THE INSTITUTE FOR SECURITY AND TECHNOLOGY

2024 ANNUAL REPORT

Contents

LETTER FROM THE CEO

Philip Reiner
Chief Executive Officer

Dear IST Supporters,

I want to take a moment to reflect on the challenges and triumphs of 2024 and to express our deep gratitude for your unwavering support.
Our role as the critical action think tank has never been more vital. Technological breakthroughs are advancing at an unprecedented rate, bringing both extraordinary benefits and significant risks. From generative AI and cyber vulnerabilities to new challenges posed by quantum computing, we find ourselves navigating a landscape that is rapidly evolving—and often unpredictable. This demands novel approaches to ensure we meet these challenges while seizing the massive benefits they portend for democratic societies as a whole.

At the *Institute for Security and Technology (IST*), we are dedicated to ensuring that as technology accelerates, we are taking creative, collaborative, and impactful steps to safeguard our communities, businesses, governments, and society as a whole from these emerging security challenges.

In 2024, we worked tirelessly to accomplish this mission and to advance a democratic world secured and empowered by technology built on trust. With your support, we brought together experts, policymakers, and thought leaders from across sectors to collaborate and drive innovative solutions. Together, we made meaningful strides in critical areas:

- **Ransomware Resilience:** The Ransomware Task Force (RTF) continued to drive impactful progress in the fight against ransomware and other cybercrime, with 92% of its recommendations seeing some or significant progress. The RTF testified in front of Congress, weighed in on cyber incident reporting regulations in the United States and worldwide, and built a map of the information sharing process in the ransomware payment ecosystem to help drive disruption efforts.

- **Generative AI's Impact on Cognition, Society, and the Future:** We published a groundbreaking report examining how GenAI may affect social cohesion and delivered a comprehensive research agenda for policymakers, industry leaders, and researchers.

In April 2024, IST, in partnership with the Center for Cybersecurity Policy and Law (CCPL), hosted the Inaugural Cyber Policy Awards, which recognized five recipients of the Cyber Policy Award of Merit for U.S. domestic policy impact, international policy impact, ecosystem championship, and cyber philanthropy.

- **AI Risk Reduction:** We worked with researchers, leading AI labs, and policy experts to propose policy and technical interventions across each stage of the AI lifecycle that target malicious use and compliance failure. In November, inspired by IST's work, a leading AI lab outlined key practices for responsible AI development.

- **UnDisruptable27:** At BSides in Las Vegas, we launched a new initiative to protect lifeline critical infrastructure that leverages storytelling to inform, influence, and inspire action on increasingly unnatural disasters, and initiated the community-building phase with outreach to formal public-private partnerships, relevant trade associations, asset owners and operators in water and emergency medical care, and relevant national labs.

- **Cybersecurity Partnerships:** As the only United States-based organization on the Private Sector Advisory Panel of the Counter Ransomware Initiative, we participated in the 2024 Summit at the White House. IST continues to assist partners around the globe, including through capacity building to raise baseline resilience and efforts to help combat the flow of profits to ransomware actors. IST also partnered with the World Economic Forum's Partnership Against Cybercrime on a project to identify, develop, and promote a set of high-impact, ecosystem-level "systemic defence" approaches to counter phishing and cybercrime.

- **Strengthening National Security:** Through our Strategic Balancing Initiative, we worked with experts across energy, quantum, and biotech to develop actionable ways to address U.S.-China techno-industrial competition—contributing directly to an expanded federal understanding of the role and impact of venture capital and the need for greater focus on capital gaps for advancing national security critical technologies.

These projects and collaborations are just a few of the many ways our work has had significant global impact. From anticipating emerging security challenges and cultivating collaborative networks to creating common understanding and activating insights with action, this year's Annual Report encapsulates the bespoke "IST way" of driving problem-solving.

The work we do is complex and urgent, but we are constantly inspired by the dedication and commitment of our team, our partners, and, most importantly, YOU. Your continued support—through financial contributions, participating in our convenings, or volunteering time and expertise—is what fuels this impact and our continued ability to provide positive benefits for so many people everyday.

We are determined to build on these successes, expand our impact, and continue to confront the toughest questions at the intersection of technology and security. This is a long term project, and it demands our unwavering commitment. We will continue to engage, collaborate, and innovate, always with the goal of building a safer, more secure future for everyone.

Thank you again for your generous support.

TOGETHER, WE ARE MAKING A LASTING DIFFERENCE.

Chief Trust Officer Steve Kelly testified before the House Committee on Oversight and Accountability Subcommittee on Cybersecurity, Information Technology, and Government Innovation.

In October, IST and the Berkeley Center for Long-Term Cybersecurity hosted an in-person dialogue to discuss how cybersecurity can support a new renewable energy infrastructure.

At REAIM 2024 in Seoul, Korea, IST CEO Philip Reiner moderated a panel on the integration of artificial intelligence in NC3 and explored its implications for the global nuclear order.

OUR SUPPORTERS

As a 501(c)(3) organization, IST relies on the generous support of foundations, organizations, government entities, and individuals. These contributions enable us to continue putting forward actionable solutions to some of the most complex national security challenges. Thank you to the following partners, in-kind supporters, and individuals and private philanthropists who contributed to our efforts in 2024. We also extend our thanks to a number of donors who chose to remain anonymous.

aws

Santander

BANK OF AMERICA

Bockus Brown Family Foundation

censys

Cooley

Coalition

COMMUNITY FOUNDATION
SANTA CRUZ COUNTY

Craig Newmark Philanthropies

Federal Foreign Office

FORTINET

GFCE

JCF JEWISH COMMUNITY FEDERATION & ENDOWMENT FUND

Longview Philanthropy

Meta Platforms

Microsoft

OMIDYAR NETWORK

paloalto NETWORKS

Patrick J McGovern FOUNDATION

Private Philanthropy

SILENT PUSH

SURVIVAL & FLOURISHING FUND

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Federal Department of Foreign Affairs FDFA

The Swiss Confederation, represented by the Swiss Federal Department of Foreign Affairs

tides

On the recommendation of Google Community Grants Fund

WILLIAM + FLORA
Hewlett Foundation

zscaler

Current investments do not adequately support Internet-enabled social and economic progress for everyone. At RSA 2024, Megan Stifel joined a panel discussion on Common Good Cyber, which looked at how to institutionalize support for common good cybersecurity and build adequate funding into law, policy, business processes, and government.

