INSTITUTE FOR SECURITY AND TECHNOLOGY

ANNUAL REPORT 2023

Institute for SECURITY + TECHNOLOGY

2023 yet again confirmed the IST thesis: the world needs a critical action think tank to address the challenges of the 21st century. Indeed, 2023 saw an uptick in ransomware attacks, heightened fervor around the potential opportunities–and risks–associated with Artificial Intelligence (AI), new concerns surrounding the trustworthiness and safety of the platforms that permeate our everyday lives, and breakthroughs in quantum computing that have the power to transform everything from research and forecasting to encryption and even warfare.

In a year of unprecedented emerging security threats, IST rose to the challenge. Our expanding team of experts and advisors, new and existing projects, in-depth research, and bespoke convenings enabled us to tackle these threats and seize opportunities, bringing together technology and policy leaders to generate novel solutions and guiding them to implementation. We hosted an incredible 83 convenings this year with experts from across sectors and industries, asking them to engage in the tough questions and brainstorm possible solutions. We participated in 43 events worldwide, bringing our perspectives and expertise to a global audience. And we engaged in deep, meaningful work across eight projects, publishing seven reports and countless recommendations.

- The Ransomware Task Force (RTF) witnessed action on 92% of RTF recommendations with 50% having significant progress, including through legislation and policy adoption.
- We published a cornerstone report on How Does Access Impact Risk? through the newly-launched AI Foundation Model Access Initiative with the support of the Patrick J. McGovern Foundation.
- We were one of nine organizations to receive the first round of support from Google.org's Digital Futures Project, which seeks to encourage the responsible development of AI, engaging with academic and nonprofit institutions worldwide.

Zoë Brammer joined the SLEUTHCON cybercrime conference to present her mini-pilot that maps ransomware threat actor behavior atop the ransomware payment ecosystem map.

Philip Reiner headed to Singapore in October 2023 to present IST's map of the ransomware payment ecosystem at Interpol's Global Cybercrime Conference.

During Cybersecurity Awareness Month, Megan Stifel joined the launch of the CISA Secure Our World Initiative to discuss how nonprofits play a role in bolstering cybersecurity. | Credit: CISA

At the March 2023 State of the Net conference, Megan Stifel joined panelists across the cyber ecosystem to discuss the state of cybersecurity in the United States. | Credit: Glen Echo Group

In June 2023, Sylvia Mishra presented research on nuclear risk reduction and crisis communications at the Alva Myrdal Centre for Nuclear Disarmament in Sweden.

Elizabeth Vish moderated a panel at the Organization of American States' Cyber Symposium on how to prepare for, protect against, and recover from cyber attacks.

- In partnership with the Global Forum on Cyber Expertise (GFCE), we researched the keys to effective public-private cyber partnerships, an effort that garnered recognition at the International Counter Ransomware Initiative Summit at the White House.
- We launched a new initiative on social identity and generative AI with support from the Omidyar Network, following the 2022 Digital Cognition and Democracy Initiative (DCDI) project.
- The Strategic Balancing Initiative (SBI) hosted Energy, Quantum, and Biotech Working Groups, working with representatives from across the public and private sectors to identify misalignments affecting U.S. technology competitiveness and national security.
- The Applied Trust & Safety Initiative, with the support of the Patrick J. McGovern Foundation, engaged in a wide-ranging listening tour to better understand the challenges confronted by trust and safety practitioners and to inform future work.
- The CATALINK Initiative published a report following a Track 1.5 Dialogue in London and launched its Crisis Communications Resilience Working Group.

As we continue to lean into our unique ability to drive impact, we will create even more collaborative spaces and policy successes in the year to come. We thank you all for your donations, dedication, and partnership. We could not do this without your support. As we work toward ensuring a more secure technological future, get engaged, stay safe, and stay healthy from all of us at IST.

