THE INSTITUTE FOR SECURITY AND TECHNOLOGY

2025 ANNUAL REPORT

LETTER FROM THE CEO

AMID TEC[H]TONIC SHIFTS IN THE LANDSCAPE, IST IS MEETING THE MOMENT.

Dear IST Supporters,

The juxtaposition was jarring. Outside, July in the Rockies was as beautiful as ever. Birds sang, we breathed the rarefied mountain air, and sunlight dappled the aspens. Inside, we were discussing the unraveling of the world as we know it.

Leaders from AI labs sat across conference tables from former senior government officials, with senior civil society leaders beside each. We were conducting an exercise, and it was not going well. As the IST team layered on new complications and pushed AI tools deeper into the decision making, the confusion intensified—but not in the intended ways. Industry participants kept looking to the government folks to understand and use powerful AI tools to move decisively. Government participants shot back that it was industry who were the experts, and that the tools were out of sync, untrustworthy… unfamiliar. We knew the truth. As one senior participant said afterwards: "we can't plan iteratively while technology moves asymptotically; [our national security leaders] need to see the full scope of preparation and strategic thinking required to meet the moment ahead."

In our after-action analysis, we wondered: had we blown our chance? Our mission at IST is to build bridges between technologists and policymakers, but now those bridges seemed to be crumbling. But then the feedback started rolling in. A long-time leader from a frontier AI lab told me the convening "had a profound influence on the direction of our research." A former Defense official highlighted that these kinds of insights were impossible to find in typical military wargames, precisely because private sector participants aren't routinely at the table. For me, the exercise solidified my conviction that technology's pace of change has outrun the playbooks we've long relied on, and that IST can and should play a role in rewriting new ones.

I think about that day in July a lot. It crystallized for me the monumental year that was 2025. In Silicon Valley and other tech centers around the world, 2025 was the year when questions surrounding AI flipped from "will it work?" to "how far will it go?" We saw decades of promise in machine learning realized in an exponential explosion of capability. If 2022 was the year AI entered the public consciousness, 2025 was the year it arrived.

At the same time, in Washington DC and other global capitals, 2025 marked the end of the post-war consensus. The rules-based international order, its decline heralded by Russia's invasion of Ukraine, collapsed. We don't yet know what will replace it—or if it will be replaced at all—but there's no going back.

At a time when tec[h]tonic shifts in the global order are an everyday occurrence, despite massive changes in the defense tech space and innovation ecosystem, the gap between California and Washington seems starker than ever. But we are policy engineers at IST who approach the increasingly complex national security challenges facing our world with concrete tools and actionable solutions to span that chasm.

The urgency of our mission was exemplified in 2025 by the SL5 Task Force. We incubated this initiative to develop immediate solutions to an existential problem: how to secure model weights, cutting edge algorithms, and treasured architectures against manipulation or seizure by the most capable nation-state

actors while preventing loss of control. With participation from major AI lab decision-makers, national security leaders, data center operators, and chip providers, we are building the roadmap that makes Security Level 5 achievable. When an AI lab CISO encourages us to keep pushing back on the status quo to raise the bar for security, you know what you're doing must be helping.

Perhaps no domain better illustrates the divide between technology and policy than nuclear. Visiting the UN last April was surreal — I arrived just weeks after the international trade landscape was permanently upended by new tariffs. Yet sitting in IST's roundtable on crisis communications, I was struck by how much civil society still matters to global stability. Whether in bilateral meetings or at the dinner we hosted with UN Under-Secretary-General Izumi Nakamitsu and heads of delegation from nuclear and non-nuclear states, our voice carried weight. As Ambassador Thomas Pickering and I agreed: at a time when empathy is scarce, dialogue is simultaneously at its hardest and its most important.

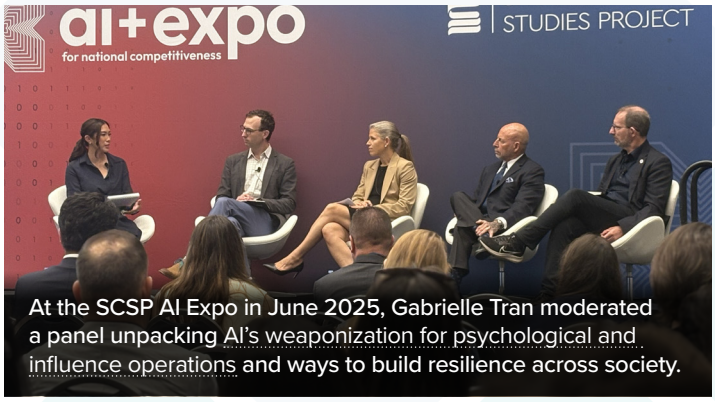
Thank you, as always, to the IST team who execute on our mission day in and out; the adjuncts, working group members, and participants who contribute their time and expertise to the tackling the national security, strategic stability, and human life-threatening challenges we take on; and the donors and supporters who supercharge our work's reach and impact. This 2025 Annual Report features a small selection of the many projects and initiatives we led–it was hard to choose just a few!

2025 saw tec[h]tonic shifts in the landscape. We are making a meaningful impact as we engineer solutions that expand opportunity and mitigate risk. As a team, we always come back to the same thesis: technology is now our entire environment, with world-changing implications, but what good does it do if the technologies that underpin our daily lives and permeate the systems we live in are not safe and secure?