IN 2024, WE...

WE ENVISIONED A DEMOCRATIC WORLD SECURED AND EMPOWERED BY TECHNOLOGY BUILT ON TRUST.

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.

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.

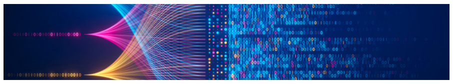
Take action: We operate with agility and a sense of urgency to address emerging security challenges in a rapidly shifting technology and policy landscape.

IN 2024, WE...

ANTICIPATED EMERGING SECURITY CHALLENGES, IDENTIFYING NEW THREATS BEFORE THEY CAUSE REAL-WORLD HARM AND TAKING ACTION TO STOP THEM.

The Institute for Security and Technology's efforts to advance national security and global stability encompass three thematic focus areas: *The Future of Digital Security*, *Innovation and Catastrophic Risk*, and the *Geopolitics of Technology*. These themes are not exhaustive, nor are they exclusive. Rather, they help to orient the work that we undertake–ensuring that we focus on emerging security challenges as they arise and pinpoint if and how we can intervene.

In 2024, IST launched a variety of new projects, including UnDisruptable27, the Strategic Balancing Initiative, and the Generative Identity Initiative. In each case, we sought to respond to an opportunity or gap that we are uniquely positioned to address by leveraging bespoke convening practices and research. In 2024, we also continued our work to advance efforts like the AI Risk Reduction Initiative, the Applied Trust & Safety Initiative, CATALINK, and the Ransomware Task Force.

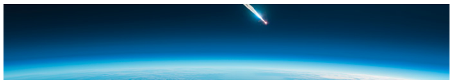


AI Risk Reduction Initiative

Assessing the emerging risks and opportunities of AI foundation models and developing risk reduction strategies

AI and Cybersecurity

Understanding the impact that AI stands to have on the cyber offense - defense balance

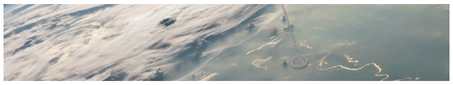


Artificial Intelligence and Nuclear Command, Control, and Communications

Pioneering action-oriented efforts to explore how advanced AI capabilities will be integrated into NC3 systems

Applied Trust & Safety Initiative

Addressing the human risks of technological change



CATALINK

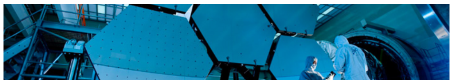
Preventing the onset or escalation of global conflict by building a resilient global communications system

Generative Identity Initiative

Exploring how GenAI will affect social cohesion and the protection of public interest

Ransomware Task Force

Combating the ransomware threat with a cross-sector approach



Strategic Balancing Initiative

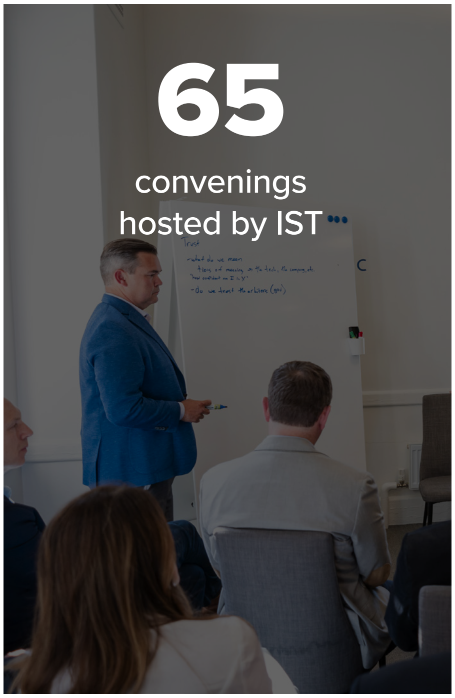
Developing actionable ways to address U.S.-China techno-industrial competition

UnDisruptable27

Driving more resilient lifeline critical infrastructure for our communities

IN 2024, WE...

CULTIVATED COLLABORATIVE NETWORKS ACROSS TECHNOLOGY, INDUSTRY, GOVERNMENT, AND CIVIL SOCIETY, INCORPORATING DIVERSE PERSPECTIVES AND EXPANSIVE TECHNICAL AND POLICY EXPERTISE.

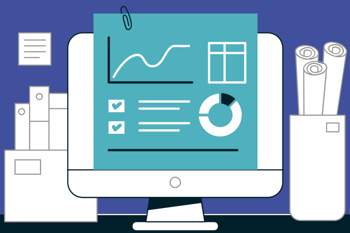


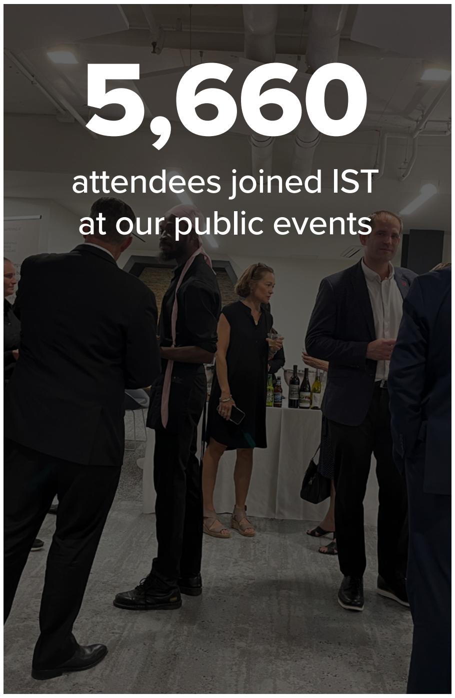
65

convenings hosted by IST

2,500+

reports downloaded on our website





5,660

attendees joined IST at our public events

24

adjunct advisors who provide crucial input on our efforts

90+

conferences, workshops, summits, and events attended by IST experts

AI AND CYBERSECURITY

Surveying the community to get to "ground truth"

AI presents opportunities to transform cybersecurity, but it also presents new risks as malicious actors seek to leverage its capabilities to carry out cyber attacks.

