CYBERSECURITY AT MIT SLOAN (CAMS)

THEMES SHAPING Q4 AT CAMS

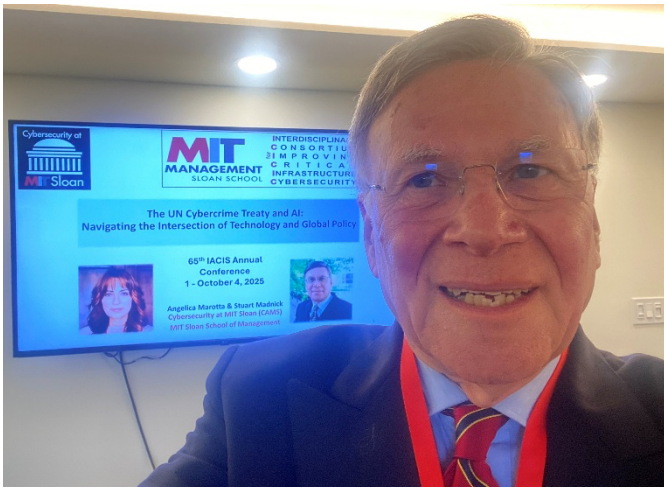
AI as a Systemic Risk Actor
Research examining AI not merely as a tool, but as an autonomous participant in cyber incidents, with implications for accountability, regulation, and control.

Limits of AI in Cyber Risk Management
Empirical and theoretical work identifying where AI underperforms, particularly in small, noisy, and critical-infrastructure data environments.

Governing Cyber and AI Risk at Scale
Advancing frameworks that connect systemic cyber risk, financial resilience, and institutional governance across interconnected systems.

AI, CYBERCRIME, AND THE LIMITS OF GLOBAL GOVERNANCE

CAMS research continues to examine the growing mismatch between AI-enabled cyber threats and existing legal frameworks. This work is reflected in recent research by Stuart Madnick and Angelica Marotta, awarded Best Paper at the 2025 International Association for Computer Information Systems (IACIS) Conference.



Their paper, *"The UN Cybercrime Treaty and AI: Navigating the Intersection of Technology and Global Policy,"* evaluates the United Nations Convention against Cybercrime against the realities of AI-driven cyber risk. Drawing on an analysis of more than 70 documented AI-related cyber incidents from 2023 to 2025, the study assesses how well current treaty provisions address threats that routinely cross-national boundaries.

The findings show that AI increasingly acts as an autonomous participant in cyber incidents, complicating regulatory assumptions around intent, attribution, and responsibility. By identifying where the UN Cybercrime Treaty aligns with emerging risks—and where gaps remain—the research informs global discussions on how cyber governance must evolve in response to AI, advancing CAMS' work at the intersection of AI, cyber risk, and governance.

ADVANCING CYBER RISK SCIENCE AT THE 2025 WINTER SIMULATION CONFERENCE

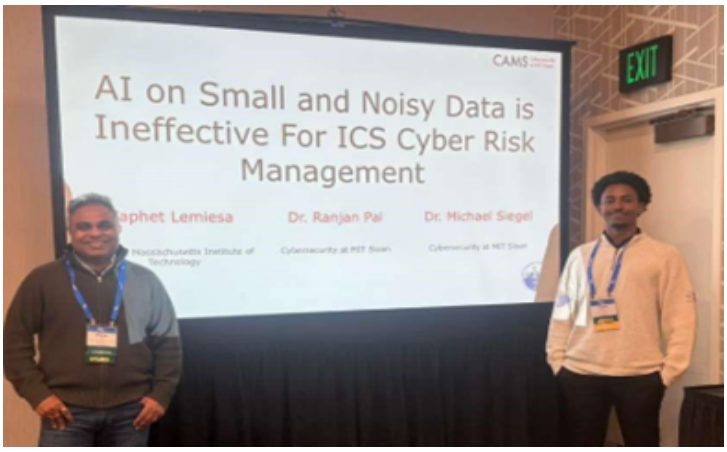


Photo of Dr. Ranjan Pal with MIT student Yaphet Lemiesa at the 2025 Winter Simulation Conference in Seattle WA.

CAMS research was prominently represented at the 2025 **Winter Simulation Conference, held in Seattle and co-sponsored by INFORMS**. CAMS researchers contributed four papers to the conference program, reflecting the ongoing work at the intersection of cyber risk, artificial intelligence, and resilience.

Among these contributions, *"AI on Small and Noisy Data Is Ineffective for ICS Cyber Risk Management,"* a paper led by Yaphet Lemiesa, a CAMS student and first author, and co-authored with Ranjan Pal and Michael Siegel, was recognized as a **Best Paper Award finalist in AI.** The research examines the limits of AI-driven approaches to cyber risk management in industrial control systems (ICS).