What gives me hope is that the challenges we're working on, the convenings we're organizing, and the concrete, actionable solutions we're developing are not just of the moment. Together with you, they meet the moment.

Sincerely,
Philip Reiner

Chief Executive Officer
Institute for Security and Technology



At the SCSP AI Expo in June 2025, Gabrielle Tran moderated a panel unpacking AI's weaponization for psychological and influence operations and ways to build resilience across society.

The second annual Cyber Policy Awards™ in February 2025 hosted by IST in partnership with the Chamber of Commerce and presented by Microsoft, celebrated progress in cyber policy.


In May 2025 at the United Nations headquarters in New York, IST co-hosted a dialogue on preventing and managing nuclear crises at the third session of the Treaty on the Non-Proliferation of Nuclear Weapons Preparatory Committee.

IST Institute for SECURITY + TECHNOLOGY

The Institute for Security and Technology (IST) is the 501(c)(3) critical action think tank, uniting policymakers, technology experts, and industry leaders to identify and translate discourse into impact. We take collaborative action to advance national security and global stability through technology built on trust, guiding businesses and governments with hands-on expertise, in-depth analysis, and a global network.

OUR MISSION

IST unites technology and policy leaders to create actionable solutions to emerging security challenges.

OUR VISION

A democratic world secured and empowered by technology built on trust.

FOLLOW US ON OUR SOCIALS

OUR VALUES

BUILD TRUST: We foster trust between government, technology, and civil society by prioritizing open communication, transparency, and collaboration.

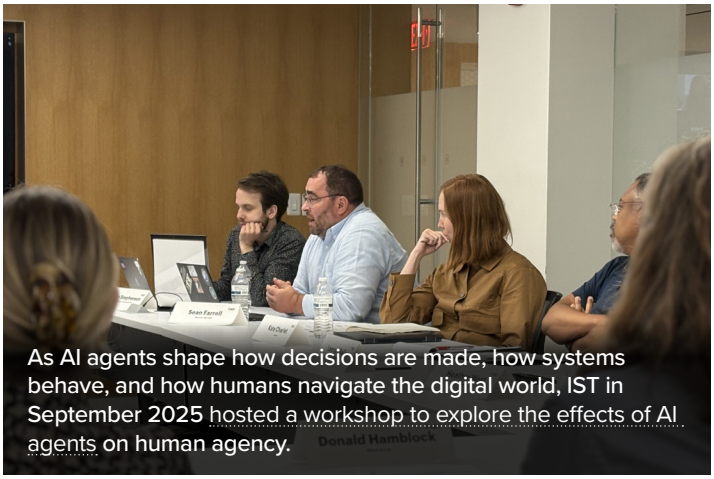
ACT WITH ACCOUNTABILITY: We value integrity over self-interest and hold ourselves and our work to the highest standards of ethics and transparency.

ANTICIPATE WHAT'S AHEAD: We leverage our analytical insights, deep experience, and network of experts to foresee and address potential risks of technological innovation.

ENCOURAGE INCLUSIVITY: We promote diverse perspectives and approaches over uniform, homogeneous thinking to produce better analysis, insights, and outcomes.

TAKE ACTION: We operate with agility and a sense of urgency to address emerging security challenges in a rapidly shifting technology and policy landscape.

Philip Reiner joined INTERPOL Secretary General Valdecy Urquiza in January 2025 to discuss the intersection of AI, cyber, and ransomware in "Horizon Scan: Scams and Deep Fakes."



As AI agents shape how decisions are made, how systems behave, and how humans navigate the digital world, IST in September 2025 hosted a workshop to explore the effects of AI agents on human agency.

OUR SUPPORTERS

As a 501(c)(3) organization, IST relies on the generous support of foundations, organizations, government entities, and individuals. Thank you to the following entities and individuals who contributed to our efforts in 2025. We also extend our thanks to a number of donors who chose to remain anonymous.

Adean and Ben Golub Philanthropic Fund
AWS
Banco Santander
Bockus Brown Family Foundation
Coalition, Inc.
Coefficient Giving (previously OpenPhil)
Community Foundation of Santa Cruz County
Craig Newmark Philanthropies
Edge Institute
Eric Grosse & Brenda Baker Donor Fund
Founders Pledge
Future of Life Institute
German Federal Foreign Office
Hellman Family Fund
William and Flora Hewlett Foundation
Loewenstern Fund
Longview Philanthropy
Mastercard
Meta
Microsoft
Organization of American States
Patrick J. McGovern Foundation
Silicon Valley Community Foundation
Special Competitive Studies Project
Swiss Federal Department of Foreign Affairs
The Policy Development Contribution Program (PDCP) of Canada
Zscaler

INTERESTED IN SUPPORTING OUR WORK?

Get in touch with **Emma Hollingsworth**, *Senior Director of Development and Partnerships*, to learn more.

DONATE

IST joined the Counter Ransomware Initiative for the fourth year in a row in October 2025 in Singapore to deliver findings on public-private partnerships to combat cybercrime.


IST Chief Strategy Officer Megan Stifel delivered a keynote at CyberNextDC in October 2025 looking at cyber policy 'through the looking glass' of the Ransomware Task Force.

