CYBERSECURITY AT MIT SLOAN (CAMS)

Q1 2026 MARKS ONE OF CAMS' MOST CONSEQUENTIAL QUARTERS TO DATE.

A €700,000 international research grant for CyGENT, two new members, Cisco and Asteria, a keynote at the Annual Security Conference in Las Vegas, a paper with Gallagher Re and Testudo. All against a backdrop of escalating AI-driven threats and growing geopolitical cyber risk from the Middle East to critical infrastructure worldwide. The throughline across all of it: AI is no longer just reshaping the threat landscape, it is reshaping how organizations govern, insure, and respond to cyber risk.

THEMES SHAPING Q1 AT CAMS

AI and Software Supply Chains As AI becomes embedded in enterprise infrastructure, securing the supply chain, from LLMs to data pipelines, emerges as a critical governance frontier.

The AI Arms Race AI now powers both sides of the cyber battlefield. CAMS research explores who is winning — and what it means for defenders, policymakers, and boards.

Governing AI Risk From electricity infrastructure to the Middle East, new research examines how sociotechnical and geopolitical forces are reshaping cyber governance.

Insuring the Unknown Ranjan Pal and Gallagher Re probe the blind spots of AI-era cyber insurance — and what smarter frameworks could look like.

New Members & Milestones Cisco and Asteria Corporation, bring CAMS' membership to a new level of industry depth — from enterprise data infrastructure to global-scale cybersecurity.

ANNUAL CONFERENCE: CYBERSECURITY AND THE NEXT WAVE OF AI SYSTEMS — JUNE 3, 2026

CAMS is pleased to announce its Annual Conference, "Cybersecurity and the Next Wave of AI Systems," taking place on Wednesday, June 3, 2026 at the Samberg Conference Center at MIT in Cambridge. The conference will bring together CAMS researchers, industry members, and practitioners for a full day of exploration into the cybersecurity challenges posed by the next generation of AI, from autonomous systems and agentic AI to emerging attack surfaces and digital risk governance.

The conference will feature two panels at the center of its program. The first, Poisoned Intelligence: How LLMs Are Reshaping Software Supply Chain Cybersecurity, moderated by CAMS Research Scientist Dr. Ranjan Pal, will examine how large language models are introducing new and poorly understood vulnerabilities into enterprise software pipelines, and what defenders, developers, and governance teams need to do about it. The second, Securing the Next Generation of Self-Acting Enterprise AI Systems, moderated by CAMS Director Michael Siegel, will tackle one of the most urgent emerging challenges in the field: how organizations can build security frameworks for AI agents that operate with increasing autonomy, making decisions and taking actions with limited human oversight.

This is a unique opportunity to engage directly with the researchers and practitioners shaping how organizations understand, govern, and defend against the threats that AI is creating and enabling. CAMS members are encouraged to register early. Registration is now open for CAMS members. Please contact Kelty Fitzgibbons at kcfitz@mit.edu for questions or assistance registering.

WHAT 42 BOARD MEMBERS TAUGHT US ABOUT GOVERNING CYBER RISK

On April 16th CAMS will present another forward-looking Meet the Researcher session, featuring a presentation by CAMS Research Affiliate Jeff Proudfoot, *"What 42 Board Members Taught Us About Governing Cyber Risk."* Corporate boards are increasingly being asked to oversee cyber risk portfolios that are more complex and volatile than ever — yet critical governance challenges remain unresolved even as boardroom attention to the issue grows. Drawing on 27 hours of interviews with 42 board directors, advisors, and board-facing executives, Jeff will surface two central obstacles boards face: internal governance gaps within the boardroom itself, and the rapidly evolving external threat landscape. Attendees can expect expert-backed insights and practical guidance on how boards can better anticipate cyber risks, strengthen their governance structures, and respond effectively when incidents occur.