Philip Reiner

Philip Reiner
Chief Executive Officer

Michael McNerney
Board Chair

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 tackling some of the world's toughest emerging security threats. Thank you to the following partners, in-kind supporters, and individuals and private philanthropists who contributed to our efforts in 2023. We also extend our thanks to a number of donors who chose to remain anonymous.

aws

Santander

BANK OF AMERICA

COMMUNITY FOUNDATION SANTA CRUZ COUNTY

Craig Newmark Philanthropies

German Federal Foreign Office

GFCE

Google Community Grants Fund

WILLIAM + FLORA Hewlett Foundation

JCF JEWISH COMMUNITY FEDERATION & ENDOWMENT FUND

Kingdom of Spain Ministry of the Interior and Ministry of Foreign Affairs, European Union and Cooperation

Meta

Metaculus

Microsoft

OMIDYAR NETWORK

paloalto NETWORKS

Patrick J McGovern FOUNDATION

Private philanthropy

Smith Richardson Foundation

Swiss Federal Department of Foreign Affairs

DONOR SPOTLIGHT

William and Flora Hewlett Foundation

IST has been a proud member of the William and Flora Hewlett Foundation Cyber Initiative, a landmark effort to cultivate the growing field of cyber institutions and expertise, since IST's inception. As the Cyber Initiative came to a close in 2023, IST extends its gratitude to the program for playing an instrumental role in the development of our portfolio of work within the Future of Digital Security focus area.

"Over the last 5 years, the Hewlett Foundation's Cyber Initiative has proudly supported IST. It has been a pleasure to witness the tremendous success of the Ransomware Task Force, sustainable growth of IST's cyber program, and IST's impact across the technology and security ecosystem. IST fills an important gap in the ecosystem by bridging the divide between those driving technological advancement and those crafting policies and regulation to manage the risks these new technologies invite."

— Sherry Huang
Special Projects Fellow and Advisor to the President on AI, William and Flora Hewlett Foundation

Craig Newmark Philanthropies

In 2023, Craig Newmark joined us in Washington, DC at the annual Ransomware Task Force convening, participating in a panel on his continued efforts to champion cyber civil defense. While at the event, he announced funding from Craig Newmark Philanthropies for 2023, supporting our work in the areas of counter-ransomware, the Ransomware Task Force, and information security policy.

"I'm on a mission to keep everyone safe. IST is a big part of that goal; through their important work to counter ransomware and support the most vulnerable in the ecosystem, they are doing what's needed to protect our neighbors and communities."

— Craig Newmark
Founder, Craig Newmark Philanthropies

Patrick J. McGovern Foundation

Artificial Intelligence technologies are advancing and proliferating at an astounding pace, creating new opportunities that can benefit and, if left unchecked, damage human societies. As IST continues to study the risks and opportunities associated with degrees of access to AI through our AI Model Access Initiative, we are thrilled to partner with the Patrick J. McGovern Foundation (PJMF).

"To ensure that researchers and technologists design cutting-edge AI in a way that promotes human dignity, private companies, academia, and civil society must also build a common understanding of risk. IST's Foundation Model Access Initiative has already made important contributions to this effort, and we hope it will serve as a model for the type of constructive, human-centered dialogue that we believe is required for technology to truly be built for everyone."

— Nick Cain
Director of Strategic Grants, Patrick J. McGovern Foundation

StatISTics: Reach and Impact

83 convenings

across all of our projects brought together representatives from across government, industry, and civil society, whether in a large-scale task force, working group meeting, or workshop.

27 blog posts by IST experts

Top blogs by viewership:

1. 2022 RTF Global Ransomware Incident Map
2. Catalyzing Security in AI Governance
3. Putting the Blueprint for Ransomware Defense to the Test
4. IST Launches New Crisis Communications Resilience Working Group
5. To Trinity Test Site: Reconciling with the Past, Taking Action for the Future

49,343 unique active users

visited securityandtechnology.org, reaching 88,000 total pageviews.

150 media hits

highlighted IST experts and outcomes in national and international news.

3,847 subscribers

receive The TechnologIST in their inboxes monthly since launch in February 2023.

7 capstone reports

captured research, analysis, actionable recommendations, and next steps for projects such as Open-Source Software Security and AI Foundation Model Access.

4 confidence-building measure categories

proposed in the February report AI-NC3 Integration in an Adversarial Context: Strategic Stability Risks and Confidence Building Measures.

1. Renouncing the use of AI technologies in certain weapon and military systems
2. Agreeing on standards, guidelines, and norms related to AI trust and safety
3. Increasing the quantity or quality of lines of communication
4. Providing education and training for policymakers, decision makers, and diplomats

6 categories of risk x 7 levels of access

mapped on a matrix in the December 2023 report How Does Access Impact Risk? Assessing AI Foundation Model Risk Along a Gradient of Access.