In addition to presenting research, Ranjan Pal was invited to speak on his work exploring how catastrophic bonds can be used to strengthen capital availability in cyber insurance markets. His presentation examined the role of financial instruments in supporting systemic cyber resilience, extending CAMS research beyond technical risk modeling to the institutional and economic structures that shape cyber risk management at scale.

STUART MADNICK AT ICIS 2025 AND MISQE WORKSHOP

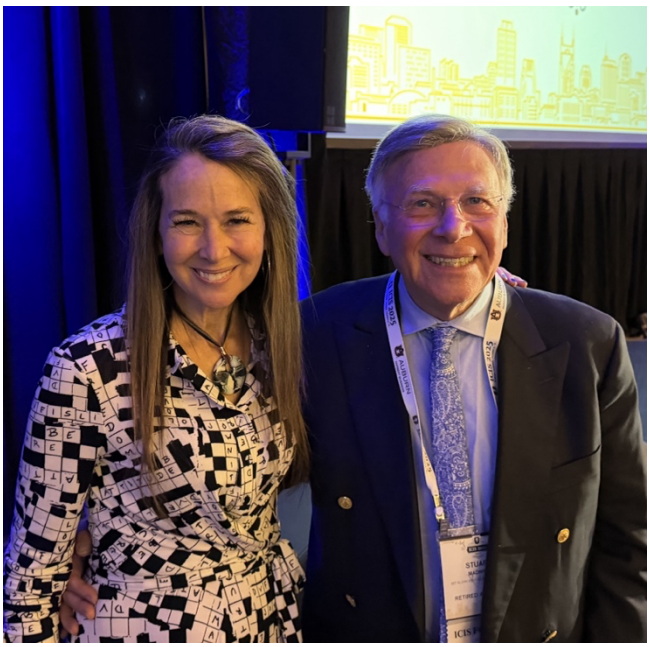


Photo of Stuart with Jan Easterly, former director of CISA, at International Conference on Information Systems (ICIS) in Nashville, Tenn.

CAMS was active at both ICIS 2025 and the MISQE Workshop. Stuart met with Jan Easterly, a noted American cybersecurity expert and had served as the Director of the Cybersecurity and Infrastructure Security Agency (CISA), where she led the nation's efforts to protect critical infrastructure from cyber and physical threats, transforming the agency into a $3 billion powerhouse with over 10,000 employees and contract personnel. She gave the keynote "fireside chat" at ICIS. Much emphasis on the benefits of AI for both the defenders … and the attackers.

Prof Madnick also co-led the MISQE workshop session on AI Technical Architecture, Security and Developer Experience. Specific topics addressed the Business Case for Small, local models in Agentic AI, Bridging the GenAI Divide with Enterprise Architecture Management, and Augmenting Enterprise Architecture: Generative AI in Managing Legacy Complexity.

CAMS FRIDAY RESEARCH DISCUSSION — OPEN TO ALL

Fridays, 11:30am–12:30pm ET (online via Zoom). You don't need to be a CAMS member to join. Each week features new cyber & AI topics, learn what others are doing, test your ideas, and meet collaborators. It's also a great first step into the CAMS community.

To attend: email us at mitcyber@mit.edu or visit https://cams.mit.edu for details and upcoming topics.

CAMS RAPID RESPONSE SESSIONS ON AI, QUANTUM, AND CYBER RISK

In November, CAMS convened a series of Rapid Response Session, available to CAMS Members via Zoom, to examine how emerging technologies, particularly artificial intelligence and quantum computing, are reshaping cyber risk, governance, and resilience. The sessions were designed to address research-driven questions about how advances in AI and quantum are shifting cyber risk from operational concerns to institutional and board-level challenges. CAMS researchers examined issues such as crypto-agility, verifiable provenance, and

accountability in increasingly interconnected supply chains and digital ecosystems.

The dialogue explored these questions across three research-informed lenses. A session moderated by Ranjan Pal examined how AI-enabled systems, third-party model pipelines, and future quantum threats are introducing new forms of systemic risk in supply chains, including long-term cryptographic exposure and vendor accountability challenges.

Stuart Madnick and Angelica Marotta led a discussion on AI-driven cybercrime and the UN Cybercrime Treaty, probing where current global governance frameworks align with emerging threats—and where they fall short.

The series concluded with a session led by Sander Zeijlemaker and Matthew Gardiner, which examined how AI both enhances and destabilizes cyber risk management, prompting discussion on governance models, investment priorities, and institutional strategies for resilience in AI-enabled environments.