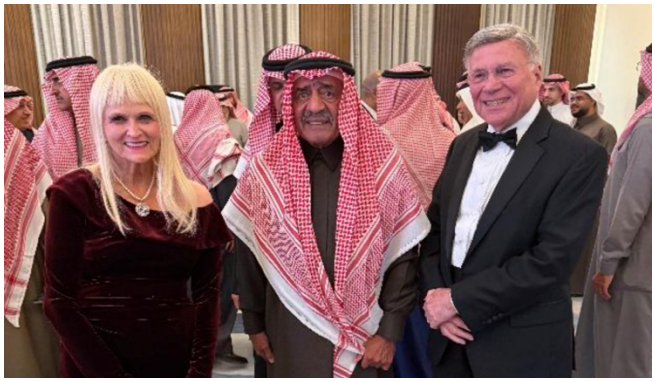
FROM THE UAE TO SAUDI ARABIA: CAMS DEEPENS MIDDLE EAST ENGAGEMENT

CAMS' engagement with the Middle East deepened significantly this quarter, spanning two country visits, a new working paper, and growing collaborative ties with regional academic institutions.

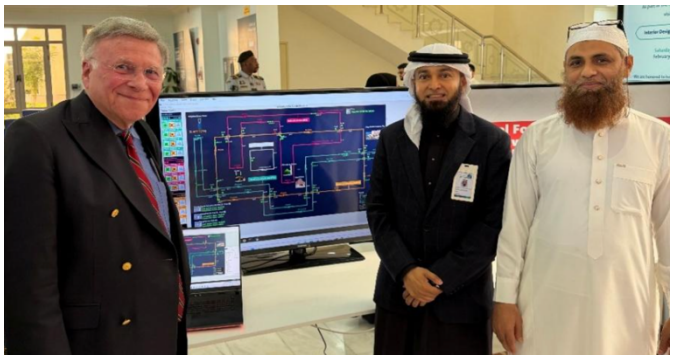
Professor Madnick traveled to the United Arab Emirates at the invitation of Dr. Saed Alrabaee, Associate Professor in the Department of Information Systems and Security and Director of the Center for Excellence in Teaching and Learning at UAE University (UAEU) — the oldest university in the UAE, founded by the nation's founding father Sheikh Zayed bin Sultan Al Nahyan in 1976, and located in Al Ain, Abu Dhabi. As part of UAEU's 50th anniversary celebrations, the university is planning an international Cybersecurity Conference bringing together professionals, researchers, and government organizations from across the region. Dr. Alrabaee — who also organizes the UAE Cybersecurity Conference — invited Professor Madnick to discuss the conference plans and the cybersecurity challenges facing the region.

Photo with Dr. Saed Alrabaee (Left) and Stuart Madnick (Right).

Professor Madnick also traveled to Saudi Arabia at the invitation of the University of Prince Mugrin (UPM), a non-profit private university in Madinah established in 2013 that offers the first degree program in Cybersecurity and AI in Saudi Arabia. The visit comes at a critical moment: escalating geopolitical tensions in the Middle East have significantly increased the volume of state-sponsored cyberattacks, phishing, and malware targeting critical infrastructure, financial institutions, and government entities, with some reports indicating attacks in the region have increased by up to 245%. Prof. Madnick participated in a Strategic Academic Forum and the UPM Executive Board Meeting in Riyadh (February 8–9, 2026), joining leading international scholars from MIT, Stanford, and Berkeley to discuss emerging trends in AI, cybersecurity, and data analytics, and to explore how UPM's programs can align with Saudi Vision 2030.



(From left to right): Dr. Mariann Drago Madnick, Prince Muqrin bin Abdulaziz Al Saud, Prof. Madnick.



Prof. Madnick reviews UPM's cybersecurity projects

These visits complement a new working paper by Professor Madnick and CAMS Postdoctoral Fellow Dr. May Almousa, "*Intelligence, Information Operations, and Cyber-Physical Security in the Middle East, with a Focus on Saudi Arabia*", which examines the intersection of intelligence operations, information warfare, and cyber-physical threats in one of the world's most strategically contested regions. Saudi Arabia's accelerating digital transformation, including smart city infrastructure and national AI initiatives, creates a rich and urgent context for this analysis. The paper reflects CAMS' expanding geographic scope and its commitment to research that bridges technical risk with geopolitical reality.

RANJAN PAL, MIT, GALLAGHER RE, AND TESTUDO: RETHINKING INSURANCE FOR THE AI ERA

CAMS researcher Dr. Ranjan Pal joined forces with Gallagher Re, CAMS Member, one of the world's leading reinsurance brokers, and Testudo Global Inc., a pioneering AI liability insurer, to produce a landmark industry white paper examining a structural challenge at the heart of the global insurance market: how do you price and underwrite risk when the systems causing harm are governed by AI?