WHAT IMPACT DOES AI STAND TO HAVE ON THE CYBER OFFENSE AND DEFENSE BALANCE?

IST in 2024 embarked on a study of the implications of AI in cybersecurity. To gather the most comprehensive understanding of the current landscape, we surveyed industry incumbents, startups, consultancies, and threat researchers. The survey captured insights into how organizations and practitioners are currently engaging with or integrating AI technologies, the evolving impact of these tools on the threat landscape, and their forecasts for the future.

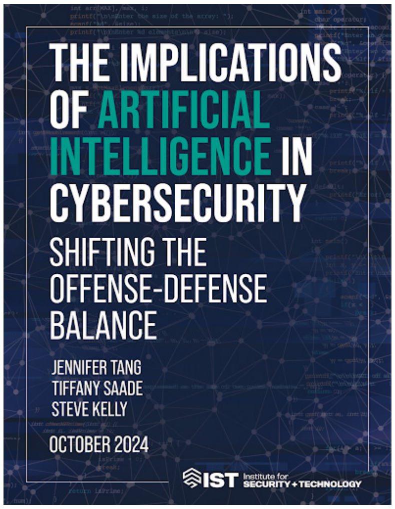
As a result of these efforts—and inspired in large part by the survey responses—we put forward seven key technical and policy recommendations to advance a more secure, sustainable digital ecosystem.

Priority Recommendations:

1. **Protect sensitive data from malicious AI-enabled content analysis.**
2. **Supplement watermarking with alternative deepfake detection approaches.**
3. **Modernize authentication approaches to account for AI.**
4. **Educate society to navigate the challenges brought by AI deepfakes.**
5. **Optimize both human and AI resources to achieve efficiency and software quality.**
6. **Integrate AI into security operations workflows, but protect your models.**
7. **Minimize external attack surface; for critical systems, strive for invisibility.**

Following the release of our findings, we gathered key stakeholders from government, civil society, and industry to invite their feedback on the recommendations, thoughts about the predictions, and input on future work needed to explore the implications of AI in cybersecurity. Ultimately, IST's efforts helped to catalyze the conversation around the implications of AI for cybersecurity, and drove industry and policy efforts to adapt to the changing landscape.

In October 2024, the AI and Cybersecurity team held a gathering in Washington, DC alongside Georgetown University's Center for Security and Emerging Technology (CSET) and the R Street Institute to brief research findings and discuss the implications of AI in cybersecurity.



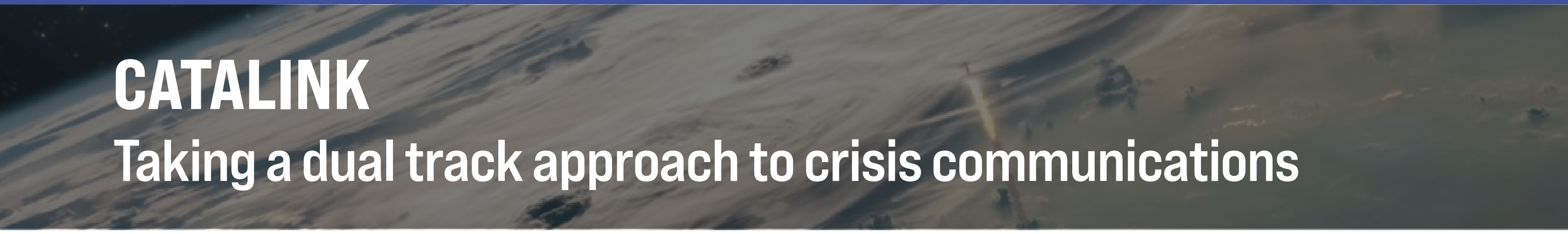
THE IMPLICATIONS OF ARTIFICIAL INTELLIGENCE IN CYBERSECURITY

SHIFTING THE OFFENSE-DEFENSE BALANCE

JENNIFER TANG
TIFFANY SAADE
STEVE KELLY

OCTOBER 2024

IST Institute for SECURITY + TECHNOLOGY



CATALINK

Taking a dual track approach to crisis communications

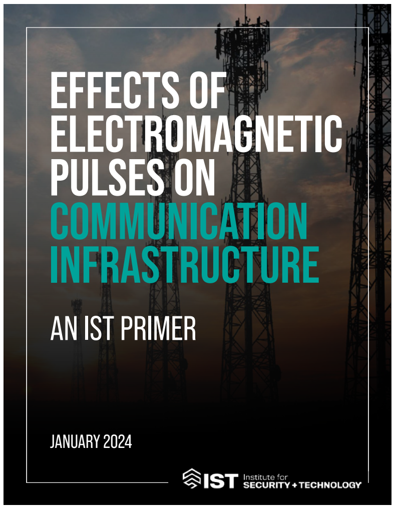
IF A NUCLEAR CRISIS WERE TO ESCALATE, CAN LEADERS FROM NUCLEAR-ARMED STATES COMMUNICATE SECURELY, QUICKLY, AND IN A TRUSTED MANNER?

Since its inception in 2019, the CATALINK project has sought to build an open-source, multilateral, additive crisis communication technology for use by leaders of nuclear-armed states. In doing so, our work has directly contributed to crisis communications being one of the most tangible and actionable paths forward in international negotiations and diplomacy for nuclear risk reduction.