THE SECURITY LEVEL 5 TASK FORCE

Setting the bar for AI lab security

What does it take to train a frontier AI model? A lot. Beyond the hundreds of millions of dollars in computing resources, there are research and development costs, infrastructure build-outs, and even untold efforts to collect and store the data that will be used for training runs.

What does it take to secure that investment from highly resourced nation state adversaries, in particular the model weights, algorithms, and unique architectures that drive how it processes inputs and generates outputs? And as these systems grow more capable and threaten to outpace human understanding and control, what is being done to ensure the security of the most powerful AI systems of the future, including those that may be designing and building their successors? Until recently, there has not been a clear answer. Despite the billions pouring into AI development and the ever-increasing applications of AI systems to every field imaginable, including the military, efforts to secure them have consistently struggled to keep pace with the technology itself.

In late 2024, RAND published a study that considered the threats facing model weights in particular—from business competitors to advanced intelligence services—and mapped how feasible it would be to exploit specific parts of the AI ecosystem. They concluded that AI secrets need to be treated like national security secrets, able to withstand attacks by the most capable nation-state threat actors. RAND proposed five security levels for protecting model weights, each calibrated to an increasingly capable adversary—from amateur hackers at Level 1 to top-priority nation-state operations at Level 5. No organization has achieved SL5, and RAND concluded it isn't yet possible with today's tools and practices. But with AI capabilities advancing rapidly, the window to build that capacity is narrowing.

Enter IST. With support from Coefficient Giving, we incubated the SL5 Task Force to translate these high-level directives into practical standards. Through simultaneous executive and technical tracks, we brought together over 100 participants, including security engineers from frontier AI labs, government security specialists, and data center providers, to translate the SL5 framing into practical steps to protect the core of a new technological era.

The SL5 Task Force moved with the urgency needed for this unique moment in the history of technology. By the end of 2025, we finished the SL5 Standard for AI Security (v0.1), a NIST SP 800-53 overlay with 43 controls across 10 families, covering the long-lead-time investments that must begin now to preserve SL5 optionality by 2028/2029. The standard addresses five security streams: network, physical, machine, personnel, and supply chain. The task force also proposed industry-adaptable clearance levels for artificial intelligence labs, among other novel solutions to meet the SL5 need.

To lower the barrier to adoption, SL5 released open source tools, including an interactive IL6 control catalog for organizations to explore the DoD security control overlays that serve as a baseline for SL5. And beyond standard-setting, the Task Force's work has already informed policy engagement: IST drew on SL5 research in its formal response to NIST's AI Safety Institute request for information on mitigating risks across the AI lifecycle.

Beyond protecting against external threats, SL5 also provides a foundation for containing increasingly autonomous AI systems, an equally critical challenge as capabilities advance. The stakes could not be higher. The future of our economy, our national security, and humanity itself are now inexorably tied to artificial intelligence—

AND IST IS LEADING THE WAY, WORKING DIRECTLY WITH INDUSTRY LEADERS TO ENSURE THE SYSTEMS AND INTELLECTUAL PROPERTY UNDERGIRDING THIS REVOLUTION ARE SECURE.

AI RISK REDUCTION

Shaping how institutions and nations approach AI risks

Powerful AI systems are embedded in the decisions that shape our daily lives: approving loans, determining social media algorithms, diagnosing disease, and transforming national security functions and missions. The promise is extraordinary, but so is the peril. The development and proliferation of AI technologies pose a variety of risks, including compliance failure, malicious use, and AI loss of control.

The window to seize the opportunities while guarding against the risks is narrow, and the technical complexity of the problem is outpacing the policy community's ability to meaningfully engage.

IST's AI Risk Reduction Initiative is closing that gap. In 2025, the initiative brought together more than 30 leaders from AI labs, government agencies, and research institutions in working groups to translate abstract concerns into practical, actionable interventions.

That collaboration is now playing a major role in real-world policy processes. IST contributed to the Paris Peace Forum's AI governance blueprint and submitted comments on the NIST AI risk management guidelines and White House AI Action Plan, bringing technical, expert-informed depth and insight to processes that can often leave those considerations out. To test these ideas under pressure, IST ran two crisis simulation exercises that placed policymakers and industry representatives in scenarios—such as potential loss of control over an AI model–and prompted them to make decisions under pressure in a hypothetical environment before they need to be made for real.

> "IST's work on Loss of Control risks is exceptional because it doesn't stop at the theoretical level–it translates these insights into carefully refined operational standards for monitoring LOC in the real world, adapting assessment frameworks first developed and field-tested by the intelligence community. In doing so, their work sets a new standard for what rigorous and grounded research on existential risk could look like."
>
> **Broderick McDonald**
> *University of Oxford & The Alan Turing Institute*

Mariami Tkeshelashvili and Jennifer Tang led an AI crisis simulation exercise in April 2025 based on a high-stakes, time-sensitive scenario involving ambiguous intelligence related to a potential loss-of-control incident at a frontier AI lab.

The results are already visible in the institutions and people shaping AI's trajectory. Inspired by IST's work, Anthropic launched a Transparency Hub tracker. The Korea AI Safety Institute is drawing on IST's frameworks to develop an AI Risk Map. Decision-makers across government and industry are walking away from IST engagements with focused, immediately actionable technical interventions and policy mitigations.

