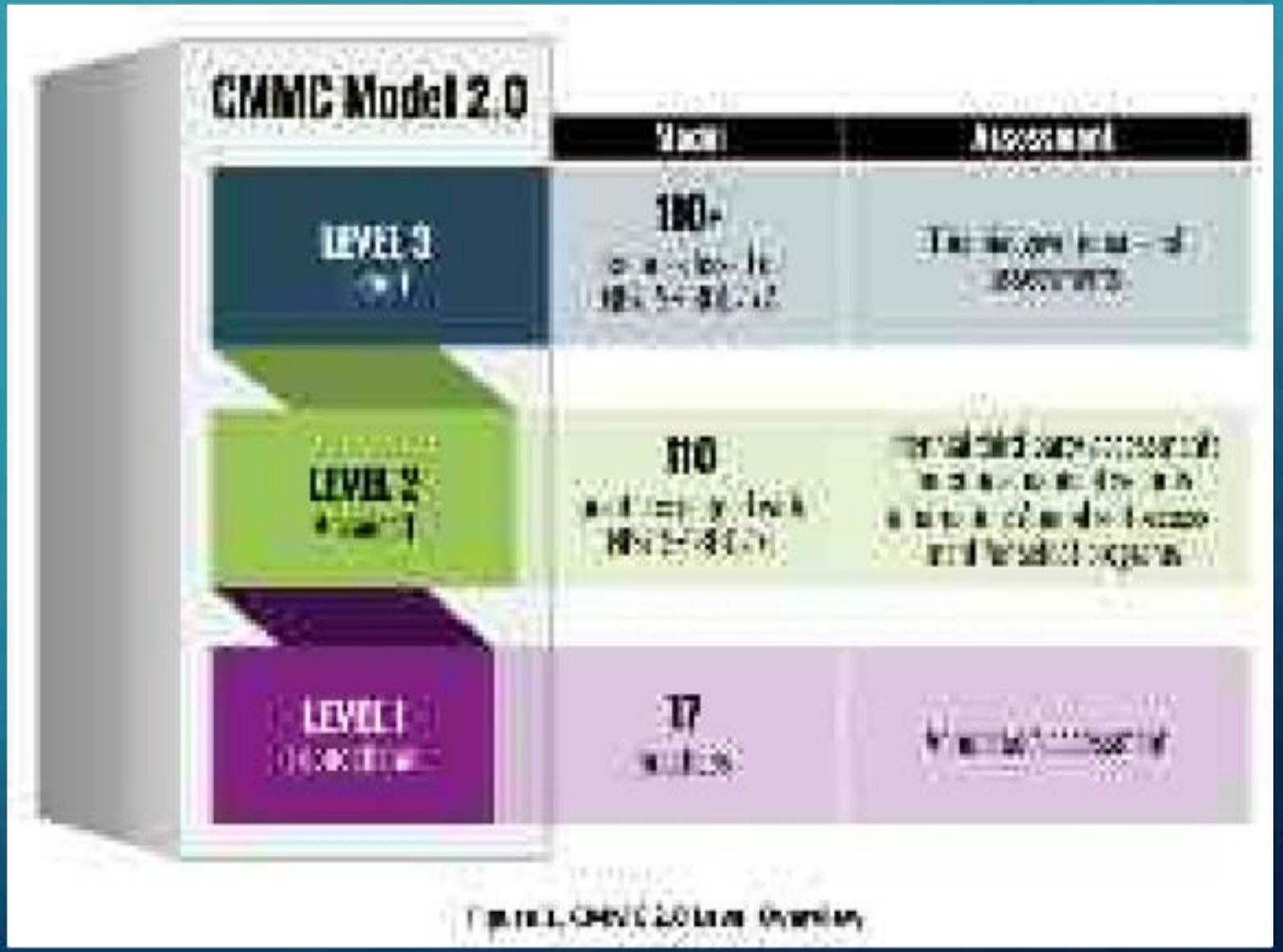
NATIONAL STANDARDS STRATEGY FOR CRITICAL AND EMERGING TECHNOLOGY

- Reinforces U.S. Government support of the private sector-led, open, consensus-based international standards system and strengthens the rules-based processes of relevant organizations

- Growing global interest in emerging areas of standardization demands a new level of coordination and effort internationally and will require the development of new ways for public- and private-sector stakeholders to work together

CYBERSECURITY MATURITY MODEL CERTIFICATION (CMMC)