In order to implement such a solution, the initiative has embarked on a dual track approach: building a technical blueprint that would allow leaders to communicate and ensuring political awareness and salience that would enable its adoption. During 2024, CATALINK continued work on both, seeking to build consensus around the need for nuclear risk reduction and secure, multilateral crisis communications and to advance technical understanding of the components needed in such a system.

In November 2024, IST hosted a technical workshop in Washington, DC, that brought together participants from fields including space exploration, mesh network infrastructure, government contracting, and the National and Nuclear Risk Reduction Center. The workshop proposed exploring the feasibility of integrating orbital-based mesh networks into the CATALINK system to maintain connectivity even if conditions on the ground are significantly degraded. At the same time, CATALINK continued efforts to engage government representatives and global policymakers on the political path forward to advance secure nuclear crisis communications efforts. In 2024, the team worked with experts to understand the history, perceptions, and perspectives on nuclear crisis communication in the United States, United Kingdom, and France; Russia; China; Pakistan; and India and met with diplomats worldwide to socialize the concept with the nuclear-armed and non-nuclear armed states whose acceptance is crucial to CATALINK's success.

An electromagnetic pulse, or EMP, is a burst of electromagnetic energy produced by a nuclear explosion that could cause widespread damage to surrounding electronic devices. In January 2024, the Innovation and Catastrophic Risk team released a primer breaking down the impact that electromagnetic interference—specifically electromagnetic pulses and associated radiation, generated by a nuclear detonation—could have on electric grids, electronics, satellites, radio and cellular, and wired communications.



EFFECTS OF ELECTROMAGNETIC PULSES ON COMMUNICATION INFRASTRUCTURE

AN IST PRIMER

JANUARY 2024

IST Institute for SECURITY + TECHNOLOGY

In November 2024, CATALINK hosted "Strengthening Nuclear Crisis Communications: Steps to Implement Mesh Networks to Enhance Resilience & Security" in Washington, DC. The team subsequently published an after action report to share key takeaways from the discussion.

CULTIVATING COLLABORATIVE NETWORKS

In September, IST Senior Director for International Cyber Engagement Elizabeth Vish and Future for Digital Security Associate Gigi Flores Bustamante attended the first convening of Brazil's Ransomware Task Force, co-organized by the Ministry of Foreign Affairs of Brazil, the Organization of American States Inter-American Committee against Terrorism (CICTE) Cybersecurity Section, and IST. "This initiative brings together public and private sector stakeholders to develop strategies that reduce ransomware risks and build resilience across Brazil's critical sectors," Gigi wrote.

At TrustCon 2024, IST SVP for Special Projects Eric Davis moderated a panel to discuss AI's impact on 2024 elections with experts from the Tech Global Institute, All Tech is Human, and Boston University. "As we navigate through this pivotal year of elections — with more than half of the world's population expected to vote by the end of 2024 — the role of AI technologies, particularly generative AI (GenAI), has become a focal point," Eric wrote.

In September, IST attended the 2024 International Counter Ransomware Initiative (CRI), the fourth annual gathering of over 70 member states and entities, including the European Union, the Organization for American States, and INTERPOL, to bolster collective resilience to ransomware. IST was honored to participate in the CRI Summit as a member of the newly-launched Public-Private Sector Advisory Panel, to convene a panel discussion for member states on information sharing in the ransomware payment ecosystem, and to co-host with the Center for Cybersecurity Policy and Law a day of industry dialogue on the sidelines.

In February, IST's Strategic Balancing Initiative convened public and private sector stakeholders in Washington, DC for a series of discussions on overcoming misalignments in the emerging technology development ecosystem to accelerate American and likeminded nations' economic competitiveness and national security strength in the face of a systemic and well-coordinated approach by the PRC to lead in critical and emerging technologies.

In March 2024, the IST team gathered for an offsite in California to share insights, collaborate across projects, and focus on strategic goals.

IN 2024, WE...

CREATED COMMON UNDERSTANDING, BRINGING BESPOKE APPROACHES TO EACH INDIVIDUAL PROBLEM SET.

No two challenges are alike; whereas one may be better suited to targeted government action, another may necessitate community-wide campaigns and engagement. In 2024, IST leveraged novel approaches across our project portfolio to tackle a unique set of challenges, whether the lack of technical and policy risk mitigations incorporated into AI development and deployment; the effects of social GenAI on cognition, society, and the future; or the threat to our lifeline critical infrastructure posed by nation-state actors, accidents, and adversaries.

AI RISK REDUCTION INITIATIVE

Developing a risk-oriented framework for AI labs, AI deployers, policymakers, and regulators

AS AI FOUNDATION MODELS CONTINUE TO PERMEATE OUR DAILY LIVES, WHAT ARE THE RISKS AND OPPORTUNITIES ASSOCIATED WITH THEIR DEVELOPMENT AND DEPLOYMENT?

In 2024, the AI Risk Reduction Initiative took a technical and policy-oriented approach to this question, aiming to provide a risk mitigation framework for AI developers, deployers, and users. The initiative oriented its efforts around six specific risks posed by the development and proliferation of AI technologies, as identified by an IST working group in 2023:

1. **Fueling a race to the bottom**
2. **Malicious use**
3. **Capability overhang**
4. **Compliance failure**
5. **Taking the human out of the loop**
6. **Reinforcing bias**

Following the release of our findings, we gathered key stakeholders from government, civil society, and industry to invite their feedback on the recommendations, thoughts about the predictions, and input on future work needed to explore the implications of AI in cybersecurity. Ultimately, IST's efforts helped to catalyze the conversation around the implications of AI for cybersecurity, and drove industry and policy efforts to adapt to the changing landscape.

