Cybersecurity at MIT Sloan

WHEN SOFTWARE STARTS TO ACT: INSIDE THE 2026 CAMS ANNUAL CONFERENCE

This year's CAMS Annual Members-Only Conference — Cybersecurity and the Next Wave of AI Systems — was held June 3 and drew over 100 members in person and online. It focused on the premise that AI no longer just generates outputs. It acts. It decides, executes, and reaches into real systems with limited human oversight. When software can act on its own, three of cybersecurity's load-bearing assumptions start to give way. The takeaway for any CISO or board member: budget and governance conversations built for yesterday's software won't hold for systems that act on their own.

IT ACTS FASTER THAN WE CAN GOVERN. CAMS founder Stuart Madnick opened by framing agentic AI as an arms race defined by who can use the technology faster — the same capabilities that help defenders find vulnerabilities help attackers automate phishing, reconnaissance, and exploitation. Dr. Yisroel Mirsky of Ben-Gurion University's Offensive AI Lab made it concrete: offensive AI is here, and his lab fooled code-analysis models invisibly, with a success rate above 97 percent. The most counterintuitive warning came from CAMS affiliate Sander Zeijlemaker: because attackers aren't slowed by compliance or approval, they benefit from AI first — and cyber risk turns *non-linear*, where a small gain in attacker capability produces a disproportionate jump in organizational exposure.

IT ACTS THROUGH A SUPPLY CHAIN WE CAN'T SEE. A panel moderated by CAMS research scientist Ranjan Pal turned to a problem most organizations have barely begun to map. Unlike conventional software, an AI supply chain includes data, models, prompts, agents, and runtime behavior — where failures are silent, and behavior is hard to verify. Pal pressed the panel, drawn from KPMG, Mastercard, and Gallagher, on the accountability trap: an organization can bear responsibility for a third-party model it did not build and cannot inspect.

CAMS Research Scientist Dr. Ranjan Pal, leading his panel, ***Poisoned Intelligence: How LLMs Are Reshaping Software Supply Chain Cybersecurity****, with panelists from left to right, Arjun Ramakrishnan (Mastercard); Bridget Quinn Choi (Gallagher); Kristy Hornland (KPMG); Katrina Hill (Gallagher Re)*

SECURING SELF-ACTING SYSTEMS DEMANDS NEW CONTROLS AND HUMAN JUDGMENT.

Industry keynote Katie Moussouris, founder of Luta Security, warned that finding vulnerabilities was never the hard part — triaging what matters is, and that still takes people. A closing panel led by CAMS director Michael Siegel confronted unauthorized agents that, unlike passive tools, can access data, call APIs, and act on their own. The remedies were concrete — agent identity, least privilege, red-teaming before deployment.

Katie Moussouris, founder of Luta Security, giving her keynote; ***From Tools to Agents: Cybersecurity in an Era of AI-Driven Attacks***

Two CAMS student researchers, Cynthia Zhang & Lillian Bluestein, introduced by Pal, grounded the day in method — presenting original work on which security investments reduce attacker success, and how to prioritize risk across industrial control systems.

The directors closed by naming where CAMS goes next: AI's impact on resilience, insurance, and risk modeling. The harder truth underneath the optimism: these dynamics are already unfolding inside enterprise environments. The organizations that understand the shift first won't just manage the risk better — they'll set the terms everyone else inherits.

Prof. Stuart Madnick and Dr. Michael Siegel, CAMS Co-Directors giving closing remarks.

Want to be in the room next year? Visit cams.mit.edu or contact Kelty Fitzgibbons at kcfitz@mit.edu.

CAMS IS PROUD TO WELCOME IPA JAPAN AS ITS FIRST EXECUTIVE MEMBER

In their own words, the Innovation Platform Agency, Japan (IPA) "captures the ever-evolving IT society trends and technological trends from a broad perspective, provides guidelines that lead to the resolution of social issues and the development of industry, strengthens information security measures, and develops excellent IT human resources. We will contribute to the realization of a safe and highly convenient 'reliable IT society.'"

CAMS is proud to be working together with an organization whose mission aligns so closely with our own, and we look forward to a productive and lasting partnership.

As our first Executive Member, IPA Japan receives every benefit CAMS extends to its members, from workshop access to Executive Education discounts, along with three additions reserved for this top tier: a seat on the CAMS Executive Board, special recognition at CAMS events and on the CAMS website, and quarterly one-on-one faculty consultations.

