CYBERSECURITY AT MIT SLOAN (CAMS)

THEMES SHAPING Q3 AT CAMS

AI & Governance: Michael Siegel and Nelson Novaes Neto at MIT EmTech Brasil explore how to govern innovation responsibly. "Gen AI has changed the game, but it's a perpetual cat-and-mouse game."'

Systemic Risk: Ranjan Pal's framework offers new ways to manage cascading cyber threats.

Research Recognition: CAMS research on emerging cybersecurity regulations were honored at AMCIS and IACIS, plus a comprehensive ACM publication on emerging regulations.

People & Partnerships: Welcoming Dr. May Almousa and deepening collaboration with Japan's IPA.

TRUSTWORTHY AI: LESSONS FROM MIT EMTECH BRASIL 2025

CAMS Director ***Michael Siegel*** *and Research Affiliate* ***Nelson Novaes Neto*** *at C6 Bank, strengthening global collaboration between academia and industry on cybersecurity challenges*

At MIT EmTech Brasil 2025, organized by MIT Technology Review Brasil, CAMS Director Michael Siegel joined Nelson Novaes Neto, CTO of C6 Bank, for a dynamic session on AI governance and cybersecurity. Nelson summed it up clearly: "Gen AI has changed the game, but it's a perpetual cat-and-mouse game." He pointed to deepfakes as a vivid reminder of AI's risks, while also highlighting how embedded AI solutions are creating powerful defenses, such as built-in fraud prevention. Siegel built on this message; security cannot be treated as an afterthought; it is a matter of survival. He also reminded the audience that with technology evolving so quickly, the challenge is not just to adopt AI, but to govern it responsibly and ethically. Together, their insights drove home a crucial point for CAMS and beyond: AI and cybersecurity are inseparable, and true digital resilience comes from balancing innovation with accountability.

BREAKING NEW GROUND IN CYBERSECURITY: A FRAMEWORK FOR MANAGING SYSTEMIC RISK

At the Association *for Computing Machinery SIGSIM Conference on Principles of Advanced Discrete Simulation (*ACM SIGSIM PADS Conference 2025) in Santa Fe, Dr. Ranjan Pal presented groundbreaking research on one of cybersecurity's toughest challenges: managing systemic cyber-risk. His paper, *A Theory to Estimate, Bound, and Manage Systemic Cyber-Risk* co-authored with CAMS student Konnie Duan, introduces both a theoretical and practical framework for understanding how cyber threats cascade across interconnected systems such as supply chain networks and how they can be contained. By linking theory with actionable insights, his work lays a foundation for building more resilient digital infrastructures worldwide. This contribution provides researchers and practitioners with tools to better estimate and manage cascading risks. This marks a significant advance in shaping global cybersecurity strategies. An earlier introductory version of this research was a best paper award finalist at the Winter Simulation Conference 2025. Dr. Pal is also serving as a technical program committee member for ACM SIGSIM PADS 2026 and

co-organizing chair for the cybersecurity and cyber-risk management track.

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.

WELCOMING DR. MAY ALMOUSA: NEW CAMS POSTDOCTORAL FELLOW

This September, CAMS proudly welcomed **Dr. May Almousa** as our newest postdoctoral fellow. A distinguished researcher, Dr. Almousa works at the intersection of **cybersecurity, AI, and data science**, focusing on intelligent systems that strengthen resilience against emerging threats. Alongside her CAMS role, she is an Assistant Professor at Princess Nourah Bint Abdulrahman University (PNU), where she leads the Information Security track at the PNU AI Center. Her academic leadership and innovative research bring fresh perspectives and global expertise to our community. We are excited to collaborate with Dr. Almousa as she helps drive CAMS' mission forward.

CAMS RESEARCH INSIGHTS FROM AMCIS 2025

At the *Americas Conference on Information Systems (AMCIS 2025)*, CAMS Researchers, Dr. Angelica Marotta and CAMS Founding Director, Stuart Madnick presented their paper, *A Comparative Analysis of the UN Cybercrime Treaty and GDPR: Balancing Global Security and Data Sovereignty*, which explores how international cybersecurity frameworks intersect with data-protection legislation. Their work, available through the *Association for Information Systems Electronic Library*, underscores the tension between global security imperatives and national sovereignty in data governance. *(Video available to view here.)*

Adding to CAMS's strong presence at AMCIS, Dr. Sander Zeijlemaker, CAMS Research Affiliate, who presented, *Advancing Cyber Risk Management by Reducing Strategic Control Gaps*, co-authored with Dr. Ranjan Pal, Dr. Michael Siegel, and Jeffrey Proudfoot