AI governance is one of the defining policy challenges of our time. The decisions being made now will set the groundwork for decades to come. At IST, we're not waiting for the consensus to emerge on its own—

WE'RE BUILDING THE INTELLECTUAL INFRASTRUCTURE TO ACT NOW.

K-12 CYBER DEFENSE COALITION:
Inserting school cybersecurity into the congressional conversation

Ransomware attacks against K-12 schools have become, in many ways, a national crisis. For too long, the burden of defending against nation-state and transnational criminal actors has fallen on individual districts, who have few resources and no back-up. In 2025, IST set out to change that.

The first step was gathering stakeholders. IST launched the K-12 Cyber Defense Coalition, a collective of 13 national education organizations to pool the knowledge and expertise needed to combat the threat. The Coalition quickly established IST as the go-to convener for K-12 cybersecurity policy, creating the national platform needed to act when the moment arrived.

That moment came when Congress began signaling its intent to reform the E-Rate program, the federal fund that finances school broadband. The FCC had just closed a wildly successful (and wildly oversubscribed) $200 million pilot to bring cybersecurity resources into schools–proof that the need was urgent and the supply did not match the demand. But with the pilot coming to an end, no permanent funding was available to take its place. IST recognized the opportunity.

IST experts moved quickly, publishing op-eds, hosting events, and distilling the policy landscape into a focused memo that gave policymakers a clear framework for action. In September 2025, IST submitted formal comments to the Congressional Universal Service Fund Working Group to offer technical assistance and concrete recommendations for modernizing the Fund to address the cyber threats facing our students.

> "We don't expect every town to stand up their own army to protect themselves against China or Russia. In the same way, I don't think we should expect every school district to stand up their own cyber-defense army to protect themselves against ransomware" attacks from major criminal groups."
>
> **Michael Klein**
> Senior Director for Preparedness and Response
> in an article by *The Hechinger Report*, *June 1, 2025*

The result speaks for itself. Congress is now actively considering amending the E-Rate statute to incorporate cybersecurity—

A CHANGE THAT COULD UNLOCK POTENTIALLY BILLIONS IN NEW RESOURCES FOR THE NATION'S MOST VULNERABLE STUDENTS.

IST education lead Michael Klein joined a Jefferson County Public Schools press conference in Louisville, KY, to help district leaders announce federal grant funding and hear directly from teachers and cybersecurity practitioners on the front lines.

COMMON VULNERABILITIES AND EXPOSURES:

Blazing a new trail for a venerable vulnerability program at a crossroads

In April 2025, the cybersecurity world awoke to shocking news. The Common Vulnerabilities and Exposures (CVE) Program, the canonical database for all known software defects, would shut down within days due to contract problems with the Department of Homeland Security.

The reaction was immediate: companies, researchers, and governments decried the loss of this critical resource that enables cyber defenders the world over to communicate unambiguously about flaws in computer code. While the funding was quickly restored, the ecosystem was shaken. Could CVE be relied upon anymore? Would new naming schemes spring up, fracturing the vulnerability landscape in a cybersecurity Tower of Babel moment?

IST met the moment. Quickly recognizing the potential for calamitous disharmony, the team began designing a policy framework to reform the CVE Program and put it on firmer footing. The resulting report put forward actionable recommendations for the development of a Global Vulnerability Catalog, supported by national vulnerability management programs. It called for substantial reforms to the program's governance, including empowering a multistakeholder board of directors and diversifying funding beyond simply the U.S. government. It also unpacked common vulnerability management programs into their constituent functions to help policymakers understand what needs to be universal and what can differ from country to country or region to region.

Through engagements with policymakers across the globe, the IST team helped create space for dialogue to preserve the program, including a call for U.S. leadership to bring in other government partners and act quickly to prevent fragmentation. Leaders in Congress have looked to the report as they draft legislation codifying a vulnerability catalog. IST's work on CVE continues to provide industry and government partners with a clear articulation of a way forward for the program.

48,185

CVE Records

The number of vulnerabilities published in the Common Vulnerabilities and Exposures Program database in 2025—the most on record

"The worst case is fragmentation. The second worst case is, government comes in and says we're going to supplant the expertise that's been built up over 25 years."

Senior Vice President for Policy Nick Leiserson joined the McCrary Institute Cyber Focus podcast with Frank Cilluffo in to discuss the future of the CVE Program.

Vulnerability management as we know it could not exist without CVE. But at IST, we're not just focused on trying to reverse history or restore the program to its former self—

WE'RE LAYING OUT A FORWARD-LOOKING VISION FOR ANOTHER QUARTER CENTURY OF PROGRESS IN PRODUCING TRUSTED TECHNOLOGY.

Cyber & Critical Infrastructure

UNDISRUPTABLE27

When cybering up isn't an option, consequence down

How long can a hospital go without water? Four hours. When the power goes out, hospitals have generators. When communications go dark, they can use paper and pencil. But without water, the clock starts ticking. And unless pressure is restored quickly, the facility ceases to function. Given that in medical emergencies, seconds count—time is brain—the closure of a hospital can mean the difference between life and death.

Yet water utilities are increasingly on the front lines of cyber conflict. Chinese military units have been found "pre-positioning" on U.S. water systems, gaining access and conducting reconnaissance in order to conduct devastating cyber strikes in the case of conflict. Utilities are in the crosshairs, but the hospitals who depend on them are potentially collateral damage.