CYGENT CONSORTIUM LAUNCHED AT CYBER SECURITY MANAGEMENT SYMPOSIUM

Sander Zeijlemaker and Michael Siegel were pleased to participate in the 2nd Cyber Security Management Symposium at the University of Twente, joining experts from academia, industry, and government to discuss the strategic impact of cybersecurity and AI. A key highlight was the launch of CYGENT (Cyber Governance & AI-Driven Threat Management), a newly funded research consortium bringing together MIT CAMS, the University of Twente, the Disem Institute, and Modat. CYGENT will develop AI-augmented threat modelling, systemic cyber risk insights, and next-generation governance frameworks to help executives better understand, manage, and strengthen cyber resilience in an increasingly AI-driven digital landscape.

Watch a 60-second video about CYGENT: https://www.youtube.com/watch?v=EyzKdUEnjto

CAMS RESEARCH HEADS TO IACIS 2026

Two CAMS researchers will present new work at the 66th IACIS Annual Conference, October 7–10 in Pensacola Beach, Florida

CAMS Postdoctoral Fellow Dr. May Almousa had her paper, co-authored with Prof. Stuart Madnick, *"Intelligence, Information Operations, and Cyber-Physical Security in the Middle East, with a Focus on Saudi Arabia"* accepted for presentation. The work examines how intelligence operations, information warfare, and cyber-physical threats intersect in one of the world's most strategically contested regions — extending the geopolitical line of CAMS research into a region undergoing rapid digital transformation.

CAMS Research Affiliate Dr. Angelica Marotta will present *"An AI–Cybersecurity Taxonomy for Regulating Hybrid Risks,"* offering a framework for classifying and governing the blended technical-and-regulatory risks that AI introduces — work that speaks directly to the

governance questions organizations are now confronting as AI moves deeper into enterprise systems.

CAMS WELCOMES A NEW RESEARCH AFFILIATE: PROFESSOR DIONYSIOS DEMETIS

CAMS welcomes Professor Dionysios Demetis as a new Research Affiliate. A Professor at Hull University Business School in the UK, Dionysios brings a research record that spans the technical and institutional dimensions of cybersecurity, exactly the bridge CAMS is built to make.

Professor Dionysios Demetis

He holds an MSc and PhD in Information Systems from the London School of Economics and an undergraduate degree in Physics from the University of Crete. At LSE's Computer Security Research Centre, his work on EU-funded projects covered biometrics, digital identity, cyber-enabled fraud, and money laundering — research that earned him the Best Paper Award from the *Journal of the Association for Information Systems* and the Senior Scholars Best Publication Award from the Association for Information Systems.

The author of three books and numerous journal articles, Dionysios also serves as Co-Chair of the Annual Security Conference in Las Vegas, now in its 26th year, and as Academic Lead for NSEC, the UK's national network of multidisciplinary academics addressing security and resilience. His connection to cultural-heritage cyber risk through the UNESCO Chair on Threats to Cultural Heritage adds a distinctive dimension to CAMS' research community.

STUART MADNICK TO KEYNOTE AT THE 20TH ANNUAL CDOIQ SYMPOSIUM AND OPPORTUNITY FOR CAMS MEMBERS TO ATTEND

We're proud to share that our center's founder, Stuart Madnick, will deliver a keynote at this year's International Chief Data Officer and Information Quality (CDOIQ) Symposium.

Now in its 20th year, CDOIQ brings together CDOs and data leaders from across industries to explore data management, governance, and leadership — with case studies spanning industry, academia, finance, government, and healthcare. Topics range from data analytics and machine learning to data quality, all centered on turning mature data capabilities into real ROI.

We're excited to see Stuart take the stage, and hope to see many of you there too. There is an important connection between the CDOIQ goals and CAMS goals. CDOIQ goal is to increase the value of an organization's data, CAMS goal is to protect this valuable data - being more valuable, it is more likely to be a target for data breach.

CDOIQ will be at the Hyatt Regency Cambridge, Cambridge, MA July 21–23, 2026 - for more info see https://www.2026cdoiq.org

The conference will be hybrid, allowing both in-person and remote attendance. By special arrangement, a limited number of CAMS members can get FREE registration. Contact Kelty Fitzgibbons, CAMS Director of Communications, for details.