- DoD requirement, created in 2020
- Still working through 5 year phase in period
- New Software Fast Track (SWFT) program builds on CMMC



OUTLOOK FOR OT/ICS CYBERSECURITY

- Focus on Ecosystem Level
- Generate the discipline to invest more in left of boom
- Risk Reallocation

New Horizons in Cybersecurity and Risk

Greg Shannon, PhD
Laboratory Fellow and Chief Cybersecurity Scientist
National & Homeland Security Directorate
Idaho National Laboratory (INL)

University of Pittsburgh.
Cyber Energy Center


New Horizons in Cybersecurity and Risk

Dr. Greg Shannon
Laboratory Fellow
Chief Cybersecurity Scientist
August 12, 2025

INL Idaho National Laboratory

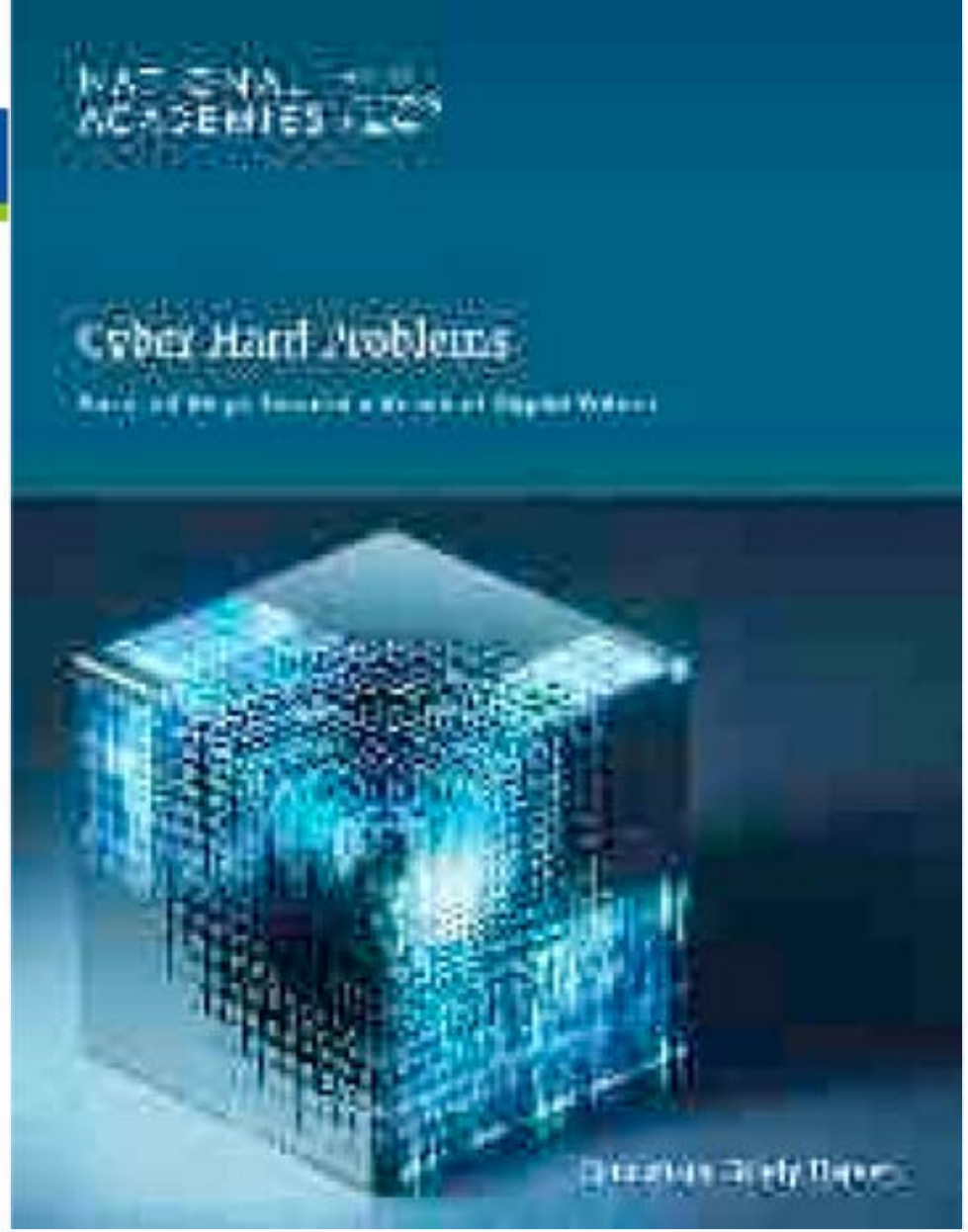
Background – www.linkedin.com/in/gregshannon