In 2024, the AI Risk Reduction Initiative began to take on each of these risks in turn, starting with malicious use and compliance failure. In the case of the risk of malicious use, the Initiative worked with researchers, members of leading AI labs, and policy experts to propose policy and technical recommendations across each stage of the AI lifecycle, focusing on technical interventions like data validation and sanitation, privacy-preserving AI techniques, red teaming, and anomaly detection. On the policy side, interventions included dataset sourcing transparency, robust security standards, legal protections and reward programs for whistleblowers, and regular security audits and penetration testing. When it came to the risk of compliance failure, the AI Risk Reduction team took a different approach, examining past compliance failures across other industries to draw conclusions for the AI ecosystem. In coordination with an expert group of working group members and other contributors, the Initiative focused on the specific, immediately actionable policy and technical interventions that could be taken to reduce the risk of institutional-, procedural-, and performance-based compliance failures.

Success Story: In November 2024, Anthropic published their Voluntary Commitment Tracker—a document outlining key processes, programs, and practices for responsible AI development and highlighting progress on voluntary commitments. According to an Anthropic representative, the transparency efforts behind the tracker were partially inspired by IST's ongoing work on AI compliance.

In the news: Deputy Director for Artificial Intelligence Security Policy Mariami Tkeshelashvili joined the SAIS Review of International Affairs' Looking Glass Podcast to discuss her work on AI compliance and offer her takes on AI best practices, norms, and principles to avoid future risks. "We really want to see adaptable and continuous oversight," she said.

AI RISK MITIGATION IN ACTION:

Sample Technical Risk Mitigation Strategies	Sample Policy Risk Mitigation Strategies
Data validation and sanitation	Dataset sourcing transparency
Privacy-preserving AI techniques	Robust security standards
Red teaming	Legal protections and reward programs for whistleblowers
Anomaly detection	Regular security audits and penetration testing
Model cards	Staff training
Threat model-informed design requirements	Education programs for end-users
Query rate limits	
Watermarking techniques	

THE GENERATIVE IDENTITY INITIATIVE

Forming a multidisciplinary research & policy agenda at the intersection of psychology, policy, and AI

Generative AI is moving at a rapid pace: we have limited time to anticipate both the risks and opportunities.

HOW CAN WE ENSURE THAT POLICY DECISIONS ABOUT GENAI ARE MADE IN A WAY THAT PRIORITIZES SOCIETAL WELL-BEING, STRENGTHENS PUBLIC TRUST, AND ENSURES THAT THE BENEFITS OF THESE INNOVATIONS ARE WIDELY AND EQUITABLY SHARED?

In response to this question, IST's Generative Identity Initiative (GII) convened 26 experts in a series of interactive working group meetings over the course of 2024–building on work that IST began in 2019 to explore future digital threats to democracy and continued in 2022 that unpacked how digital technologies would impact cognition and democracy. Experts represented a wide cross-section of the voices needed to ensure that GenAI works for all of us: a pediatric physician; AI researchers; professors of bioethics, social sciences, and psychology; representatives from global organizations like USAID, IREX, and the National Endowment for Democracy; and experts in public policy and legal questions around GenAI. Rather than presenting the group with a series of pre-established goals and research questions from the outset, GII took an iterative approach, asking the experts to identify precisely which tough problems required multidisciplinary solutions. They identified a set of four:

1. **Challenges in Metacognition**
2. **The Confusion of Social and Interpersonal Trust**
3. **Modulating the Traditional Socialization Process**
4. **"Curated for you" vs. "Created for you"**

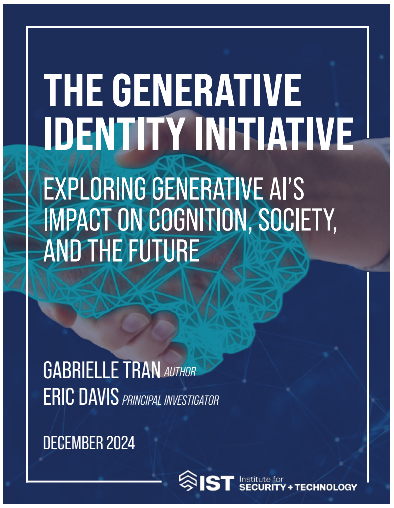
Over subsequent meetings, the group expanded on these themes, developing insights and actionable strategies to address the multifaceted implications of GenAI on society. In a final report, the GII team summarized the group's findings, putting forward recommendations for a policy agenda that government, industry leaders, and researchers can use to navigate the rapid advancement of generative technologies. The recommendations drew insights from other industries and challenges, a feature of the group's unique composition. For example, GII proposes a "Helpful, Honest, and Harmless" AI framework, originally used to inform and shape the development of AI systems, to address the challenges of social GenAI development. GII looks to other areas of Congressional action, like the Kids Online Safety Act, to map out a strategy for proposing legislation to regulate social GenAI. And GII uses gambling regulations worldwide as a starting point for thinking about practical social GenAI policies, including advertising warnings and restrictions; limits on engagement; policies around transparency; self-exclusion, "cooling off," and user feedback options; age restrictions; behavioral monitoring and intervention planning; and vulnerability screening.

26 experts participated in the Initiative

27 specific, actionable recommendations for a practical approach to GenAI

6 working group meetings allowed for collaboration and input

GenAI represents a profound evolution in tech that can affect and manipulate cognition, and outsource cognitive functions. The Generative Identity Initiative (GII)'s inaugural report asked the question: How will this emerging tech affect social cohesion? Author Gabrielle Tran and principal investigator Eric Davis lay out the ways GenAI might impact social cohesion and present a comprehensive research agenda, noting 27 areas of exploration for addressing these challenges.