RECOGNITION: RANJAN PAL INDUCTED INTO SIGMA XI

CAMS research scientist Dr. Ranjan Pal has been inducted as a Full Member into Sigma Xi, the international scientific research honor society founded in 1886, for his contributions to cybersecurity. Membership is by nomination from existing members and recognizes a demonstrated record of original, high-impact research

— a peer-endorsed mark of scientific achievement. Sigma Xi counts more than 200 Nobel laureates and numerous National Academy of Science and National Academy of Engineering Fellows among its historical membership, and an induction places Dr. Pal within an elite community spanning every field of science and engineering. The honor reflects the depth and influence of his work on cyber risk quantification and cyber insurance aspects of cybersecurity that CAMS members have seen advance across recent quarters.

SANDER ZEIJLEMAKER: INFORMING GLOBAL AI GOVERNANCE

CAMS Research Affiliate Dr. Sander Zeijlemaker brought CAMS research into the international policy conversation this quarter. On April 23, he contributed to the second stakeholder consultation of the Global Dialogue on AI Governance, arguing that AI governance cannot be treated as a narrow technical problem — it must be approached as an interconnected system linking economic, social, and security dimensions. His call to pair scientific insight with real-world policy, through shared frameworks, harmonized regulation, and joint capacity-building, points to exactly the kind of evidence-based, cross-border governance CAMS research is positioned to inform.

His research also continues to reach new venues: Zeijlemaker's work *"Cultivating Collective Intelligence in Cyber Risk Governance: An Enterprise Architectural Approach"* has been accepted for an interactive lightning talk at the 2026 International System Dynamics Conference (ISDC) in Delft this July.

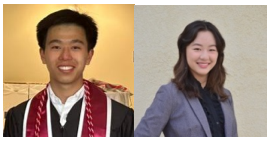
Join us for a Friday Research Discussion

Fridays 11:30am – 12:30pm EST
Each week, we bring together researchers, practitioners, and policymakers for candid, wide-ranging conversations spanning cybersecurity, AI, agentic AI, cyber risk, and policy

FIVE CAMS STUDENT PAPERS ACCEPTED TO THE WINTER SIMULATION CONFERENCE

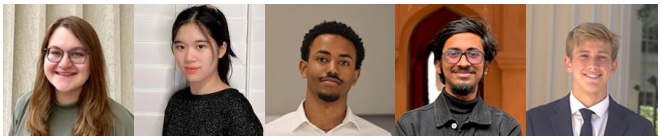
Graduate Students

1. *Luisa Pan (not pictured)*
2. *Darren Yao*
3. *Cynthia Zhang*



Undergraduate Students

1. *Lillian Bluestein*
2. *Konnie Duan*
3. *Yaphet Lemiesa*
4. *S M A Nahian*
5. *Canon Robins*



CAMS Student research had a standout quarter, with five co-authored papers accepted to the 2026 Winter Simulation Conference — an INFORMS event, published by IEEE Press — to be held in Glasgow, Scotland. Mentored by CAMS researchers Dr. Ranjan Pal and Dr. Michael Siegel, the papers span the center's core themes, from critical-infrastructure resilience to cyber insurance and software supply-chain risk:

L. Pan, R. Pal, and M. Siegel — *Optimal Cyber Resilience of Network Flows in Critical Infrastructure*

C. Zhang, R. Pal, G. Bassett, and M. Siegel — *Risk-Driven Strategic Resilience in Digital Infrastructure Networks*

R. Pal, Y. Lemiesa, and M. Siegel — *An AI Simulation Theory for Scaling Cyber Insurance with CAT Bonds*

C. Robins, Y. Lemiesa, D. Yao, S M A Nahian, R. Pal, and M. Siegel — *A Network Theory for Optimal Software Supply Chain Risk Management*

L. Bluestein, R. Pal, S M A Nahian, and M. Siegel — *An Automated Critical Risk Assessment Theory for ICS Security*

On most of these papers a student appears as lead author, ahead of their CAMS faculty mentors — a reflection of how research training works at our center, with students driving original work that reaches peer-reviewed, international venues.

CYBERSECURITY IN THE BOARDROOM

Stuart Madnick, Michael Coden, and Jeffrey Proudfoot published a paper in the June issue of MIS Quarterly Executive titled "Recommendations for Advancing Cybersecurity Governance in the Boardroom to Address Persistent and Emerging Challenges," which examines how corporate boards can better oversee cyber risk amid escalating threats and growing regulatory scrutiny. Drawing on 27 hours of interviews with 42 board directors, advisors, and board-facing executives, the study identifies two major categories of governance challenges: internal structural barriers that limit effective oversight, and external cyber threats that continue to evolve in scale and complexity. The research team translates these expert insights into practical recommendations for boards to anticipate, prepare for, and respond to cyber risk more effectively. The study also highlights unresolved challenges that will require continued attention as cyber risk becomes an increasingly central issue for corporate governance.