- 4 years at Idaho National Laboratory in National & Homeland Security
- 12 years to Carnegie Mellon's Software Engineering Institute
- 2014, recognized the imperative and possibility to feasibly formally prove critical properties at various scales given the tools and infrastructure
- 2016, while serving in the White House Office of Science and Technology Policy, recognized how formal methods are a strategic U.S. opportunity.
- 2020, infused formal methods/perspectives in the work of the DOE's Cybersecurity Manufacturing Innovation Institute
- 2022, led INL's efforts to formalize problems and solutions that protect key cyber-physical elements in our nation's critical infrastructures

A note on risk outcomes – Disasters

- List of disasters by cost
  - https://en.wikipedia.org/wiki/List_of_disasters_by_cost
- No cyber/software in the over $1 billon losses
  - count is ~380
- Two under one $billion
  - Both are spacecraft losses, 1962 and 1996

- The Largest and Most Notorious Cyber Attacks in History
  - https://blog.netwrix.com/biggest-cyber-attacks-in-history
  - "largest" is WannaCry with $4-8 billion in losses estimanted
  - How much of impact was actually buying down accumulated technical debt?



- CHP-1: Risk Assessment and Trust
- CHP-2: Secure Development
- CHP-3: Secure Composition
- CHP-4: Supply Chain
- CHP-5: Policy and Economic Incentives
- CHP-6: System-Human Interactions
- CHP-7: Information Provenance and Media
- CHP-8: Cyber-Physical Systems
- CHP-9: Artificial Intelligence
- CHP-10: Operational Security

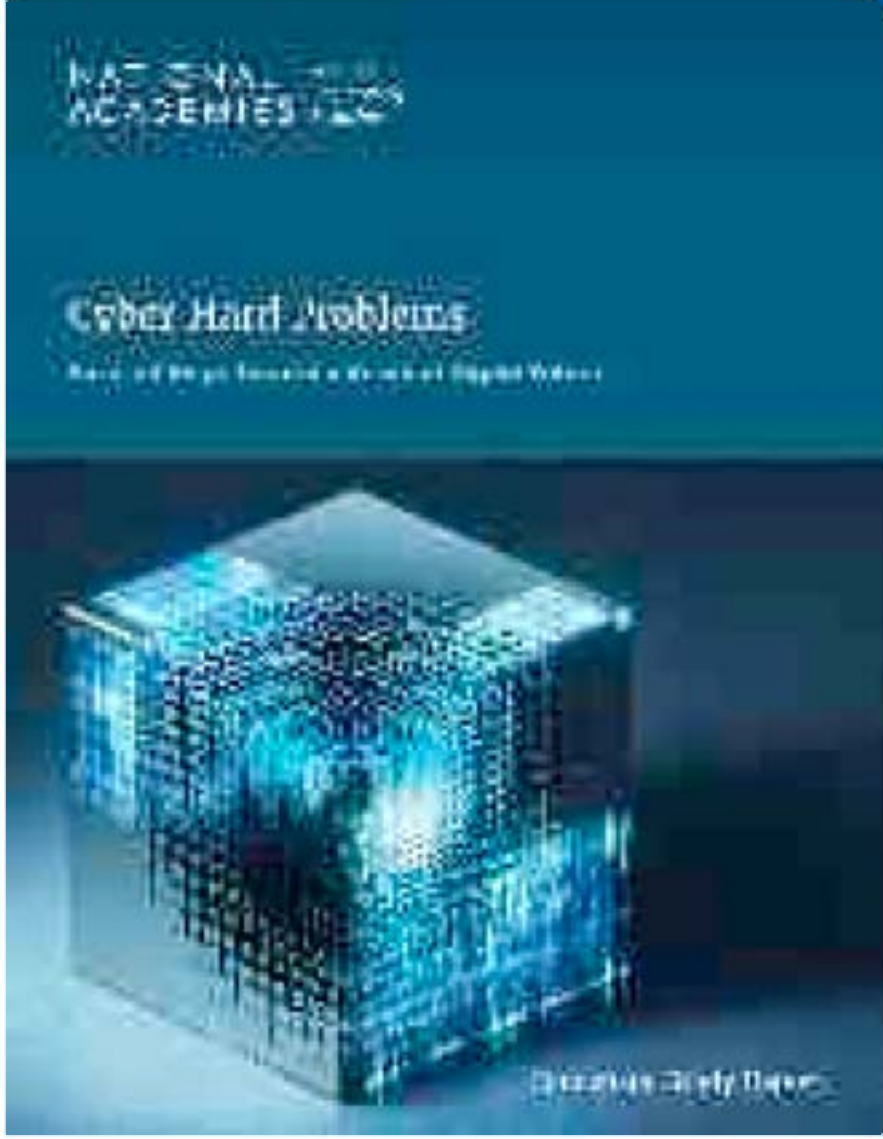
https://www.nationalacademies.org/our-work/cyber-hard-problems