*CAMS Founder **Stuart Madnick** and Research Affiliate **Sander Zeijlemaker** at AMCIS 2025, where CAMS research on decision-making under cyber pressure gained international recognition.*

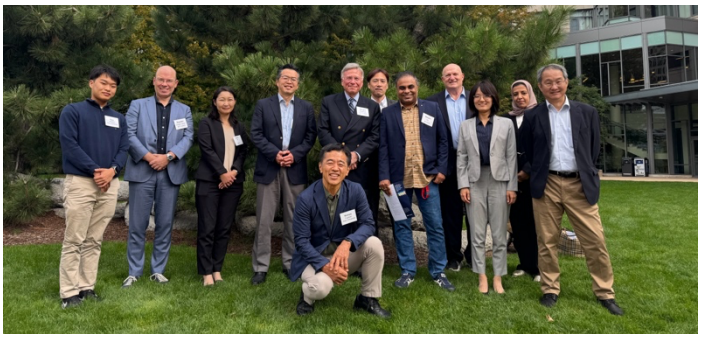
CAMS RESEARCHERS WIN IACIS 2025 BEST PAPER AWARD

Congratulations to Dr. Angelica Marotta and Dr. Stuart Madnick, recipients of the International Association for Computer Information Systems (IACIS) 2025 Best Research Paper Award for their paper, *The UN Cybercrime Treaty and AI: Navigating the Intersection of Technology and Global Policy.*

The research, presented on October 2 at the 65th Annual IACIS Conference, provides a critical analysis of the interrelationship between artificial intelligence technologies and international cybercrime regulatory frameworks, offering recommendations for the development and implementation of effective policies.

Their work highlights both the strengths and gaps in the treaty's ability to regulate fast-evolving AI-driven cybercrime. This award-winning research advances the global conversation on policy, governance, and cybersecurity at a time when AI is rapidly reshaping the threat landscape. Takeaway: Executives should review how AI-driven threats are handled in current policy frameworks and prepare for gaps in global treaties.

CAMS AND IPA JAPAN JOIN FORCES TO STRENGTHEN GLOBAL CYBER RESILIENCE



Pictured outside the Sloan School of Management. From left to right: ***Mr. Ray Hirano*** *(Keio University),* ***Dr. Sander Zeijlemaker*** *(MIT CAMS),* ***Ms. Kaori Ito*** *(Ministry of Economy, Trade, and Industry, METI),* ***Dr. Daisuke Takayanagi*** *(IPA – Information-Technology Promotion Agency, Japan),* ***Dr. Kenzo Fujisue*** *(Keio University),* ***Professor Stuart Madnick*** *(MIT CAMS),* ***Mr. Yutaka Takami*** *(IPA),* ***Dr. Ranjan Pal*** *(MIT CAMS),* ***Dr. Michael Siegel*** *(MIT CAMS),* ***Ms. Minami Koga*** *(IPA),* ***Dr. May Almousa*** *(MIT CAMS), and* ***Mr. Uchida Tsutomu*** *(IPA).*

The Information-Technology Promotion Agency (IPA) Japan (**独立行政法人情報処理推進機構**) is a government-affiliated agency responsible for promoting IT security, developing IT human resources, and supporting digital transformation in Japan. Its activities include cybersecurity measures like threat analysis and awareness campaigns, IT professional training through programs like the Information Technology Engineers Examination, and initiatives to build common digital platforms for Japanese society. The IPA is a new CAMS Member. IPA, along with representatives from MITI and Keio University, came to MIT Sloan for a three-day (September 22–24, 2025), in-depth collaborative workshop. There was a great exchange of ideas, and innovative approaches to cybersecurity including technical sessions, research exchanges, and strategic discussions focused on risk management and AI applications. The workshop brought together senior leaders to explore the intersections between AI, regulation, and cyber risk management. Dr. Ranjan Pal proposed his Critical Asset Management, (CAM) framework for cyber risk assessment, designed to identify and govern critical assets in infrastructure networks in a cost and time-efficient manner. He proposes to develop the CAM framework with MIT students and postdoctoral fellow Dr. May Almousa over the next year. The outcome of this research will help automate currently manual cyber risk management processes in Japan's critical infrastructures, contributing to faster and more resilient cybersecurity. By advancing both practical solutions and academic insights, this work also sets the stage for strengthening digital resilience in critical systems worldwide.