Jeffrey Proudfoot also co-authored research presented in June at the European Conference of Information Systems titled "IT Governance in the Boardroom: The Emergence of Boards as Digital Fiduciaries in the Information Age." This research examines how boards of directors are becoming "digital fiduciaries" as organizations face mounting opportunities and risks from rapidly advancing technologies. Drawing on interviews with 27 board members and technology leaders across 22 companies, the study shows that effective IT governance is no longer limited to oversight of isolated technologies but now requires boards to take a holistic role in shaping digital strategy and protecting organizational resilience. The findings identify two core responsibilities: stewarding digital innovation for value creation and safeguarding the organization against digital threats. To fulfill these duties, boards are developing new capabilities, investing in education and renewal, and strengthening governance mechanisms that help directors better understand, oversee, and guide technology-related decisions in the information age.

WHAT DIRECTORS NEED TO HEAR

Michael Coden, CAMS Associate Director, was invited by HMG Strategy to present the paper *Advancing Cyber Governance in the Boardroom* to a group of CIOs and CISOs on Zoom on June 11. The paper makes the case that cybersecurity is a governance problem that lands on the board, not an IT problem.

He started with the structure: boards face six pressing concerns, split into three internal structural issues (establishing an effective board hierarchy, balancing cyber operations with governance, and building cyber knowledge on the board) and three external threats (incident preparedness and response, AI as a mounting threat, and boards' own emergence as a target).

Coden spent the most time on how boards should evaluate the CIO and CISO—framing it directly as a career issue for his audience. Boards should treat cyber crises as opportunities to assess executive composure and competence, retaining leaders who perform under pressure. The lesson for executives: presenting clear strategic insight rather than technical minutiae is how you make yourself valuable to your board.

The point that drew the most attention was that board members are now prime targets themselves—something most of the room hadn't considered. Directors increasingly access sensitive operations while having less training and weaker protections, making them the soft, high-value entry point an attacker would seek. Boards should monitor for leaked director information, mandate secure communication tools, and enforce strict password policies at the board level.

He closed on resilience, using the diagram from the earlier cyber resilience work. It contrasts a resilient company with a nonresilient one through a shock: both take the hit, but the resilient one absorbs it more

shallowly and recovers faster. Coden focused on diversity and redundancy of systems, and why they matter even more in an AI world—as organizations converge on similar AI models and tools, they risk a brittle monoculture where one failure cascades across everything. Redundancy and genuine diversity are the antidote.

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

Directors:

Stuart Madnick, smadnick@mit.edu

Michael Siegel, msiegel@mit.edu

Administration & Finance:

Dagmar Trantinova, dagmar@mit.edu

Communications & Member Engagements:

Kelty Fitzgibbons, kcfitz@mit.edu

CAMS IN THE NEWS & PUBLICATIONS

Congratulations to Michael Siegel, Ranjan Pal, and Sander Zeijlemaker, whose paper has been accepted at AMCIS 2026.
Title: A Systems Dynamics Approach to Understanding Threat Intelligence Sharing
https://amcis2026.aisconferences.org/

April 2, 2026: Stuart Madnick and Jeffrey Proudfoot (Research Affiliate Cybersecurity, MIT Sloan; Professor, Bentley University) were Co-authors in a Harvard Business Review article, "Boards Are Falling Short on Cybersecurity," examining why corporate boards are failing to govern cybersecurity effectively despite growing awareness, and offering guidance on improving board-level oversight amid rising cybercrime losses.

Proudfoot, J., Cram, W. A., Madnick, S., Coden, M. (2026). Cybersecurity Governance in the Boardroom: Persistent and Emergent Challenges with Recommendations for Action. Management Information Systems Quarterly Executive (MISQE), (25) 2 117-132.

Bui, Q., Proudfoot, J. G., Adelakun, O. (2026). "IT Governance in the Boardroom: The Emergence of Boards as Digital Fiduciaries in the Information Age" 34th European Conference on Information Systems (ECIS), June 13-17. Milan, Italy