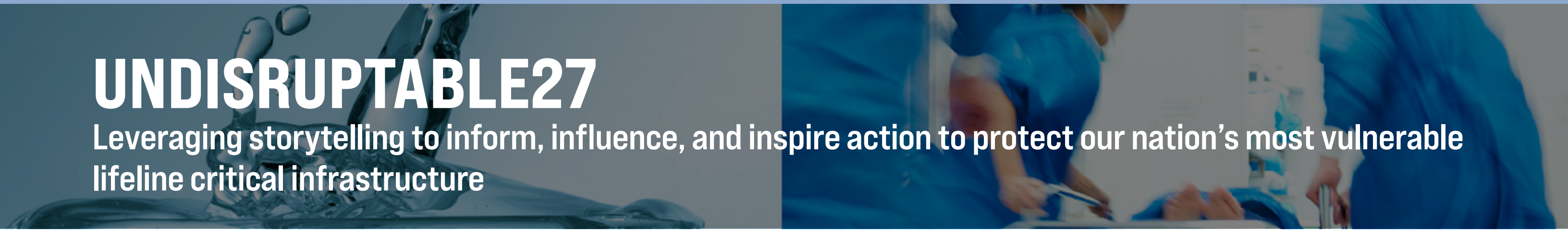
THE GENERATIVE IDENTITY INITIATIVE

EXPLORING GENERATIVE AI'S IMPACT ON COGNITION, SOCIETY, AND THE FUTURE

GABRIELLE TRAN *AUTHOR*
ERIC DAVIS *PRINCIPAL INVESTIGATOR*

DECEMBER 2024

IST Institute for SECURITY + TECHNOLOGY



UNDISRUPTABLE27

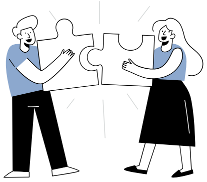
Leveraging storytelling to inform, influence, and inspire action to protect our nation's most vulnerable lifeline critical infrastructure

We are too dependent on undependable things. The water we drink, the hospitals we rely on for emergency medical care, the food we put on our tables, and the power we use to light our homes are subject to escalating harms by accidents, bad actors, and nation-state adversaries.

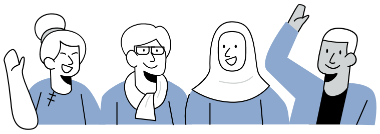
UnDisruptable27, led by Executive in Residence Joshua Corman, launched at IST in August 2024 with foundational support from Craig Newmark Philanthropies. In order to prevent these unnatural disasters–whether food shortages, water disruptions, delays in lifesaving care, or power outages–the effort takes inspiration from how we prepare our communities for natural disaster:

UnDisruptable27 focuses on the creative, storytelling strategies needed to achieve these three goals. Confronted with a massively multidisciplinary challenge and a wide-ranging group of essential collaborators, the initiative spent its first few months identifying, engaging, and building trust with key stakeholders. This early community-building phase included outreach to formal public-private partnerships, relevant trade associations, asset owners and operators in water and emergency medical care, and relevant national labs. In all cases, the effort used empathy and fit-for-purpose narratives tailored to meet stakeholders where they are.

1. **INFORM:**
What do our communities need to know?



2. **INFLUENCE:**
What are the well-prioritized, well-vetted actions that we should take accordingly?



3. **INSPIRE:**
How can we encourage and motivate a whole-of-society approach?

TECHNOLOGIST TALKS: A NEW IST PODCAST

In 2024, we launched TechnologIST Talks, dedicated to bringing conversations on the technological advancements threatening global security and stability to the forefront. In the first season, we zeroed in on the race to accelerate innovation in technologies of national strategic importance.

TECHNOLOGIST talks
THE STRATEGIC EDGE IN TECHNO-INDUSTRIAL COMPETITION EPISODE 1
Why Venture Capital Is Indispensable for U.S. Industrial Strategy
Michael Brown & Pavneet Singh
Senior Fellows, IST
an Institute for SECURITY + TECHNOLOGY podcast

In the first episode, Senior Adjunct Advisors Michael Brown and Pavneet Singh joined host Philip Reiner for a conversation on their plan for harnessing the power of venture capital.

TECHNOLOGIST talks
THE STRATEGIC EDGE IN TECHNO-INDUSTRIAL COMPETITION EPISODE 4
The Cleantech Boom
Alex Gagnon
Co-Founder and CEO, Banyu Carbon
an Institute for SECURITY + TECHNOLOGY podcast

Host Steve Kelly sat down with Banyu Carbon co-founder and CEO Dr. Alex Gagnon to explore the emerging field of carbon dioxide removal and its role in decarbonizing the economy.

TECHNOLOGIST talks
THE STRATEGIC EDGE IN TECHNO-INDUSTRIAL COMPETITION EPISODE 6
A Transatlantic Perspective on Quantum Tech
Markus Pflitsch
CEO and Founder, Terra Quantum AG
an Institute for SECURITY + TECHNOLOGY podcast

Host Megan Stifel spoke with Markus Pflitsch, founder and CEO of Terra Quantum, to explore how Chinese technological approaches to quantum differ from that of Europe and the West.

TECHNOLOGIST talks
THE STRATEGIC EDGE IN TECHNO-INDUSTRIAL COMPETITION EPISODE 2
The Deep Tech Renaissance
Manish Kothari
Founding Managing Partner, First Spark Ventures
an Institute for SECURITY + TECHNOLOGY podcast

Philip Reiner sat down with Dr. Manish Kothari to discuss the current "renaissance" in deep tech, the unique funding environment at play, and how to further galvanize the industry.

On April 24, 2024, IST hosted “24 in 24,” an all-day event to assess the status of the Ransomware Task Force’s 48 recommendations and zero in on the 24 that had seen little to no progress.

IN 2024, WE...

ACTIVATED INSIGHTS WITH ACTION, ISSUING PRACTICAL RECOMMENDATIONS, TRACKING THEIR PROGRESS, AND AIDING WITH IMPLEMENTATION.

In 2024, we did not just theorize; we took action. As a result, IST issued a total of 95 practical recommendations across all of our projects calling for governments, industry, and civil society to take action.

RANSOMWARE TASK FORCE:
“Doubling Down” in its fourth year of action

For the Ransomware Task Force—one of IST’s standout initiatives—achieving impact is not only about updating and iterating on policy recommendations, but also about tracking their progress and in many cases guiding their implementation.