The paper, *"Smart Systems, Blind Spots: Rethinking Insurance for the AI Era,"* makes the case that traditional actuarial models — built on historical loss data and human-driven incident patterns — are increasingly unfit for purpose. As AI agents operate with greater autonomy, they introduce failure modes that are novel, difficult to attribute, and largely uninsured under existing policy structures.

The paper identifies where conventional coverage frameworks break down: in scenarios involving algorithmic discrimination, AI hallucinations, model drift, and supply chain compromises where the originating failure is an algorithm rather than a human actor. It documents a 978% surge in GenAI-related litigation in the United States between 2021 and 2025, underscoring the urgency of the problem, and maps a path toward more adaptive, purpose-built underwriting approaches for the AI era.

This collaboration extends CAMS' research directly into the frameworks used by global capital markets to price and transfer cyber risk — a meaningful expansion of the center's real-world influence.

CAMS AT THE ANNUAL SECURITY CONFERENCE, LAS VEGAS

CAMS made a strong showing at the Annual Security Conference in Las Vegas (March 25–26, 2026), with both a keynote address and a research paper presentation.

Professor Madnick delivered the keynote, "The Cybersecurity AI Arms Race… and the Winner Is?" — his signature examination of how AI is simultaneously transforming cyber defense and arming adversaries with unprecedented capabilities. The talk challenged attendees to confront a central question: both sides are getting better, but who is getting better faster? Drawing on years of CAMS research, Madnick laid out the evolving interplay between AI-powered threat detection and AI-enabled attacks, and what it means for every organization operating in an AI-powered threat environment.

CAMS Research Affiliate Jeff Proudfoot also presented at the conference, extending CAMS' research into one of the most consequential domains of critical infrastructure: the electricity sector. His paper, *"Cybersecurity Challenges in Electricity Infrastructure: A Socio-Technical Perspective,"* draws on 20 in-depth interviews with specialists across diverse organizational roles. Applying a sociotechnical systems (STS) framework, the study reveals that cybersecurity challenges in electricity infrastructure are not purely technical — they span people, processes, and institutional structures. The findings underscore why integrated approaches are essential to strengthening a system that underpins every other form of critical infrastructure in modern society.

Stuart Madnick (Left) and Jeff Proudfoot (Right) Pictured together at the Annual Security Conference, Las Vegas.

WELCOMING NEW CAMS MEMBERS: ASTERIA & CISCO

CAMS is proud to welcome two distinguished organizations to its membership community.

Asteria is a Tokyo Stock Exchange-listed Japanese technology company founded in 1998, specializing in enterprise data integration and IoT edge computing. Known for its ASTERIA Warp integration platform — Japan's most widely used in its category — Asteria brings deep expertise in connecting systems across complex digital environments. As cyber risk increasingly flows through interconnected data infrastructure, Asteria's perspective bridges the technology and governance dimensions central to CAMS' research mission.

Cisco is the world's leading networking and cybersecurity technology company, securing the digital infrastructure of enterprises, governments, and critical systems globally. CAMS' engagement is led by Peter Bailey, SVP and General Manager of Cisco Security, who brings extensive experience from Mandiant and Google Cloud Security. Cisco's membership connects CAMS' research with one of the most influential security organizations operating at global scale.

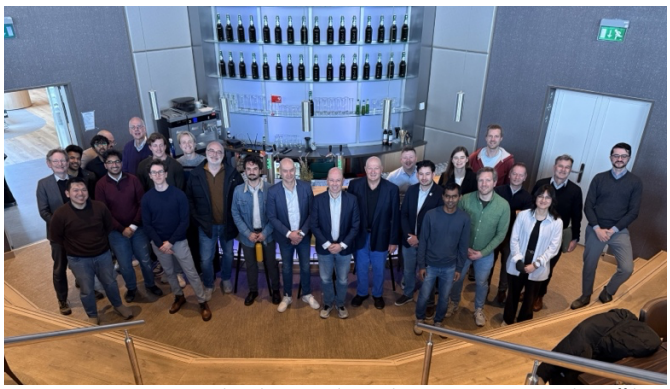
CYGENT: A MAJOR GRANT FOR AI-DRIVEN CYBER THREAT MANAGEMENT

CAMS, the University of Twente, and the Disem Institute have been awarded a €700,000 (approximately $850,000 USD) research grant for the CyGENT project, Cyber Governance and AI-Driven Threat Management. The award reflects growing institutional recognition of the urgency of AI's role in the evolving malware ecosystem.