IST's UnDisruptable27 (U27) project is working to build societal resilience in the run up to 2027, the year Chinese leadership has targeted for its military to be prepared to invade Taiwan. Led by hacker and policy entrepreneur Josh Corman, the U27 team is intent on co-creating engineering-first solutions that can help communities across the country turn knockout punches in cyberspace into glancing blows.

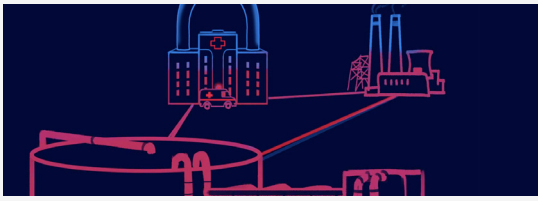
In 2025, with the foundational support of Craig Newmark Philanthropies, U27 focused on developing its novel methodology. While water has long been regarded as a weak link in critical infrastructure cybersecurity, aging systems and underfunding have made shoring up its cyber defenses incredibly challenging. Drawing on engineering guidance from the National Laboratories, U27 explored techniques to make small changes in system design—like the installation of water pressure "circuit breakers"—that effectively immunize utilities no matter their cyber maturity.

In 2026, the team is taking their program on the road to iterate on the approach side-by-side with utility owners and operators while simultaneously building the network they'll need to scale it to the 6,000 hospital communities across the country. Leading with empathy. Tackling tough, urgent problems. Designing solutions with scaling in mind.

THAT'S THE IST WAY.

> "With great connectivity comes great responsibility. And while we're struggling to protect credit cards or websites or data, we continue to add software and connectivity to lifeline infrastructure like water and power and hospitals. We were always prey."
>
> **Josh Corman**
> *Executive in Residence for Public Safety & Resilience* sat down with The Verge for a Q&A on what sectors are at risk, the consequences of a cyber attack, and UnDisruptable27's plan to increase community resilience.

> "No water means no healthcare. The hospital can't run without clean water. No water means no sterilization, no surgery scrubbing, no laboratories, and eventually, no access to life-saving care.... We must strive to make our lifeline basic needs undisruptable, and where we cannot, ensure that our communities are more resilient under fire."



AI AND NUCLEAR COMMAND, CONTROL, AND COMMUNICATIONS:

Navigating the most consequential intersection in modern security

Nuclear command, control, and communications systems (NC3)–the architecture that connects nuclear weapons to the humans authorized to use them—were designed for a different era.

Though some level of automation has been a part of NC3 systems for decades, nuclear-armed states are increasingly looking to modernize their nuclear infrastructures and architectures —and several nuclear-armed states are considering tying in more general-purpose AI systems with their military platforms. For example, they may look to use AI to augment their strategic warning systems, provide decision support, or adapt targeting as new intelligence becomes available or battlefield conditions change.

As AI capabilities advance and the pressure to incorporate new use cases into military infrastructure grows, how can we ensure that this integration is carried out safely and securely? It's increasingly essential to bring together the industry experts from frontier AI laboratories who understand what these models do with the nuclear strategists who understand what's at stake.

In April 2025, IST did just that: the Nuclear Policy team brought both worlds together for a rare workshop that surfaced specific challenges and opportunities in AI-NC3 integration, like the technical reliability, testing and evaluation, and security of AI systems, governance frameworks that balance transparency with operational security and the evolution of military doctrine in an AI-enhanced nuclear context. To continue and capitalize on the workshop's momentum, IST established working groups with participants including the CEOs of technical companies and globally-recognized scholars, as well as a former Commander of U.S. Strategic Command, a former Deputy Secretary General of NATO, and a former Director of the Defense Threat Reduction Agency.

Public findings from this work have reached audiences at SIPRI's Stockholm Security Conference, Scale.AI, AI+ Expo, Outrider Foundation, and other international fora. Through technical primers, policy explainers, and carefully orchestrated convenings...

> "The intersection of artificial intelligence and nuclear command, control, and communications is one of the most consequential and perhaps least understood strategic issues of our time. IST is playing a vital role by bringing together a diverse group of policy, technical, and operational experts to examine the risks, opportunities, and necessary safeguards from multiple perspectives. I'm honored to be part of this critical effort."
>
> **Lt. Gen. Jack Shanahan (USAF, Ret.)**
> *Inaugural Director, Joint Artificial Intelligence Center at U.S. Department of Defense*

> "The AI-NC3 project is a singular body of work, at the exact right time, helmed by a truly world class cadre of leaders. The team's expertise is simply unparalleled: the rare combination of frontier AI knowledge with decades of Nuclear Command and Control operations could not be more perfectly aligned to the challenge at hand. And that challenge - defining the safest and most effective ways to employ AI in NC3 - sits right at the nexus of the world's hardest problems. IST went straight to the heart of our national security imperatives and chose the most intractable one. But never has a team been more prepared to solve it."
>
> **Geoffrey M Schaefer**
> *VP, AI Strategy and Governance, Leidos*

IST IS BUILDING THE SHARED NORMS, CODES OF CONDUCT, TESTING AND EVALUATION STANDARDS, AND NUCLEAR RISK REDUCTION AND MITIGATION MEASURES NEEDED TO ENSURE THAT THE INTEGRATION OF AI AND NC3 DOES NOT RESULT IN CATASTROPHIC CONSEQUENCES.