To mark the fourth anniversary of the task force’s establishment, IST in April 2024 published Doubling Down, a progress report that assessed the level to which the U.S. government and its partners had successfully followed through on the 48 recommendations put forward in the original task force report. In concert with the progress report, IST also hosted “24 in 24,” an all-day event that took a pillar-by-pillar approach to the 24 recommendations.

To help continually assess the state of the ransomware threat to individuals, businesses, governments, and society, the RTF also authored its third annual Global Incident Map, which analyzed ransomware incidents occurring in 117 countries and carried out by 66 ransomware groups. The analysis found a 73% year-over-year increase in ransomware attacks and identified sector-specific trends to guide future RTF efforts.

In 2024, the RTF also focused on ensuring that some of the communities most affected by ransomware—including everyday citizens, small- and medium-sized businesses with fewer resources to dedicate to cyber threats, and governments and entities worldwide—have the resources they need to defend themselves. To reach everyday citizens, the RTF launched campaigns on social media and supported efforts like Cyber Civil Defense and the Take9 initiative. For small- and medium-sized businesses, the RTF published a “quick start” guide to help them choose and implement the most effective safeguards against cyber threats. And to provide resources to a global audience, the RTF published the Blueprint for Ransomware Defense in Portuguese, in addition to the English and Spanish editions.

One example of the RTF’s role in guiding implementation of recommendations is its work on public-private partnerships. In collaboration with the Global Forum on Cyber Expertise and in partnership with the International Counter Ransomware Initiative (CRI), the RTF examined three existing partnerships to identify the keys to success, outline the challenges they faced, and ultimately help others replicate these successes. Establishing more effective public-private partnerships was a key component of the RTF’s initial recommendations; this research, published in March 2024, helped to pinpoint exactly how to do so. In October 2024, IST was named a member of the newly-launched Public-Private Sector Advisory Panel of the CRI. During the fourth annual gathering, we met with governments worldwide to share actionable insights and guidance gathered from our research.

Success Story: In November 2022, the RTF published a Cyber Incident Reporting Framework in collaboration with the Cyber Threat Alliance and other major organizations; in March 2023, they published a follow-on edition that focused on aligning global reporting efforts. In March 2024, the U.S. Department of Homeland Security and the European Commission’s Directorate General for Communications, Networks, Content, and Technology (DG Connect) announced an initiative to compare cyber incident reporting and better align approaches. And in July 2024, IST and the Cyber Threat Alliance submitted comments to CISA on the implementation of the Cyber Incident Reporting for Critical Infrastructure Act.

IST Institute for SECURITY + TECHNOLOGY CYBER THREAT ALLIANCE

CYBER INCIDENT REPORTING FRAMEWORK

Cyber Threat Alliance, Institute for Security and Technology, CREST, CipherTrace, Coveware, Cybera, Cybercrime Support Network, CyberPeace Institute, Open Cybersecurity Alliance, and SolarWinds

NOVEMBER 2022

IST Institute for SECURITY + TECHNOLOGY CYBER THREAT ALLIANCE

CYBER INCIDENT REPORTING FRAMEWORK: GLOBAL EDITION

Cyber Threat Alliance, Institute for Security and Technology, Chainalysis, Ciphertrace, CREST, Cybera, Cybercrime Support Network, CyberPeace Institute

MARCH 2023

National Impact: On April 16, 2024, Chief Strategy Officer and RTF Executive Director Megan Stifel testified before the House Committee on Financial Services Subcommittee on National Security, Illicit Finance, and International Financial Institutions for a hearing entitled, “Held for Ransom: How Ransomware Endangers Our Financial System.” In her testimony, she focused on three specific ways to reduce the risk and impacts of ransomware on the financial services sector, including building resilience against ransomware; allocating local, state, and federal resources to support this resilience; and leveraging the reach of the financial services sector to raise collective digital resilience.

STRATEGIC BALANCING INITIATIVE:

From problem → solution → implementation → community engagement

HOW CAN LEADERS IN WASHINGTON, DC AND SILICON VALLEY WORK TOGETHER TO IDENTIFY PRACTICAL WAYS TO ACCELERATE U.S. TECHNOLOGICAL COMPETITIVENESS AND ALLEVIATE THESE MISALIGNMENTS BETWEEN THE PUBLIC AND PRIVATE SECTORS?

The United States increasingly finds itself engaged in a technological competition with China and the global technology ecosystem. As technological strength plays a growing role in national security, incentives in the private sector are not necessarily aligned with national security interests in the public sector.

The Strategic Balancing Initiative in 2024 focused its efforts on quantum, biotech, and energy in the United States: three sectors that face increasing global competition, but see misalignments between the public and private sectors that can stifle their competitiveness on the world stage. For each sector, the SBI team, in partnership with investors, government representatives, and members of companies in each sector, identified the misalignments that exist and the factors that lead to each; explored initial solution sets; and proposed specific solutions, considering the mechanisms for implementation.

Across each of the three sectors, the SBI team identified a common thread: investors in the United States have become less inclined to invest in hardware-based or capital-intensive projects–many of which are essential for success in quantum, biotech, energy, and other technologies that bolster U.S. technological competitiveness. In response, the SBI team released Why Venture Capital Is Indispensable for U.S. Industrial Strategy, a capstone report that calls for the government to prioritize promising federal research for commercial development; establish a program to cultivate entrepreneurial founding teams; promote transparency in the federal total addressable market; encourage demonstration of technology maturity; and develop a public capital framework.

To translate these recommendations to a broader audience–and continue to follow through on the work of the Initiative–IST launched in 2024 a podcast series focused on the strategic edge in techno-industrial competition. The podcast featured conversations with deep tech entrepreneurs, materials scientists, energy founders, and quantum leaders.