IST in the News

The Nuclear Risk Reduction Approach: A Useful Path Forward for Crisis Mitigation
Sylvia Mishra, January 27, 2023

Cybersecurity and Compliance in the Age of AI
Zoë Brammer and Katherine Schmidt, September 14, 2023

The United States and China Still Need to Talk About Nuclear Weapons
Sahil Shah, February 6, 2023

New wave of scams coming and world is unprepared, warns former Obama adviser
David Sun and Christine Tan, October 17, 2023

In his new cybersecurity strategy, Biden identifies cloud security as a major threat
Steve Inskeep, April 4, 2023

Ransomware Soars as Myriad Efforts to Stop It Fall Short
Andrew Martin, October 25, 2023

Institute for Security and Technology calls for shared responsibility model to secure open source software
Sara Friedman, April 19, 2023

Latest hospital cyberattack shows health care systems' vulnerability
Nicole Sganga, November 29, 2023

Ransomware Task Force: Data Sharing Needed to 'Build a Clear Picture'
Lindsey O'Donnell Welch, May 5, 2023

Open access to AI foundational models poses various security and compliance risks, report finds
Caroline Nihill, December 13, 2023

Influential task force takes stock of progress against ransomware
Tim Starks, May 5, 2023

Why extortion is the new ransomware threat
Carly Page, December 18, 2023

Google pledges $20 million for responsible AI fund
Ina Fried, September 11, 2023

Tech security group examines risks from increased access to AI foundation models
Charlie Mitchell, December 20, 2023

IST Goes Global

WASHINGTON, DC

During the Diplomacy and Capacity Building Pillar session of the White House-convened Counter Ransomware Initiative Summit, Elizabeth Vish presented preliminary findings from research in partnership with Global Forum on Cyber Expertise that examines case studies of public-private collaboration to combat ransomware. The presentation earned IST a mention in the statement released following the Summit.

Megan Stifel joined CISA for the launch of the Secure Our World campaign. Speaking on the role of nonprofits in cybersecurity, she said, "I think of us...as key partners, not only for industry but also for governments."

NASSAU, BAHAMAS

Elizabeth Vish moderated a panel at the Organization of American States Cybersecurity Symposium, a gathering of cybersecurity experts and government representatives from across the Americas to share information and raise awareness about the state of cybersecurity in the region.

BATAVIA, IL

The Strategic Balancing Initiative team attended the Superconducting Quantum Materials and Systems Center's Ecosystem Day at Fermi National Accelerator Laboratory to better understand the state of innovation in the quantum sector.

WHITE SANDS NATIONAL PARK, NM

On the 78th anniversary of the detonation of the world's first atomic bomb, Sylvia Mishra had the chance to visit the Trinity Test Site, where she reflected on the history of the atomic age.

SAN JOSÉ, COSTA RICA

Zoë Brammer and Elizabeth Vish joined senior government officials, C-suite members, and cyber and legal experts from across Latin America for the Duke University Cybersecurity Leadership Program. They presented to attendees on the Ransomware Task Force's lines of effort, including the Blueprint for Ransomware Defense, best practices for cyber incident reporting, and the ransomware payment ecosystem.

SAN FRANCISCO, CA

Following IST's new partnership with the World Economic Forum's AI Governance Alliance, Steve Kelly attended the WEF AI Governance Summit, joined by 200+ Alliance community members, AI experts, and leaders across the field in discussing issues of safety, access, and ethics in AI systems.

ACCRA, GHANA

Elizabeth Vish moderated a panel on how to ensure that developing countries do not get left behind in cybersecurity developments at the Global Forum for Cyber Expertise's annual Global Conference on Cyber Capacity Building.

LONDON, UNITED KINGDOM

Nile Johnson participated in the Marketplace Risk Global Summit as a panelist on "Measuring the Efficacy of Trust & Safety Programs," a discussion of the impact of policy work on trust and safety.