IST in the News

As Trump pivots to Russia, allies weigh sharing less intel with U.S.
Dan De Luce, Courtney Kube, Carol E. Lee and Kevin Collier, *NBC*, March 6, 2025

ROOST Reminds Us Why Open Source Tools Matter
Fatima Faisal Khan, *Tech Policy Press*, March 17, 2025

"Just as open source helped software development to evolve into a field characterized by collaboration and rapid innovation, the trust and safety field has the potential to redefine itself through open source."

Fatima Faisal Khan
Senior Associate for Ecosystem Trust and Safety

Inside a romance scam compound—and how people get tricked into being there
Peter Guest, Emily Fishbein, *MIT Technology Review*, March 27, 2025

Cyberdefense cuts could sap U.S. response to China hacks, insiders say
Joseph Menn, *Washington Post*, May 23, 2025

"This is no time to pull defenders from the resilience and continuity of operations of lifeline human needs like water, power and access to emergency care. The coming storms need more help and better help. The risks are nonpartisan and affect all communities."

Joshua Corman
Executive in Residence for Public Safety and Resilience

Trump cuts could expose student data to cyber threats
Jill Barshay, *The Hechinger Report*, June 1, 2025

How vulnerable is critical infrastructure to cyberattack in the US?
Justine Calma, *The Verge*, June 27, 2025

How spy agencies are experimenting with the newest AI models
The Economist, July 29, 2025

"There still remains a huge gap in our understanding as to how and how far China has moved to use DeepSeek [for military and intelligence gaps]. They probably don't have similar guardrails like we have on the models themselves and so they're possibly going to be able to get more powerful insights, faster."

Philip Reiner
Chief Executive Officer

Cyberthreats grow as school budgets shrink
Dana Nickel, *POLITICO*, September 4, 2025

Trump's Vagueness Over Nuclear Testing Could Fuel an Arms Race
Sahil Shah, *Foreign Policy*, *October 30, 2025*

"History shows that ambiguity about nuclear intent is destabilizing. A phrase such as 'resume nuclear testing' can be interpreted in different ways: a political flourish to show resolve; an order to increase testing of nuclear-capable delivery systems; an instruction to expand simulations and subcritical experiments; or, worst of all, authorization of explosive nuclear warhead detonations."

Sahil V. Shah
Senior Adjunct Advisor for Nuclear Policy

Don't let Congress punt on cyber insurance reform
Nick Leiserson and Mark Montgomery, *Cyberscoop*, November 3, 2025

When it comes to nukes and AI, people are worried about the wrong thing
Joshua Keating, *Vox*, November 20, 2025

Scaling Disruption: What the Next Cyber Strategy Must Get Right
Megan Stifel, *Claroty Nexus*, December 2, 2025

2025 Reports

Deterring the Abuse of U.S. IaaS Products: Recommendations for a Consortium Approach

Malicious cyber actors have long employed network obfuscation techniques to route and launder their traffic, including leveraging Infrastructure as a Service (IaaS) products to exploit U.S. targets. In 2024, the U.S. Department of Commerce proposed a new rule that could require all U.S.-based IaaS providers to implement an Abuse of IaaS Products Deterrence Program (ADP). Authors Steve Kelly and Tiffany Saade present recommendations for how an ADP Consortium, powered by AI and privacy-preserving technologies, could be best shaped to deter abuse.

FEBRUARY 2025

Navigating AI Compliance, Part 2: Risk Mitigation Strategies for Safeguarding Against Future Failures

How exactly can AI builders and users defend against future failure risks, and increase trust in their products? In the second report of a two-part series, authors Mariami Tkeshelashvili and Tiffany Saade propose risk mitigation strategies inspired by lessons learned from case studies of institutional, procedural, and performance failures in AI-adjacent industries explored in Part 1. By developing an actionable compliance pathway for AI builders and users tailored to each stage of the AI lifecycle, they aim to bridge the gap between the drive to AI innovation in global markets and the desire to manage risk.

MARCH 2025

Enhancing Cyber Resilience through Insurance: Revisiting Anti-Bundling Regulation

Small- and medium-sized businesses in particular struggle to understand and mitigate the full extent of their exposure to cyber risk. Nearly two decades after Bruce Schneier predicted that cyber insurance would become synonymous with cybersecurity, while a majority of large corporations are insured against threats, only 10% of SMEs hold policies. Authors Sophia Mauro and Taylor Grossman explore how cyber insurance can bolster ecosystem-wide cyber resilience by unpacking one set of incentive structures: bundling.

APRIL 2025

Strengthening Nuclear Crisis Communications: Steps to Implement Mesh Networks to Enhance Resilience & Security

In November 2024, IST convened a diverse group of experts for a technical workshop to advance discussions on improving the resilience of nuclear crisis communications systems. In this after-action report, author Christian Steins presented and summarized the working group's recommendations to guide the CATALINK initiative's ongoing efforts to enhance nuclear crisis communication infrastructure, focusing on the technical development of a resilient, global wireless mesh network.