	STAGE 1 – Identifying Existing Problems	**STAGE 2 –** Exploring initial solution sets	**STAGE 3 –** Proposing specific solutions with tangible mechanisms for implementation
BIOTECH	- Data is paramount - Unintended legislative consequences - Complexity of supply chains - Balancing innovation with protection	**Data repository:** A federal government-driven repository to manage biotech data that provides fee-based access to researchers for identification and usage.	*[Executive Branch]* **Solution:** U.S. government to establish an executive office entity to plan the repository, considering how to incentivize participation; the scope, scale, and format; uses; and enforcement.
ENERGY	- Availability of infrastructure - Political uncertainty - Innovation ecosystem - Grants and contracts	**National policy to stimulate demand:** Demand-side mandates to drive incentives in the energy ecosystem, such as a national quota that could provide a market signal to investors and the financial ecosystem.	*[Legislative Branch]* **Solution:** A narrow mandate to increase subsidies for bio-related fuel production, attached to a must-pass bill as an amendment.
QUANTUM	- Access to financing - Differences and definitions - Availability of infrastructure - Evolving & complex extant innovation programs and government mechanisms	**Quantum ecosystem mapping:** A holistic view of the different technologies and applications possible with quantum technology and the dependencies that exist in input materials, infrastructure, downstream partnerships, or use-cases.	*[Industry and Analysis Unit at the Department of Commerce or Legislative Branch]* **Solution:** Commerce to lead the supply chain mapping and industry engagement necessary to create a map of the quantum ecosystem.

IST in the News

Bank Info Security

Ransomware Experts See Problems With Banning Ransom Payments

Mathew Schwartz, February 19, 2024

CNN

ATT Leak Exposes Info of 73M Current & Former Customers

Fredrika Whitfield, March 31, 2024

ReadMe_

CISA cyber reporting mandate faces tough road

Shaun Waterman, April 10, 2024

POLITICO

How Israel's cyber defenses fared during Iran strikes

Joseph Gedeon, April 15, 2024

The Hill

AI making ransomware easier, more prevalent, committee hears

Clayton Vickers, April 17, 2024

The Hill

The future of clean energy hinges on cybersecurity

Steve Kelly and Sarah Powazek,
April 23, 2024

Decipher

Ransomware Task Force: We need to disrupt operations at scale

Lindsey O'Donnell Welch, April 24, 2024

The Washington Post

Hack targeting hospital chain Ascension is impacting patient care

Daniel Gilbert, Joseph Menn, and Dan Diamond, May 9, 2024

BBC

Don't blame us for people suffering - London hospital hackers

Joe Tidy, June 19, 2024

The Wall Street Journal

Companies Sharply Criticize Draft U.S. Cyber Reporting Rules

James Rundle, July 11, 2024

NBC News

Release of Russian hackers believed to be first U.S. prisoner swap to include international cybercriminals

Kevin Collier, August 1, 2024

WIRED

A New Plan to Break the Cycle of Destructive Critical Infrastructure Hacks

Lily Hay Newman, August 6, 2024

The Record from Recorded Future

Ransomware incidents hit 117 countries in 2023, task force says

Jon Grieg, September 26, 2024

WIRED

Hacker Charged With Seeking to Kill Using Cyberattacks on Hospitals

Andy Greenberg, October 16, 2024

NPR

A TikTok sale under Trump? Experts say it could actually happen this time

Bobby Allyn, November 11, 2024

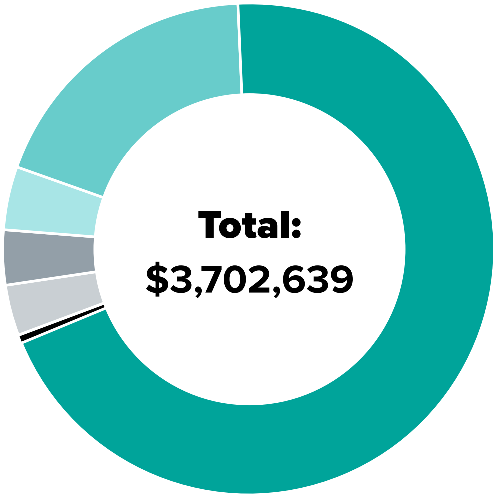
Forbes

Revitalizing the U.S. Innovation Ecosystem

Michael Brown, November 27, 2024

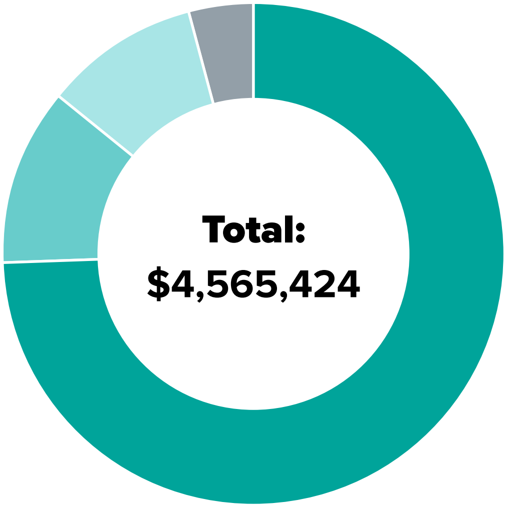
IST Financials

FY 2024 Revenue*



■ Contributions **68.8%**	$2,579,360
■ Grants and Contracts **18.4%**	$691,011
■ Investment Return **4.1%**	$153,798
■ Program Service Revenue **3.7%**	$140,209
■ Contributions In-Kind - Services **3.4%**	$128,530
■ Other Income **0.3%**	$9,731
Total	**$3,702,639**

FY 2024 Expenses



■ Program **74.5%**	$3,400,027
■ Administrative **11.6%**	$530,882
■ Fiscal Sponsorship **10%**	$455,000
■ Fundraising **3.9%**	$179,515
Total	**$4,565,424**

***Note:** IST received a significant contribution of $1 million in late-December 2023 for 2024 programming that is not accounted for in the numbers above, in line with Generally Accepted Accounting Principles (GAAP).