MIT CAMS AI & Cybersecurity Conference
Meeting Summary

Hosted by Stuart Madnick & Michael Siegel
May 20th & 21st, 2025

Attendees at the MIT CAMS AI and Cybersecurity Conference listen to a keynote, while overlooking the Cambridge skyline from the Samberg Conference Center.

AI AND CYBERSECURITY: NAVIGATING A DOUBLE-EDGED FUTURE

Advancements in artificial intelligence are happening at such a rapid pace that it is nearly impossible for organizations or individuals to keep up. That certainly includes cybersecurity professionals, who on the one hand benefit from more robust security defensive tools, but who also face better-armed cyber threat actors. Quite simply, AI is enabling more frequent and more intense cyber attacks, and greatly improved fraud measures that threaten corporate systems and data. While this game of one-upmanship has gone on for many years, the threat/counter measure pace is at an all-time high thanks to AI advancements. In response, Cybersecurity at MIT Sloan devoted its May 20-21 members-only conference to the topic of AI & Cybersecurity. This conference explored how AI is shaping both sides of the cybersecurity equation and what organizations can do to better defend themselves in the future.

SIMULATING THE CYBER ARMS RACE: HOW AI SHAPES ATTACK AND DEFENSE

Una-May O’Reilly from MIT CSAIL, opened the conference on May 20th at the Welcome Reception and VIP Dinner. She started with a timely and thought-provoking keynote on the accelerating arms race between cyber attackers and defenders, fueled by advances in AI. She introduced the concept of “cyber adversarial intelligence,” exploring how both offense and defense evolve through a competitive, coevolutionary process. Drawing from her team’s research, she illustrated how AI can be used to simulate these rivalries and help security professionals better anticipate and counter threats.
O’Reilly also examined how large language models are now being trained and deployed as autonomous agents capable of performing reconnaissance, launching exploits, and even exfiltrating data. While these tools can help bolster defenses, through log analysis, deception tactics, and reasoning over threat data.

They also lower the barrier for launching sophisticated attacks. Her message was clear: to stay ahead, defenders must pool knowledge, leverage simulation, and invest in systems that are secure by design. Learn more about Una-May and her work here.

GROWING RISK IN A RAPIDLY EVOLVING LANDSCAPE

Kicking off the day's activities on May 21st were CAMS co-directors Michael Siegel and Stuart Madnick, who set the tone for the conference and reviewed its goals. Tackling first things first, Siegel offered a brief history lesson on MIT's beginnings; when the terms 'digital security' or ''computer security' were first coined (1955); when the first computer password was introduced at MIT (1961); and when the term 'cybersecurity' emerged (1989). But turning the clock way back, Siegel said what is the first actual cyber-attack occurred in 1834, though obviously not involving actual computer systems. Madnick then spoke about the vulnerabilities of modern-day systems and data, the reasons for those vulnerabilities, and how AI is rapidly changing the security game. He presented a chart that outlined a dozen areas where AI is helping both attackers and defenders. He explained how AI can use publicly available resources to look for vulnerabilities at individual organizations, and it can be trained to write code to target specific companies. Not surprisingly, he said that 80% of ransomware attacks are now AI-driven. Madnick also shared polling results from CAMS members revealed their top concerns: trust, AI-enhanced threats, slow defensive adaptation, data privacy, and the challenge of effective governance. Stuart emphasized that AI is already transforming how threats emerge and evolve, and how cybersecurity must evolve with it.

KEYNOTES AND EXPERT PERSPECTIVES

The first keynote address was by John Williams, Professor of Information Engineering and Civil and Environmental Engineering at MIT. Williams spoke on the topic "Generative AI and Security: DeepFakes and Super- Human Performance." Interest in Generative AI has sky rocked over the past couple of years, and that includes the use of GenAI to create fraud tools to fool individuals and employees into security blunders that lead to cyber incidents. Williams reviewed how such tools and techniques have been evolving, and how DeepFakes created today are almost undistinguishable from the real thing. He played a conversation with a digital friend in which they discussed the top issues today with cybersecurity, and then a video of himself created as a seemingly real DeepFake. Speaking about such examples, Williams noted that one of the biggest challenges going forward will be verifying identities for sources and resources to maintain trust in digital information.

John Williams, professor of information engineering and civil and environmental engineering, giving his keynote.