CAMS MEMBERS-ONLY: INSIGHTS FROM "MEET THE RESEARCHER" WITH DR. RANJAN PAL

Last month's Meet the Researcher event gave CAMS members an exclusive look into one of today's biggest business cybersecurity challenges: securing the AI and software supply chain.

Dr. Ranjan Pal presented new research showing that with more than 70% of business applications built on third-party or open-source code, hidden vulnerabilities can ripple across industries. His network-science framework helps identify the most critical "weak links" in AI and software ecosystems, the few modules whose failure could cause widespread disruption. A striking finding: in an AI supply chain network of 1,000 models, securing on the order of 10 key nodes can significantly strengthen overall resilience - whereas in a software supply network with a similar number of nodes, securing on the order of 100 key nodes results in a similar degree of resilience. The research also found that the reason for this trend is that software supply chains are denser and more vulnerable than AI-specific ones, meaning small flaws can have systemic consequences. Pal's practical framework, designed to be automated, scalable, and cost-effective, offers us a way to target their cybersecurity efforts where

they matter most. Events like these are a hallmark of a CAMS membership, providing members direct access to research and the experts shaping the future of cybersecurity.

JILLIAN KWONG PRESENTS ON SUPPLY CHAIN RESILIENCE AT PACIS 2025

At the Pacific Asia Conference on Information Systems (PACIS 2025) in Kuala Lumpur, Malaysia, CAMS Research Scientist, Dr. Jillian Kwong, presented her paper, *Building a Resilient Supply Chain: Collaborative Approaches to Small and Medium-Sized Enterprises Cybersecurity*. The paper highlights how companies can help their small and medium-size enterprises (SME) suppliers, often the most vulnerable points in supply chains, strengthen their cyber resilience through collaboration. Drawing on case studies and empirical research, Dr. Kwong highlights mechanisms and programs used by companies to go above and beyond required standards to help suppliers with cybersecurity. This included sharing resources, exchanging threat intelligence, and adopting collective defense strategies. Rather than tackling cybersecurity in isolation, the paper argues, networked resilience is the key to managing today's complex risks. Her work underscores the importance of cross-organizational collaboration not just for SMEs, but for the stability of global supply chains, an increasingly urgent issue in our interconnected digital economy.

At PACIS 2025 in Kuala Lumpur, **Dr. Jillian Kwong** *(pictured with a colleague) presented her research on building resilient supply chains through SME cybersecurity collaboration.*

CAMS RESEARCH SHOWCASED AT UNIVERSITY OF PISA: GLOBAL PERSPECTIVES ON AI AND CYBERSECURITY

About four years ago, the University of Pisa started offering the first interdisciplinary master's program in Cybersecurity in Italy. It is a two-year Master of Science degree and the first of its kind, with contributions from multiple departments. Dr. Angelica Marotta and Dr. Stuart Madnick had the opportunity to meet many of the faculty and understand the various perspectives in the U of Pisa program and explore opportunities for collaboration. In turn, they described the research and directions of MIT CAMS. Their presentation encompassed the following components: an introduction to the Cybersecurity at MIT Sloan (CAMS) research program; an analysis of organizational vulnerabilities that facilitate security compromises; an examination of regulatory frameworks, incident analysis methodologies, and international treaty implications; and an investigation into the bidirectional relationship between artificial intelligence advancements and evolving cybersecurity paradigms.

(Right to left): Prof. Stefano Chessa, Chair of the M.Sc. in Cybersecurity at U of Pisa; Prof, Stuart Madnick; Dr. Angelica Marotta, CAMS Research Affiliate.

NEW ACM PUBLICATION: EMERGING CYBERSECURITY REGULATIONS

Stuart Madnick and Angelica Marotta have had their paper, *Analyzing and Categorizing Emerging Cybersecurity Regulations*, recently published in ACM

Computing Surveys. The paper is the result of analyzing about 170 recent cybersecurity regulations by countries around the world, which were found to be made up of 17 distinct features or components, such as Required Incident Reporting, Required Software Bill of Materials, and Required Security by Design. The publication presents a methodical classification system for contemporary cybersecurity regulatory structures, providing a comprehensive resource for organizations navigating multijurisdictional compliance requirements. This work gives academics and practitioners a valuable roadmap to navigate today's complex regulatory environment. A database of the 170 regulations is provided in the Appendix.

AI'S IMPACT ON CYBERSECURITY … AND VICE VERSA

At the Chief Data Officer / Information Quality (CDOIQ) Symposium, Dr. Madnick presented "AI's Impact on Cybersecurity and Vice Versa: The AI Arms Race," exploring how artificial intelligence is reshaping both attack and defense in today's digital landscape. His talk built on ideas first introduced in his Chief Information Officer (CIO) Symposium keynote this past May, expanding them into a deeper discussion for an academic and practitioner audience.
Watch the presentation here.