CyGENT will leverage large-scale threat data platforms — including VirusTotal and Malware Bazaar — to improve malware classification and distinguish AI-driven threats from conventional ones. The research aims to bring data-driven cyber governance frameworks directly into boardroom decision-making.

The project's launch was marked at the 2nd Cybersecurity Management Symposium at the University of Twente, where CAMS researcher Sander Zeijlemaker and CAMS Director Michael Siegel, joined a distinguished panel exploring the strategic and technical dimensions of cybersecurity and AI. Discussions spanned governance, innovation, and real-world cyber challenges — underscoring the interdisciplinary collaboration across academia, industry, and policy that CyGENT is built to advance.

This grant, awarded in January 2026, represents a significant milestone for CAMS' European research partnerships and advances the center's work at the intersection of AI, threat intelligence, and institutional governance. Watch the 60-second CyGENT overview.



CAMS Director Michael Siegel and CAMS Research Affiliate Sander Zeijlemaker in a group photo from the University of Twente.

UPCOMING EVENTS

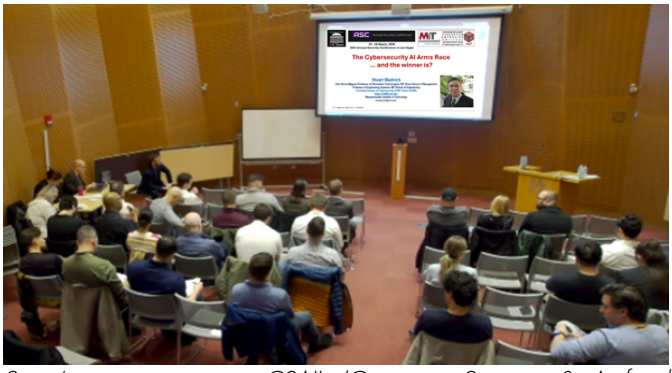
Meet the Researcher | Thursday, April 16th, 11:00am – 12:30pm ET | Members Only Join CAMS Research Affiliate Jeff Proudfoot for a members-only session, "What 42 Board Members Taught Us About Governing Cyber Risk," exploring the governance gaps and external threats boards face in managing cyber risk today.

CAMS Annual Conference | June 3rd | Members Only Our flagship annual event returns on June 3rd, bringing together CAMS members, researchers, and industry leaders for a full day of research presentations, insights, and networking.

Friday Research Discussions | Weekly, Fridays 11:30am – 12:30pm ET | Open to the Public Each week, CAMS hosts a public Zoom discussion exploring the latest and most pressing topics at the intersection of cybersecurity and AI. All are welcome to join. Contact Kelty Fitzgibbons for more information.

MIT US GOVERNMENT AI DAY

Professor Madnick delivered a presentation, *"AI Threats and Vulnerabilities: The AI Arms Race — Who Will Be The Winner? The Cyber Defenders or Attackers,"* for USGA Cyber AI Day, a US government agency event. The talk reinforced Madnick's consistent message that while defenders are growing more capable, adversaries are leveraging AI even faster — a dynamic with direct implications for national security and public-sector cyber resilience.