PANEL: AI FOR CYBERSECURITY

Michael Siegel served as moderator for the day's first panel discussion, on "AI for Cybersecurity." Joining him were panelists from C-6 Bank, MasterCard, and Safe Security. One of most important messages from this panel was that AI advancements are being made so fast that it Is nearly impossible to predict what the state of AI and Cybersecurity will be only a couple of years from now. They called today's environment "AI on steroids." Another panelist said the hope is that defenders will be able to train GenAI to improve cyber risk management, by evaluating an organization's overall systems and communication to find the week points and close defensive gaps. On the attackers' side, another panelist noted that AI is increasingly being used to locate vulnerabilities in systems, and to provide validation of fake individuals, accounts and capabilities used in attacks. Threat actors now have access to technology that enables them to move so fast it is unlikely defenders will keep pace. An important role for AI in cyber defense will be helping organizations identify gaps in their defenses, a panelist said. Within the vendor space, some large companies are acquiring smaller start-ups that have developed security tools that serve niche security needs. Those products are then being rolled into the offerings of larger companies to expand their defensive capabilities.

Panelists discuss the evolving role of AI in cybersecurity at the MIT CAMS conference. Pictured from left: Michael Siegel (MIT CAMS), Vidit Baxi (Safe Security), Arjun Ramakrishnan (MasterCard, speaking), and Nelson Novaes Neto (C6 Bank).

INDUSTRY PERSPECTIVE ON DEFENSIVE READINESS

Providing the industry keynote address on "Harnessing Generative AI for Cybersecurity" was Peter Bailey, newly appointed Senior Vice President and General Manager, Security, at Cisco Systems. The discussion noted that understanding the key threats targeting your industry and prioritizing the right defensive measures across people, processes, and technologies has always been critical to a successful cyber defense program. It continued with the analysis of the AI arms race is very much a real thing, with few being able to predict even six months out when it comes to what AI development in store. After all, only six months ago we weren't using the term "agentic" in relation to AI. Noted was the that wide-scale interest in GenAI will lead to better products soon. Instead of organizations needing to manage a group of detection analysts, there might be someone managing a bunch of AI detection agents. On the flip side, regarding cyber-attacks,it was noted that what comes next will seem like science fiction. The average company today will be completely unprepared to prevent or prepare for cyber-attacks. We can expect there will be new attack vectors that we haven't seen before.

PANEL: CYBERSECURITY FOR AI

The second panel of the day examined how to secure the AI systems themselves. “Cybersecurity for AI” Moderated by CAM’s Stuart Madnick, included panelists from BCG, KPMG, Microsoft, MongoDB, and Schneider Electric. This panel emphasized that AI introduces new data risks and that defenders cannot protect everything. Instead, the focus should be on identifying and securing the most critical systems and data. Most attendees agreed that cybersecurity may be in a worse state ten years from now unless defenders adapt quickly. Madnick began this session with a quick poll of conference attendees, which revealed that 80%-plus expect the cybersecurity situation to be worse a decade from now, meaning that cyber threat actors will get much better at what they do, while cyber defenders won’t. Defenders simply won’t be able to protect everything in the organization, so they should concentrate of first making sure the ‘crown jewels’ are safe, Madnick said. That was in reference to the critical systems and data. Because of the extreme volatility in the cybersecurity space, a major responsibility of cybersecurity defenders going forward will be to instill trust in data among workers. A panelist noted that one trust is lost, it is difficult for security experts to set up systems to defend against incidents. Another emphasized that the growing interest and use of AI only increases vulnerabilities, since AI demands so much data to be effective. The more data provided, the greater the potential risks. With no signs of AI interest slowing down, Madnick suggested that while the focus of cyber security used to be protection, it has changed to include more focus on resilience.

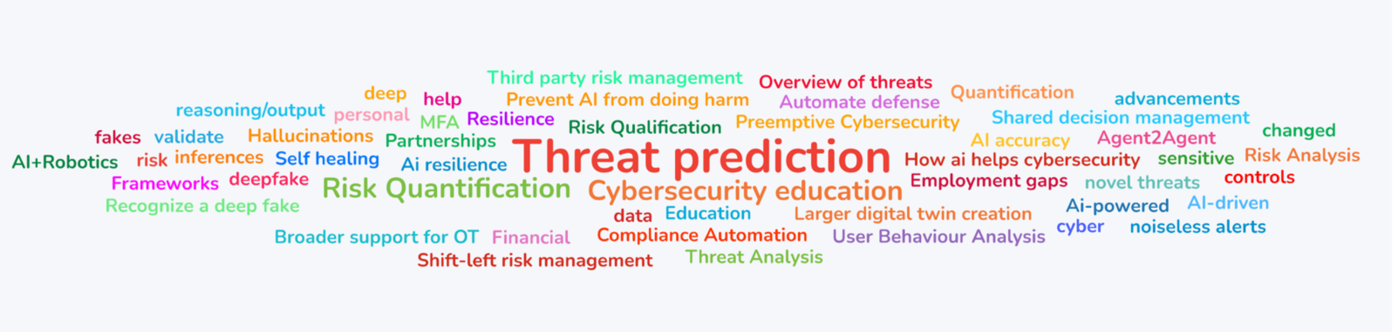
Panelists and attendees listen to insights from Robert Lembree, Schneider Electric.