MAY 2025

2025 Reports (cont.)

Securing the Signal: Mitigation Strategies to Strengthen Crisis Communication Channels

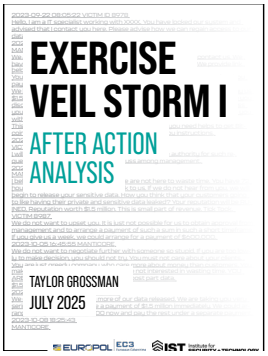
Amid challenges to global norms and accelerating development and adoption of emerging technologies, crisis communication systems between nuclear-armed states face urgent new threats. Designed to prevent escalation, these channels are increasingly vulnerable to both technical interference (e.g., cyber attacks, deepfakes) and diplomatic misuse (e.g., refusal to respond, use for coercion). Author Christian Steins identified four critical scenarios and outlined a matched set of mitigation strategies designed to reinforce the reliability of crisis communications in high-stakes environments.

MAY 2025

Nuclear Command, Control, and Communications (NC3): A Primer on Strategic Warning, Decision Support, and Adaptive Targeting Subsystems

Nuclear Command, Control, and Communications (NC3) systems are critical to ensure the authorized use of nuclear weapons. What exactly is NC3, and how might AI be integrated into each of its subsystems? Authors Alice Saltini, Sylvia Mishra, and Philip Reiner presented a technical and in-depth overview and analysis of strategic warning, decision support, and adaptive targeting subsystems that comprise the NC3 "system of systems."

JULY 2025



Exercise VEIL STORM I: After Action Report

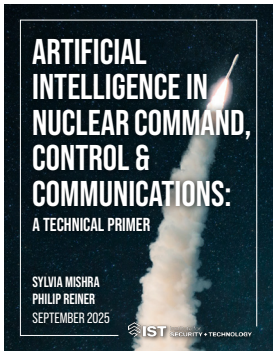
Information sharing is a crucial part of public-private collaborations to disrupt threat actors and mitigate cyber incidents. In partnership with Europol European Cybercrime Centre, IST and the RTF's International Engagement Working Group designed and delivered Exercise VEIL STORM I, a tabletop exercise focused on operational collaboration across international law enforcement agencies and private sector firms in responding to cyber incidents. In this after action report, author Taylor Grossman summarized the proceedings and key takeaways of the exercise.

JULY 2025

Improving Private Sector Cyber Victim Notification and Support

Notifying victims of a cyber incident is key to mitigating harm, but providing timely, secure notifications has proven a challenge across industries. Building off the Cyber Safety Review Board of Directors' recommendation that cloud service providers work with mobile device platform vendors to develop an Amber Alert-style notification mechanism, author Rob Knake explored the challenges to developing the native-notification concept, and laid out a roadmap for overcoming them.

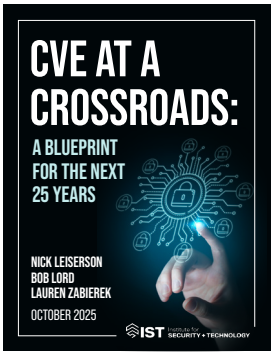
AUGUST 2025



Artificial Intelligence in Nuclear Command, Control & Communications: A Technical Primer

Automation and AI have been integral to nuclear weapons systems and operations for decades. Given AI-enabled tools' ability to assess enormous amounts of intelligence data at unprecedented speeds, the integration of modern AI machine learning programs with nuclear command, control, and communications systems can only grow with time. Ahead of a scenario-driven workshop hosted by IST, Sylvia Mishra and Philip Reiner co-authored a short primer to establish what constitutes 'novel' AI in the context of nuclear weapons decision-making.

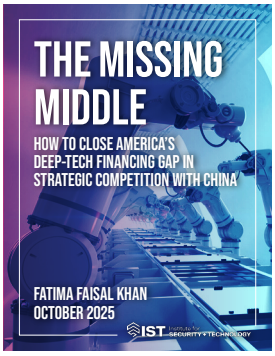
SEPTEMBER 2025



CVE at a Crossroads: A Blueprint for the Next 25 Years

The Common Vulnerabilities and Exposures (CVE) Program has been a core element of software security since 1999. Yet it is at a crossroads. After narrowly avoiding a shutdown in April 2025, issues with continued funding have laid bare fundamental challenges, and without action, the vulnerability identification landscape will fragment. Report authors Nicholas Leiserson, Bob Lord, and Lauren Zabierek provided recommendations for global policymakers on how to reimagine the CVE Program for the next 25 years.

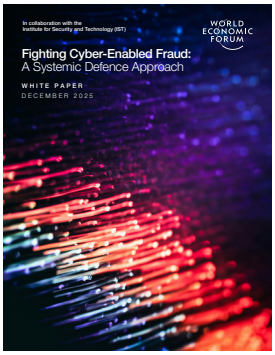
OCTOBER 2025



The Missing Middle: How to Close America's Deep Tech Financing Gap in Strategic Competition with China

The United States and China are locked in competition to finance and deploy foundational technologies that will underwrite economic leadership and ensure national security for decades to come. Building on the prior work of IST's Strategic Balancing Initiative, author Fatima Faisal Khan dug into the systematic gap between early-stage capital and late-stage financing facing American deep-tech companies, and explored the strengths and weaknesses of China's bifurcated system.