AI AND THE SYSTEMIC DYNAMICS OF CYBER RISK

In recent work led by Sander Zeijlemaker, published as the cover story in *MDPI Systems*, the research moves beyond traditional attacker–defender models to analyze how AI alters the systemic foundations of cyber risk. Drawing on executive insights, expert workshops, and existing literature, the study identifies three reinforcing feedback loops, deceptive defenses, cascading two-step attacks, and the proliferation of autonomous AI, that change how cyber risks emerge, interact, and spread across interconnected environments. The findings show that AI can introduce both stabilizing and destabilizing effects, underscoring the need for new governance approaches and more formalized use of deception in cyber risk management.

BOARDS, GOVERNANCE, AND AI RISK

CAMS research is also examining how boards are adapting governance practices in response to cyber and AI-related risk. Researcher Jeff Proudfoot is contributing to this work through an upcoming article in *Management Information Systems Quarterly Executive* on cybersecurity governance in the boardroom, as well as research presented at the International Conference on Information Systems that analyzes workplace surveillance in the age of generative AI platforms.

CAMS ENGAGEMENT AT THE UPCOMING 20TH CDOIQ SYMPOSIUM

CAMS will participate in the Chief Data Officer & Information Quality (CDOIQ) Symposium this July, as the symposium marks its twentieth year convening senior leaders and researchers focused on data, information quality, and governance. Stuart Madnick, who has been involved with CDOIQ since its early years, will deliver a keynote as part of the anniversary program.

CAMS members are eligible for a registration discount for the upcoming CDOIQ Symposium. Members seeking additional information and how to get the discount may contact Kelty Fitzgibbons at kcfitz@mit.edu.

STUART MADNICK — NPR INTERVIEW ON DATA BREACHES AND AI

On October 7, 2025, Professor Madnick was interviewed on National Public Radio (NPR) show: The Indicator from Planet Money. The subject of the session was "What's supercharging data breaches?"

His comment start at around 6 ½ minutes into the recording. He repeated his frequent concern that "although the goodguys are getting better, the bad guys are getting badder even faster." In particular, one way that the cyber criminals are staying ahead of the curve is AI.

As an example, they discussed spear phishing, a highly targeted form of phishing that relies on learning as much as possible about an individual and then impersonating a trusted colleague, supervisor, or partner to gain access or influence behavior. Then you ask for login info or to transfer some money. AI can generate such phishing emails much faster and higher quality than humans.

ABOUT CAMS

Cybersecurity at MIT Sloan (CAMS) advances research and convenes dialogue at the intersection of AI, cyber risk, governance, and resilience. The center brings together faculty, researchers, and senior leaders to examine emerging challenges and develop forward-looking frameworks for managing cyber risk in complex, interconnected systems.

TO LEARN MORE ABOUT MEMBERSHIP, REACH OUT TO THE CAMS TEAM:

Directors:

Stuart Madnick, smadnick@mit.edu

Michael Siegel, msiegel@mit.edu

Administration:

Dagmar Trantinova, dagmar@mit.edu

Communications:

Kelty Fitzgibbons, kcfitz@mit.edu

IN THE NEWS & RECENT PUBLICATIONS

December 12, 2025: Ranjan Pal was a Co-author in a Forbes India thought-leadership article, "Future-proofing your company from quantum cyber risks," discussing strategic guidance for CISOs on anticipating and mitigating quantum-related cybersecurity risks.

December 3, 2025: Stuart Madnick was quoted in a TCPalm contributor-content article, "Strengthen Your Cloud Defenses with Data Security Posture Management," emphasizing the need for organizations to look beyond basic cloud configurations and adopt a more comprehensive, proactive approach to protecting sensitive data in cloud environments.

November 12, 2025: Ranjan Pal was a Co-author in a Forbes India thought-leadership article, "Safeguarding against the new frontier of cyberattacks in AI," contributing to the discussion of strategic governance controls to mitigate systemic cyber risks in AI and software supply chains.

October 30, 2025: R. Pal, D. Yao, and B. Nag: How Can Companies Secure Their Future with Rise in Agentic AI Adoption. Forbes (I), Mentioned in MIT Sloan in the News.

October 30, 2025: Stuart Madnick was interviewed for an article published by the Miami Herald, "Coral Gables is investigating a commissioner accused of 'phishing.' What to know"

October 16, 2025: R. Pal, B. Nag, and S. Mukherjee: Cyber Risk on India's Electric Roads. Forbes (I), October 16, 2025. Mentioned in MIT Sloan in the News.

October 10, 2025: Stuart Madnick was quoted in a World of Software / HackerNoon article, "Why blockchain verification could eliminate Indonesia's $22 billion fake degree problem," offering cautionary perspective on blockchain adoption by referencing his research on blockchain security breaches to temper overly optimistic narratives about immutable systems.

October 7, 2025: Stuart Madnick was featured as an expert in an NPR article and audio interview, "What's Supercharging Data Breaches," discussing the factors accelerating the scale and frequency of data breaches, including supply-chain vulnerabilities, increasing system complexity, and the limits of purely technical security solutions.