CHP-1: Risk Assessment and Trust

- Cyber risk is difficult to evaluate because vulnerabilities are complex, hidden, and hard to measure with current tools.

Progress Requires

- Reliable, evidence-based approaches for **evaluating** system security
- Greater transparency from vendors to support meaningful risk **assessments**
- **Incentives** that encourage the development and sharing of assurance-related evidence



https://www.nationalacademies.org/our-work/cyber-hard-problems

Q: What's Missing?

A: What decisions are we/people trying to make?

Risk Decisions – Very Multidisciplinary

Risks involve threats to outcomes that we value.

0. What do we value?
1. What are the options?
2. What are the outcomes?
3. What are the uncertainties?

- Normative Analysis
  - Ideal decisions
- Descriptive Analysis
  - Actual decisions
- Prescriptive Analysis
  - Influencing decisions

Fischhoff, B., & Kadvany, J. (2011). **Risk: A very short introduction**. Oxford University Press. https://academic.oup.com/book/454

What is "Certified" Software for Our Discussion

- Ideally, Certified means formally analyzed whole systems shown to possess provable properties relative to a set of assumptions.
  - Complete is that a system does what is specified and only that
    - This traditionally is hard, expensive, time consuming, limits to scalability
  - Partial is that a model of a system (and its software) has a given property such as:
    - No buffer stack overflows, CWE-121
    - No external leakage of private data without consent
    - All key functions used only by recently authenticated entities
    - Remote update is completely secure
  - The most useful Certifications are those that can be easily or reproducibly verified
- There are other definitions of certified
  - Inspected, analyzed, conformed to standards, tested

Decades of Work Coming to Fruition in Formal Methods in Cyber

- DARPA work highlighted at their recent event on Resilient Software Systems
  - https://creative.spa.com/darpa/i2o/resilient-software-systems-colloquium/index.php?p=agenda
  - 13 video's here https://www.youtube.com/@DARPAtv/videos starting with DARPA Keynote: Forging a New Era of Cyber Resiliency)
  - DAPRA's FMs landing page: https://www.darpa.mil/research/research-spotlights/formal-methods
- Amazon's Web Services (AWS) work over the years
  - Tools: https://www.amazon.science/tag/formal-verification
  - Videos & articles, https://aws.amazon.com/security/provable-security/resources/
  - https://www.amazon.science/publications/how-amazon-web-services-uses-formal-methods
  - Byron Cook: Formal Reasoning about the Security of Amazon Web Services https://www.youtube.com/watch?v=JfjLKBO27nw

What do we Value?

- Traditionally – Information Security
  - Confidentiality, Integrity, Availability
- What has evolved in what we value?
  - Cyber-physical aspects of critical infrastructure
    - E.g., power grid, water systems, pipelines, etc.
  - Macro values and impacts
    - Scale of use
    - Longevity of use

How do formal methods change what we value?

- Be unambiguous in what we mean for essential system properties
- Feasibly enforce values or elements that protect values
- We can value understanding the **complicated** elements of **complex** systems as a path to reducing risk

What are the Options?

- Traditionally focused on:
  - Point-wise testing
  - Vulnerability discovery
  - Compliance & Process
- Accept ambiguities in software
  - Provenance and Pedigree
  - Capabilities
  - Specification & Correctness
- Ignore software cyber risks till one can't
  - Post-hoc protections **(our world today)**
- Other emerging options
  - Model based systems engineering
  - Generative AI, large language models

How do formal methods change what are the Options?

- Formalize policy to ensure compliance
- Efficiently handle the correctness of complicated software
- See more clearly the risks in the remaining system complexity
- Property assertions can be easily / reproducibly verified
- Agility to update systems and preserve critical properties
- Reason about human behaviors more rigorously

What are the Outcomes?