OCTOBER 2025



Fighting Cyber-Enabled Fraud: A Systemic Defence Approach

Across the globe, phishing and cyber-enabled fraud are escalating, targeting individuals as well as businesses and governments. How can we begin to turn the tide? The World Economic Forum's Partnership against Cybercrime, in collaboration with IST, presented a systemic defense framework to confront this challenge. IST authors Steve Kelly, Jennifer Tang, Tiffany Saade, and Taylor Grossman, along with WEF authors Tal Goldstein and Giulia Moschetta, call for strengthening safeguards at the foundational layers of the internet, embedding user safety by default, and enabling rapid detection and collective response to incidents when they occur.

DECEMBER 2025

StatISTics: IST's 2025 by the Numbers

97,650

Linkedin members engaged with our updates, announcements, and events

175

mentions of IST's experts and work across major media outlets

6,764

subscribers receive IST's monthly newsletter, *The TechnologIST*, in their inboxes each month.

Most-read editions:

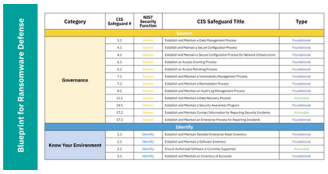
- » The Strategic Potential of Cyber Insurance
- » Defending our Lifeline Sectors
- » Approaching the Nuclear Brink?

83,677

unique active users visited our newly-updated website, **up 22%** from 2024

62 blogs

published by IST's experts in 2025 analyzed recent policy proposals, unpacked findings from working group sessions and public events, and announced new lines of effort. Top blogs:



Governance and Cyber Risk for SMEs: Remapping the Blueprint for Ransomware Defense

The RTF developed the Blueprint for Ransomware Defense in 2022 to provide SMEs with an actionable framework to defend against common attacks, aligning with NIST's Cybersecurity Framework 1.0 – this year, IST's Michael Klein remapped the Blueprint to NIST's updated framework, incorporating a new core function and updating key considerations for the most vulnerable SMEs.

NOVEMBER 2025

Cracked and Nulled: International Law Enforcement Takes Down Two of the World's Largest Cybercrime Forums

IST's Gigi Flores Bustamante examined the joint international law enforcement operation in January to disrupt Cracked and Nulled, two of the world's largest cybercrime forums, noting key actions and the collaboration's strategic approach to disrupting ransomware.

MARCH 2025

Bridging the Policy, Military, and Technology Fields: IST Hosts Critical Workshop on AI in Nuclear Command, Control, and Communication Systems

IST's Sylvia Mishra reflects on an April workshop hosted by the Innovation and Catastrophic Risk team to present cross-sector experts in Washington, D.C. with a scenario-driven exercise built to examine the risks and opportunities of the integration of AI into nuclear command, control, and communications systems.

APRIL 2025

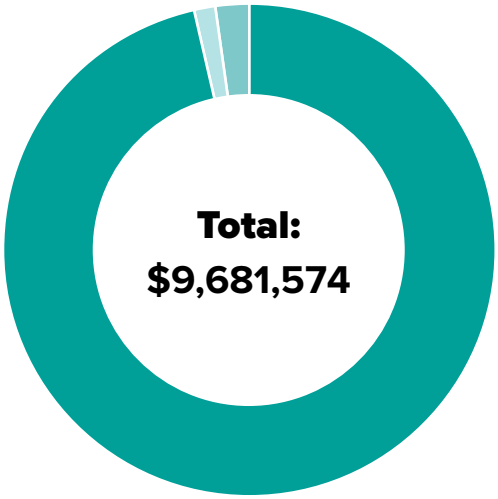
Setting the Foundation of a New National Strategy on AI: IST Submits Comments on an AI Action Plan

Informed by eight years of engagements with stakeholders across the ecosystem, IST submitted public comment to the White House Office of Science and Technology Policy on the development of an AI Action Plan, offering 6 strategic objectives that could serve as the foundation of a new national strategy on AI.

MARCH 2025

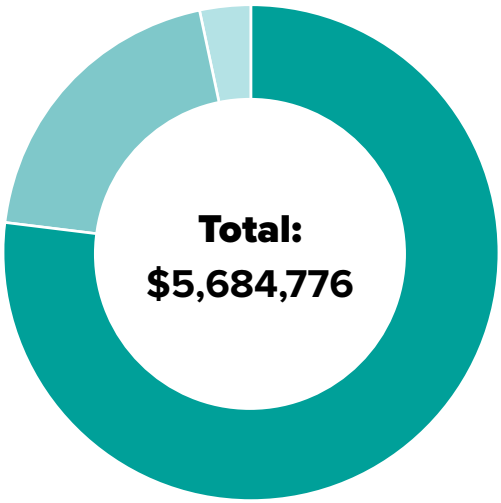
IST Financials

FY 2025 Revenue*



Non-Government Grants	$9,279,924
International Government Grants	$201,263
Contributed Income	$124,211
Other	$76,176
Fiscal Sponsorship	$0
Sponsorship Income	$0
Government Grants	$0
Total	**$9,681,574**

FY 2025 Expenses



Program	$4,390,346
Administrative	$1,117,396
Fundraising	$177,034
Fiscal Sponsorship	$0
Total	**$5,684,776**

Note: Graphs and tables include IST 2025 operational financial data.
For further information and analysis please refer to forthcoming 2025 audited financials.