THE HAGUE, THE NETHERLANDS

Alexa Wehsener spoke at the Swiss Ministry of Foreign Affairs and Stockholm International Peace Research Institute (SIPRI) breakout session, "Responsible Adoption of AI in the Nuclear Domain," at the first summit for Responsible Use of AI in the Military Domain (REAIM), hosted by the Netherlands Ministry of Foreign Affairs. REAIM 2023 created space to discuss global perspectives on how AI can and will affect the battlefield and strategic incentives.

Zoë Brammer traveled to The Hague for the Europol EC3 Cybercrime Conference, a multistakeholder gathering focused on the global fight against cybercrime, including ransomware mitigation, digital investigations, and the impact of AI. She presented her map of the ransomware payment ecosystem, breaking down the actors, processes, and information involved in the ransom payment process and providing insight into the relevance of the map in combating financially-motivated cybercrime.

SINGAPORE

Philip Reiner headed to Singapore to attend Singapore International Cyber Week, an annual conference that brings together international leaders from across government, the private sector, and academia to discuss the evolving cyber threat landscape in a high-level panel. On the sidelines of the event, Reiner spoke with The Straits Times on the rising threat of cybercrime worldwide. He also joined INTERPOL's inaugural Global Cybercrime Conference, where he presented IST's map of the ransomware payment ecosystem in a closed-door presentation.

HANOI, VIETNAM

At a workshop hosted by the British American Security Information Council and the Institute for Conflict, Cooperation and Security for Nuclear Responsibilities and Nuclear Crises in Southern Asia, Philip Reiner discussed the CATALINK project in the South Asian context of crisis communications, building off of BASIC and ICCS's work through the lens of their framework for shared nuclear responsibilities.

Spotlight on the Ransomware Task Force

2023 marked two years since the release of the Ransomware Task Force's foundational report, Combating Ransomware, with 48 recommendations for government, industry, and civil society designed to deter and disrupt the ransomware model and help organizations prepare for and respond to attacks at scale.

> "The Institute for Security and Technology's influential Ransomware Task Force released a progress report this month that was altogether heartening: Not only have 92 percent of the group's recommendations "seen some action" but also the usual suspects are laying off the usual targets."
>
> — The Washington Post Editorial Board
> "To keep fighting ransomware, the United States needs more information," May 15, 2023

The April 2023 RTF Progress Report noted significant progress against the threat, concluding that 50% of the recommendations had seen significant action, including through public-private and government-to-government collaboration on disruptive activity, increasing focus on reporting and information sharing, and ongoing efforts to reduce some of the risks posed by cryptocurrency.

Over the course of 2023, governments achieved remarkable progress in alignment with RTF recommendations, including operational collaboration leading to the takedown of major ransomware actors like ChipMixer and the botnet Qakbot, the arrest of a cryptocurrency exchange founder, joint U.S.-UK sanctions against members of a prominent Russian cybercrime group, and clear commitments from U.S. and worldwide governments to continue to prioritize counter-ransomware efforts, to name a few.

> "I am so grateful for the insights, advice, and great ideas that have come out of IST...including meeting with the NSC as we work to catalyze the U.S. government's unified approach to countering ransomware... The conversations IST has put together today are really at the heart of some of the most difficult ongoing policy discussions that we're grappling with in the Counter Ransomware Initiative."
>
> — Anne Neuberger, Deputy National Security Advisor for Cyber and Emerging Technology
> Remarks at Gaining Ground, Ransomware Task Force Anniversary Event, May 5, 2023

To reflect on progress and anticipate future action, the Ransomware Task Force in April 2023 gathered key members of government, industry, and civil society at a large-scale anniversary event. Gaining Ground: Two Years of Implementation and Impact featured keynote remarks from Deputy National Security Advisor Anne Neuberger and U.S.

"IST's Ransomware Task Force is one of the most successful non-government-led cyber initiatives we've seen."

— Charley Snyder
Head of Security Policy, Google

Representative Elissa Slotkin, a fireside chat with IST's Megan Stifel and then-Acting National Cyber Director Kemba Walden, and a series of in-depth panels on operational collaboration, the shifting cyber insurance market, the Cyber Civil Defense initiative, global counter-ransomware collaboration, and ransomware implications of the Russian invasion of Ukraine.