Stuart's presentation at CSAIL (Computer Science & Artificial Intelligence Laboratory)

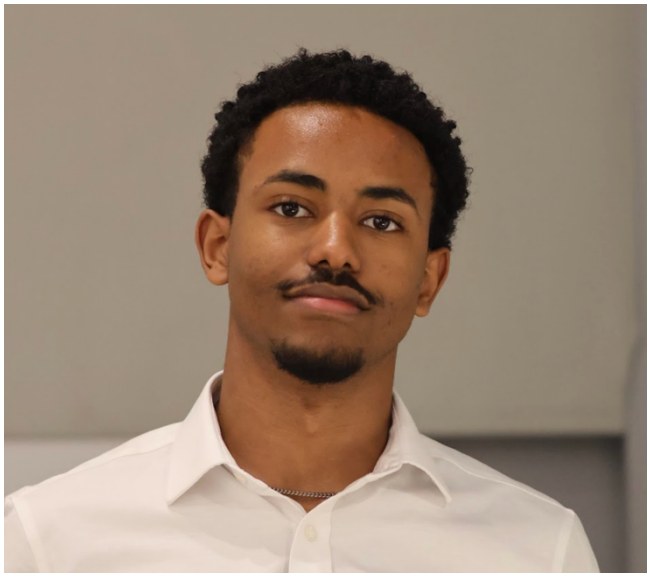
NEW RESEARCH & PUBLICATIONS

Professor Madnick and CAMS Research Affiliate Dr. Angelica Marotta have had their paper "A Feature-Driven Analysis of Global Cybersecurity Regulations and their Impact on Safeguarding Data Value" accepted for publication in the Journal on Data and Information Quality (JDIQ). This work builds on the duo's landmark ACM Computing Surveys publication from Q3 2025, deepening the analytical lens on how regulatory frameworks affect the real-world protection of data assets across jurisdictions.

This quarter also saw the release of a new working paper by Professor Madnick and CAMS Postdoctoral Fellow Dr. May Almousa: "Intelligence, Information Operations, and Cyber-Physical Security in the Middle East, with a Focus on Saudi Arabia." (See From the UAE to Saudi Arabia above.)

For a full list of Q1 publications, media appearances, and conference presentations, see the In the News & Recent Publications section.

AND THE OUTSTANDING UROP AWARD FOR 2026 GOES TO... We are proud to announce that CAMS UROP student Yaphet Kumsa Lemiesa has been named the recipient of the 2026 Outstanding UROP Student Award for the Sloan School of Management — one of MIT's most prestigious recognitions for undergraduate research. Selected by a dedicated awards committee from nominations submitted by UROP mentors across the Institute, the award honors students who have made exceptional contributions within their field. This recognition reflects the outstanding AI for small data research Yaphet under the mentorship of CAMS researcher Dr. Ranjan Pal over the past year. Yaphet will be celebrated alongside nine other recipients from across MIT at the Student Awards Convocation on May 8th, a well-deserved honor and a testament to the caliber of research happening at CAMS.



CAMS UROP student Yaphet Kumsa Lemiesa, recipient of the 2026 Outstanding UROP Student Award for the MIT Sloan School of Management

SANDER ZEIJLEMAKER: Q1 RESEARCH & ENGAGEMENTS

CAMS Research Affiliate Dr. Sander Zeijlemaker had an active quarter across research, publication, and practitioner engagement.

At the System Dynamics Benelux Chapter Symposium (February 27), Zeijlemaker presented work on collective intelligence systems that enable executives to collaborate with AI in simulating cyber-risk scenarios — improving decision speed and accuracy through a secure-by-design enterprise architecture. He also participated in a panel on AI and digital twin technologies for strategic decision-making in complex environments.

Sander also led a *Meet the Researcher* session for CAMS members, focusing on Rethinking Cyber Risk Governance Resourcing in the AI Era, offering senior practitioners three concrete examples of how AI can inform board-level cyber risk reporting and decision-making.

At Forum in Cyber Lille (March 31–April 2) Europe's most prestigious cybersecurity conference, drawing 20,000 visitors from 103 countries, Sander contributed to the Secure AI stream with a panel on the AI Act model passport, sharing insights on governance, digital trust, and how documentation standards can support transparency, drive innovation, and create strategic advantage. He also presented CyGENT to the international audience, reinforcing the project's cross-sector vision for AI-driven cyber governance. Learn more about Forum in Cyber →

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

IN THE NEWS & RECENT PUBLICATIONS

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.