REFLECTIONS ON TECHNOLOGY AND INEQUALITY

One of the highlights of the afternoon lineup was the Nobel Laureate keynote delivered by Simon Johnson, professor of entrepreneurship at the MIT Sloan School of Management, and Head of the Global Economics and Management Group. He provided a broader lens on AI’s social impact. He urged technologists to focus on ways AI can create new, accessible job roles, particularly for less educated workers. Without this shift, AI may continue to widen economic divides. He continued to speak on the topic “Technology and Inequality in the Age of AI.” In 2024, Johnson received the Nobel Prize “for studies of how institutions are formed and affect prosperity.” He is also the co-author of the 2023 book “Power and Progress: Out 1,000-Year Struggle over Technology and Prosperity.” Johnson noted that his Nobel Prize was awarded for work that he did more than two decades ago. “It can take years for everyone to agree that you have made a big impact,” he joked. He hopes we can find a way for AI to create new task-oriented job roles to help lift up populations that would otherwise be left behind. Working with AI requires workers that have advanced skills and education. That helps a minority of our workforce. Johnson said the United States hasn’t really created new-task oriented types of jobs since the 1980s. The result is an expanding wage gap between educated and non-educated workers. He posed the question of whether tech firms can develop a “pro worker” version of AI – one that would boost the jobs and opportunities for less- educated workers by giving them new types of tasks to master.

INTRODUCTION TO POSTER SESSION, LIGHTENING TALKS, AND WORD CLOUD

Following Simon Johnson's keynote, the remainder of the afternoon was devoted to a series of short segments and hot topic discussions. These three brief sessions were moderated by Sander Zeijlemaker of MIT CAMS, and included Nelson Novaes Neto of C-6 Bank, and Cynthia Zhang of MIT CAMS. Discussion focused on vulnerabilities in industrial control systems, and a dozen key areas where AI can bolster cyber defenses and cyber-attack tools. Other topics covered included agentic AI and agent functions; automated security hygiene; autonomous and deceptive defense systems; and augmented oversight and reporting.



The final Word Cloud made by participants who were asked, "What future research in AI and Cybersecurity do you suggest?"

HOT TOPICS DISCUSSIONS

This section on AI & Cybersecurity for Regulations and Compliance included moderator Joram Borenstein, General Manager at Microsoft, and Jeffery Proudfoot of Bentley University and a CAMS research affiliate. Much of the discussion centered on the pressure that organizations place on themselves to adopt AI platforms, and if this puts them under increased vulnerability. A key factor is how well the organization handles data management.

Jeff Proudfoot of MIT CAMS leads a discussion on regulation and compliance. He also discussed challenges faced, during the afternoon Hot Topics session.

In the meantime, there was discussion with the audience on whether the increased use of AI-based products or decisions increases an organization's liabilities, and if so, what that might do to insurance coverage and rates. That discussion was the perfect segue into the second Hot Topics discussion on Cyber Insurance, with moderator Katrina Hill, cyber security consultant with Gallagher Re, and Ranjan Pal, research scientist with CAMS. Themes discussed in this segment included what new security threats are being introduced into the organizations of attendees through AI adoption. Attendees were asked how their employers managed these risks, and how they can successfully measure how much of their risk level is truly due to AI. Finally, discussion turned to the topic of insurance, and whether AI impacts should remain part of traditional cyber insurance, or if it needs its own new category for coverage. It was agreed by attendees that organizations need to pool their views and experiences on the topic for industry to come up with uniform policies, rather than the current piecemeal policies in effect now.

CAMS co-directors Michael Siegel and Stuart Madnick share closing reflections at the end of the AI and Cybersecurity Conference.

Co-Directors Michael Siegel and Stuart Madnick concluded the event by outlining three key areas that CAMS will continue to develop in the months ahead. They are AI's impact on resilience practices; insurance practices; and risk modeling.

This conference reinforced that while AI brings complexity, it also offers opportunities. The real challenge is staying informed, staying curious, and working together to build systems that can withstand whatever comes next

Interested in Learning More?
If you'd like to learn more about the work of Cybersecurity at MIT Sloan (CAMS), explore membership opportunities, or get involved in future events, we'd love to hear from you. Visit cams.mit.edu or reach out to our Senior Director of Communications, Kelty Fitzgibbons directly at **kcfitz@mit.edu**.