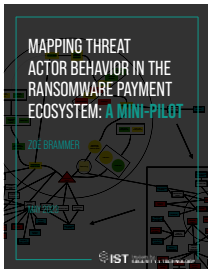
The RTF's work does not stop at simply reflecting on progress achieved; in 2023 the Ransomware Task Force team, together with RTF Working Groups, mapped threat actor behavior in the ransomware payment ecosystem, produced a global cyber incident reporting framework harmonized with existing global regulations, among other research and analysis, and led behind-the-scenes efforts to inform Congress and government about better, more effective regulation to combat ransomware.

"The Institute for Security and Technology's inaugural report on ransomware came out one month before the May 2021 attack on Colonial Pipeline, which turned computer-borne blackmail into the stuff of dinner table conversation. Since then, IST's work has become a lodestar for federal ransomware policy, with 92 percent of the think tank's recommendations seeing "some degree of action" since its release."

— John Sakellariadis, POLITICO reporter
"Ransomware Check In," Morning Cybersecurity Newsletter, May 5, 2023

RTF PUBLICATIONS: 2023

MAY 2023 | Mapping Threat Actor Behavior in the Ransomware Payment Ecosystem: A Mini-Pilot

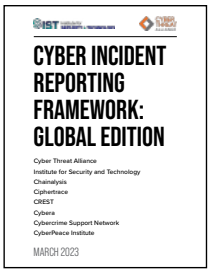


Taking four threat actor case studies, this mini-pilot overlays threat actor behavior atop the original, theoretical map of the ransomware payment ecosystem and identifies the tools, services, and entities that they leveraged as they prepared for and carried out attacks. Ultimately, the mini pilot seeks to identify which kinds of disruption could be most effective and where to apply friction in the payment process.

AUGUST 2023 | Putting the Blueprint for Ransomware Defense to the Test

This study maps claims data from Resilience to the Blueprint Safeguards and determines whether or not, if implemented properly, the Blueprint could have prevented an attack. It finds that at least 68% of attacks in this data set could have been prevented.

MARCH 2023 | Cyber Incident Reporting Framework: Global Edition



In Fall 2022, multiple industry groups, led by Cyber Threat Alliance and IST, developed a model framework that CISA could use for incident reporting. This edition makes the original CIRF accessible and applicable for a global audience, answering questions about what conditions should be in place to make a reporting mandate effective and harmonizing suggested definitions with existing global regulations.

OCTOBER 2023 | 2022 Global Incident Reporting Map

This effort uses data from ecrime.ch to map incidents worldwide in 2022, focusing on the shifting dynamics of ransomware groups, increased targeting of the education sector, and attacks on under-researched–and often under-resourced–entities.

IST's Efforts in an Age of AI

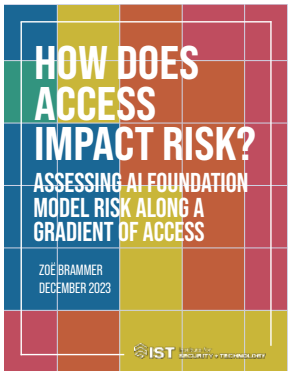
At IST, we have been observing recent developments in the AI ecosystem with interest; conversations around AI and governance align with our own mission to harness opportunities enabled by emerging technologies while also mitigating their attendant risks. 2023 saw the launch of new initiatives centered around AI, as well as continued work on the risks of integrating AI into nuclear command, control, and communication systems.

AI FOUNDATION MODEL ACCESS INITIATIVE

In 2023, IST began the AI Foundation Model Access Initiative, an effort to study ways in which increased access to cutting-edge AI foundation models—across a gradient of access from fully closed to fully open—drives risk and enables opportunity. Over the course of a six-month sprint, the effort brought together AI developers, researchers, and practitioners in a closed-door working group; conducted a survey with representatives of leading AI labs; and interviewed experts to address the question: How does access to foundation models and their components impact the risk they pose to individuals, groups, and society? In December 2023, the Initiative released *How Does Access Impact Risk?*, a study that presents the results of the Initiative's initial efforts. Now, work continues in 2024 to provide policymakers and regulators with risk mitigation strategies.

> "The working group's conclusions point to the need for clear technical mechanisms and policy interventions to maintain continued AI benefits while ensuring these new capabilities do not cause harm. This report lays important groundwork to inform the global debate on foundation model openness and responsible release."
>
> – Steve Kelly
> Chief Trust Officer, IST

DECEMBER 2023 | How Does Access Impact Risk?