CAMS Founder ***Prof. Stuart Madnick*** *with conference organizer,* ***Dr. Richard Wang*** *at the CDOIQ Symposium, advancing the conversation on AI's role in shaping both cyber threats and defenses.*

CAMS STUDENT FEATURED IN BUSINESS INSIDER

Photo by Melia Russel / Business Insider. CAMS student ***Cynthia Zhang*** *(front row, right) featured in Business Insider for her role in Figma's IPO, showcasing how CAMS students bridge research with real-world cybersecurity practice.*

CAMS student **Cynthia Zhang was recently featured in *Business Insider*** for her work during an internship on the security team at Figma in New York City. This summer, Cynthia had the opportunity to contribute to Figma's landmark IPO on Wall Street, applying her academic research to real-world cybersecurity challenges. At Figma, she worked on preventing account takeovers, securing developer tools, and tackling industry-wide problems such as zero-trust overhead, privilege creep, and log fatigue. Her experience highlights how students are bridging research with practice in some of the world's most cutting-edge industry environments.

PROUDFOOT HIGHLIGHTS RISK AND REGULATION AT THE 42ND INTERNATIONAL SYMPOSIUM ON ECONOMIC CRIME, CAMBRIDGE, U.K

At the **42nd International Symposium on Economic Crime** in Cambridge, U.K., CAMS research affiliate Jeff Proudfoot presented research examining the gaps between rules and real-world outcomes in cybersecurity and data governance. His first presentation, delivered as a workshop, *The Persisting Paradox of Regulatory Compliance and Cybersecurity Outcomes*, explored how organizations can meet compliance standards yet still fall short of true cyber resilience. The study emphasized the role of boards in moving beyond formal compliance to

more effective risk management. In his second presentation, which he presented during the main session, *Checking on Checkpoints,* Proudfoot analyzed U.S. Customs and Border Protection practices, showing how unclear federal guidance led to inconsistent data collection at checkpoints. Together, these works reveal the challenges of regulation and data governance across both corporate and public-sector domains, offering lessons for strengthening accountability and resilience.

JOIN CAMS TODAY — LEAD THE FUTURE OF CYBERSECURITY

Membership at CAMS gives you exclusive access to cutting-edge research, members-only webinars, and executive education programs designed for leaders on the front lines of cyber risk. Stay ahead of emerging threats, shape the global cybersecurity conversation, and connect directly with top researchers and industry peers.

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

September 30, 2025: Michael Siegel had an article published by MIT Technology Review, Published and available in Portuguese: *"Cultura da ciberseguranca é um problema vital" English Translation "Cybersecurity culture is a vital issue"*

September 9, 2025: Angelica Marotta and Stuart Madnick published their research article "Analyzing and Categorizing Emerging Cybersecurity Regulations" in ACM Computing Surveys, vol. 58, no. 2, Article 51 (September 2025), 36 pages. https://doi.org/10.1145/3757318

August 28, 2025: Ranjan Pal had an article published by Forbes India: "How AI hallucinations endanger software supply chain" The article outlines the risks of AI-generated code hallucinations, false APIs, insecure configurations and highlights mitigation strategies such as SBOM practices, dependency management controls, and stronger AI governance to secure digital supply chains

August 12, 2025: Stuart Madnick authored an article for the MIT Technology Review. *"The Hidden Cyber Risks of Well-Intentioned Regulations"*. Published and available in Portuguese: *"Os riscos cibernéticos ocultos de regulamentações bem-intencionadas"*

August 11, 2025: Ranjan Pal had an article published by Forbes India, "Operational economics insights to boost cyber resilience" The article maps key cyber resilience measures to the operational realities of digitally transformed businesses, emphasizing how enterprises can align anticipation, absorption, responsiveness, and recovery strategies with their operational economics.

July 9, 2025: Stuart Madnick was featured in a Bloomberg article titled "US Pushes Software Developers to Embrace Memory Safe Languages. "Professor Madnick emphasized that while performance remains critical in domains like defense and AI, concerns about switching languages have waned as computing power grows more affordable.

July 2, 2025: Ranjan Pal had an article published by Forbes India. "Why does cybersecurity management in enterprises fail?" The article discusses governance gaps, misaligned incentives, and profit-first mindsets leave even well-funded organizations vulnerable in the age of AI and digital supply chains