April 2, 2026: CAMS UROP Student ***Yaphet Kumsa Lemiesa*** wins the *2026 Outstanding UROP Student Award for the MIT Sloan School of Management* for his research on AI and small data, mentored by Research Scientist Dr. Ranjan Pal

March 31–April 2, 2026: Sander Zeijlemaker presented at In Cyber Forum in Lille, France. Europe's most prestigious cybersecurity conference, drawing 20,000 visitors from 103 countries — contributing to the Secure AI stream with a panel on the AI Act model passport and presenting CyGENT to an international audience. Learn more →

March 25–26, 2026: Stuart Madnick (keynote) and Jeff Proudfoot (paper presentation) at the Annual Security Conference, Las Vegas.

March 25, 2026: Ranjan Pal was a co-author in a Gallagher Re report, *"Smart Systems, Blind Spots: Rethinking Insurance for the AI Era,"* examining the growing gap between AI-related exposures and existing insurance coverage, and offering a framework for insurers, reinsurers, and enterprises to address liabilities arising from AI system failures.

March 17, 2026: Ranjan Pal's research was featured in a Forbes India article published by IIM Calcutta, *"The Rising APT Risk: Reshaping Cyber Insurance for Critical Infrastructure,"* in which the authors cited Pal et al.'s work on quantifying and bounding cyber risk in IT/OT systems as foundational to understanding the growing APT threat landscape and its implications for cyber insurance and enterprise risk management.

February 27, 2026: Sander Zeijlemaker and Michael Siegel participated in the 2nd Cybersecurity Management Symposium at the University of Twente, presenting at the official launch of CyGENT and joining a panel on AI-driven cyber governance. Watch the 60-second overview →

February 24, 2026: Stuart Madnick delivered "The AI Arms Race: Who Will Be The Winner?" at Schneider Electric's Engineers Week, attended by over 100 engineers.

February 9, 2026: Stuart Madnick and Angelica Marotta were co-authors in an MIT Sloan Management Review article, *"What the UN Treaty on Cybercrime May Mean for You,"* discussing the treaty's intended global framework for cross-border cybercrime investigations, its implications for organizations, and associated concerns regarding privacy and enforcement.

February 5, 2026: Ranjan Pal, Sander Zeijlemaker, and Bodhibrata Nag were co-authors in a Forbes India article published by IIM Calcutta, *"Synthetic Data: The New Backbone of Next-Gen Cybersecurity,"* examining how generative AI-driven synthetic data is transforming cybersecurity model development, the associated policy risks around privacy, bias, and weaponization, and emerging directions for national data sovereignty in cyber defense.

February 4, 2026: Sander Zeijlemaker and Michael Siegel were co-authors in a World Economic Forum article, *"How to prioritize cyber resilience in the healthcare sector,"* discussing strategic priorities, investment challenges, and governance approaches to strengthen cyber resilience in healthcare organizations.

January 19, 2026: Ranjan Pal was a co-author in a Forbes India article, *"Cyber risk in the boardroom: Why judgment matters more than numbers,"* examining the limits of quantitative cyber-risk models and the importance of strategic judgment and governance in managing systemic cyber risk.

January 2026: Delvecchio, Zeijlemaker, De Bernardis & Siegel published *"Human-Centered Interface Design for a Dynamic Cyber-Risk Group-Based Training Game"* in Computer Standards & Interfaces, Vol. 95.

January 2026: Delvecchio, Zeijlemaker et al. published "Employing Board Cyber-Risk Management Collaborative Game Under Condition of Uncertainty" in Springer Communications in Computer and Information Science, Vol. 2459.

January 7, 2026: Digital Holland covered the CyGENT grant award to CAMS, University of Twente, and Disem Institute: *"CyGENT: Hoe krijgen we data gedreven cybersecurity samen de bestuurskamer in?"*

December 30, 2025: Ranjan Pal, Akhilesh Tuteja (KPMG), and Bodhibrata Nag were co-authors in a Forbes India article, *"Businesses need future-ready LLM supply chains,"* discussing governance, resilience, and security risks in large language model supply chains.

Accepted for publication: Madnick & Marotta, *"A Feature-Driven Analysis of Global Cybersecurity Regulations and their Impact on Safeguarding Data Value,"* forthcoming in the Journal on Data and Information Quality (JDIQ).

New working paper: Madnick & Almousa, *"Intelligence, Information Operations, and Cyber-Physical Security in the Middle East, with a Focus on Saudi Arabia."*