- Traditionally, most cybersecurity efforts focus on post-hoc responses.
  - Responding to new vulnerabilities
  - Managing 100's of thousands of old vulnerabilities
  - Large human (or AI) capabilities needed to keep systems online
  - Systems/software becomes brittle with scale or longevity
- Adversaries have lots of material to work with and are too easily **successful**
  - Vulnerabilities, Weaknesses
  - Humans
  - Salt Typhoon, Volt Typhoon

How do formal methods change what are the Outcomes?

- Easier to prioritize risks/incidents given more specificity on what's valued
- Adversaries use more resources to achieve their outcomes
  - Harder to find executable paths to impact

What are the Uncertainties?

- Traditionally, ambiguity in
  - Provenance and Pedigree
  - Capabilities
  - Correctness
  - Specification
  - Vulnerability
  - Exploitability
  - Dependencies
- Complexity
  - Esp. emergent properties

How do formal methods change what are the Uncertainties?

- Allows us to reduce uncertainties in risks that most threat what we value
- Efficiently apply “slow thinking” (reasoning) to what we value
  - vs. fast thinking of GenAI

Implications for Risk Analysis and Formal Methods (FM's)

- Normative Analysis (Ideal decisions)
  - What are the most impactful uses of FM's?
  - What are the longitudinal implications for risk decisions?
- Descriptive Analysis (Actual decisions)
  - Why are FM's adopted in reducing risk?
  - How were FM's adopted in reducing risk?
- Prescriptive Analysis (Influencing decisions)
  - What are policies to encourage the use of FM's to reduce risk?
  - What are the barriers to using FM's to reduce risk?

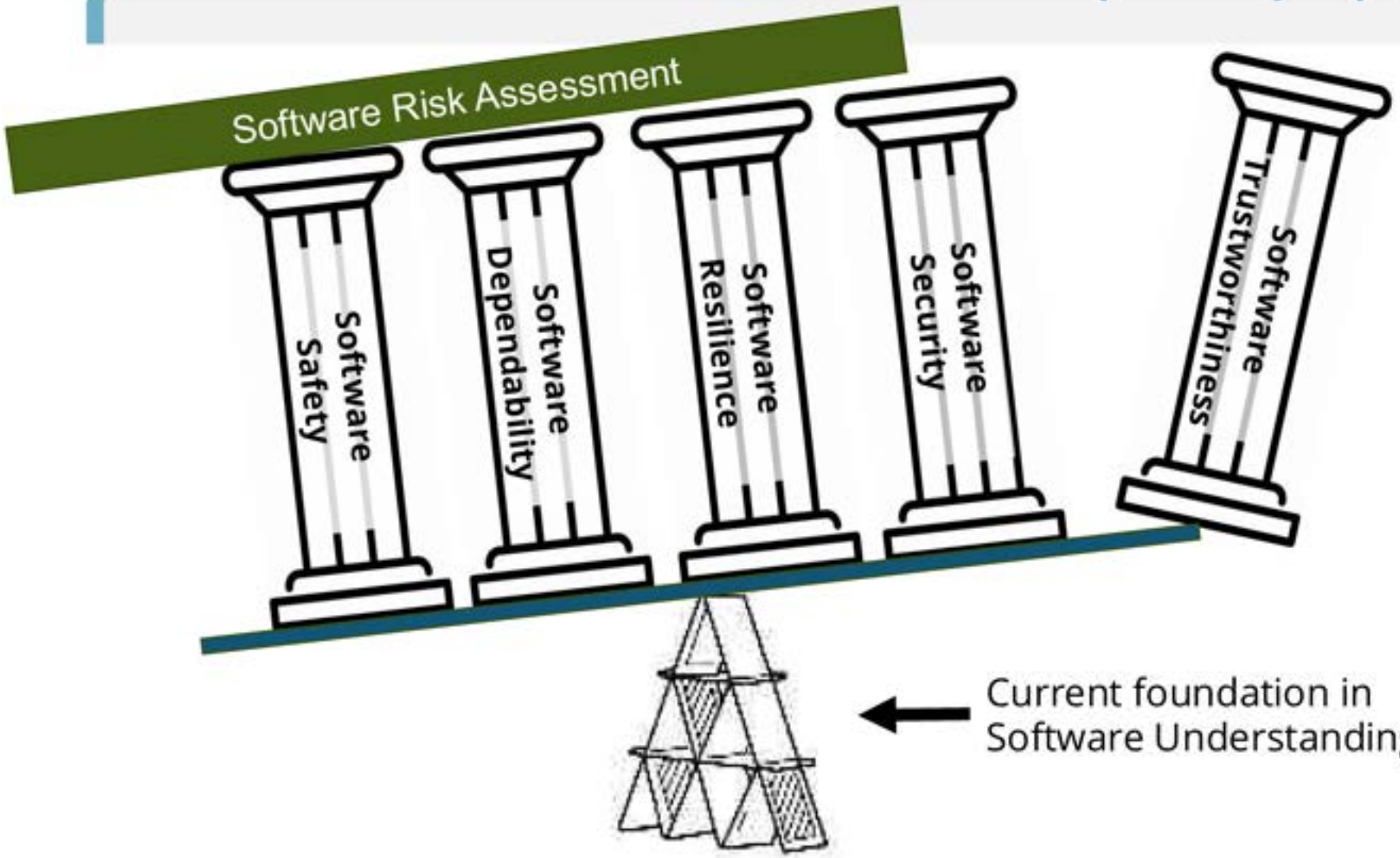
For further multidisciplinary discussion

What do we value?
What are the options?
What are the outcomes?
What are the uncertainties?

- Analysis always has assumptions and simplification, how do we ensure the use of FM's still reduces risk?
- Assumptions and semantic gaps become key attack surfaces
- How do we get decision makers comfortable with the highly abstract foundations of using formal methods?
- How do we engineer long-lived systems to be able to incorporate new risk/security protections continuously?

Gap: *Missing Foundation for Reasoning About Software*

- **The need to understand software behavior underpins many important activities.**



Malware detection
Ransomware prevention
Software forensics
Vulnerability research
Safety assessments
Software maintenance
Malicious indicator extraction
…

Courtesy of Doug Ghormley, Christopher Harrison at Sandia National Laboratories

SUNS History: *Overview*

- **The USG has been wrestling with software understanding challenges for decades. Recently, efforts have focused on defining challenges, needs, and opportunities.**

Presents a technical research, development, and engineering roadmap to enable the U.S. government to achieve greater software understanding.

Defines a call to action for the U.S. government to take decisive and coordinated action to close the software understanding gap.

The forum served as the "launch event" for the "Closing the Software Understanding Gap" whitepaper.

Outlines the challenges of software understanding for NS&CI missions, discusses the shortcomings of traditional investment approaches, documents the outcomes of the SUNS 2023 Workshop and concludes with recommendations.

Courtesy of Doug Ghormley, Christopher Harrison at Sandia National Laboratories

These documents are available at https://suns.sandia.gov/

A note on risk outcomes – Disasters

- List of disasters by cost
  - https://en.wikipedia.org/wiki/List_of_disasters_by_cost
- No cyber/software in the over $1 billon losses
  - count is ~380
- Two under one $billion
  - Both are spacecraft losses, 1962 and 1996

- The Largest and Most Notorious Cyber Attacks in History
  - https://blog.netwrix.com/biggest-cyber-attacks-in-history
  - "largest" is WannaCry with $4-8 billion in losses estimanted
  - How much of impact was actually buying down accumulated technical debt?

Perspectives on Risk

Derek Brown, EQT
Jim Gillespie, GrayMatter
Mark Hairston, Seubert & Associates
Sarah Scheffler, CMU (Chair)

University of Pittsburgh.
Cyber Energy Center

Certification and Policy

Chad Heitzenrater, RAND Pittsburgh
Zia Hydari, Pitt
Sam Perl, CMU SEI
Cheri Caddy, McCrary Institute (Chair)

University of Pittsburgh.
Cyber Energy Center

Designing the Future of Cybersecurity

Robert K. Cunningham, PhD
Vice Chancellor for Research Infrastructure
University of Pittsburgh

University of Pittsburgh.
Cyber Energy Center

Thank you for attending

Hosted by

PITT CYBER & CYBER ENERGY CENTER

Daniel G. Cole, dgcole@pitt.edu
Erica Owen, ericaowen@pitt.edu

Cyber Energy Center,
cyberenergy@pitt.edu
Pitt Cyber, cyber@pitt.edu

TRANSFORMING CYBERSECURITY

A MULTIDISCIPLINARY APPROACH TO RISK, TECHNOLOGY, AND POLICY

University of Pittsburgh.
Cyber Energy Center