As a number of leading AI labs release advanced AI systems, some models remain highly restricted, limiting who can access the model and its components, others provide fully open access to their model weights and architecture. To understand the risks that can arise as access to these models increases, this report develops a matrix to map categories of risk against a gradient of access to AI foundation models. It concludes that uninhibited access to powerful AI models and their components significantly increases the risk these models pose across a range of categories, as well as the ability for malicious actors to abuse AI capabilities and cause harm. At the highest levels of access, the risk of a "race to the bottom"–a situation in which conditions in an increasingly crowded field of cutting-edge AI models might incentivize developers and leading labs to cut corners in model development–increases when assuming a "winner takes all" dynamic.

APPLIED TRUST & SAFETY INITIATIVE

IST in 2023 launched the Applied Trust & Safety (AT&S) Initiative, a long-term effort to ensure technology products and services are safe to use and capabilities such as AI are fully leveraged to address these challenges at scale. As the field of Trust & Safety continues to mature, organizations offering technology products and services must anticipate how they might be misappropriated, abused, or serve as a vector to target their users. The Initiative seeks to help industry and government anticipate and actively manage these risks, in turn building trust, safety, and confidence in a product and its provider while simultaneously addressing risks with societal implications.

DECEMBER 2023 | Addressing the Human Element of Technological Change

Based on a broad listening tour across the trust & safety landscape, the Initiative identified six key themes to guide its work going forward, including:

- Adapting approaches in light of AI
- Addressing the crisis of legitimacy
- Closing the gap between T&S practice and public policymaking
- Adopting a global lens for T&S issues
- Tackling cross-platform spreading
- Promulgating frameworks and resources

AI AND STRATEGIC STABILITY

IST in 2023 also investigated the risks of AI in the nuclear context, partnering with the U.S. Department of State's Bureau of Arms Control, Verification, and Compliance to clarify the often opaque strategic stability risks posed by the integration of AI-enabled emerging technologies with nuclear command, control, and communications (NC3) systems across the globe.

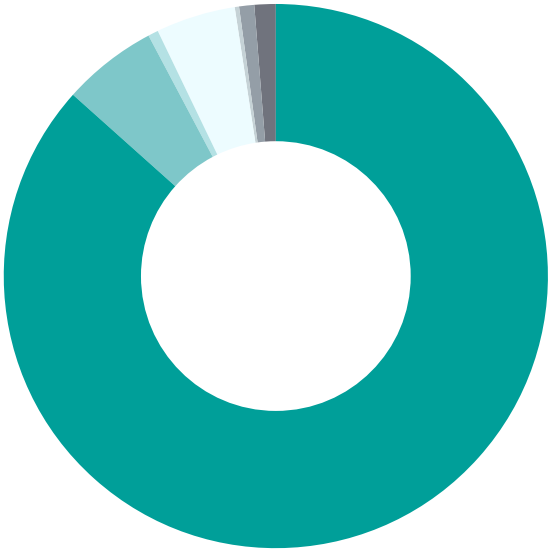
> "Given the nascent nature of AI-NC3 integration and the uncertainty surrounding it, it is clear that an international, multi-stakeholder conversation to outline the nuclear stability risks posed by AI-based capabilities is necessary."
>
> — Alexa Wehsener, Andrew W. Reddie, Leah Walker, Philip Reiner
> authors, *AI-NC3 Integration in an Adversarial Context*

FEBRUARY 2023 | AI-NC3 Integration in an Adversarial Context: Strategic Stability Risks and CBMs

This project convened scientists, engineers, policymakers, and academics in the San Francisco Bay Area and Washington, DC focused on the imperative to manage and mitigate risks posed by AI-enabled emerging technologies. Ultimately, the results of this study suggest fitting CBMs into four categories: CBMs that involve agreeing to, or communicating an intent to, renounce or limit the use of AI technologies in certain systems; CBMs that encourage governments and industry players to agree on standards, guidelines, and norms related to AI trust and safety, as well as "responsible" use of AI technologies; CBMs that increase lines of communication, such as hotlines and crisis communications links, and/or improve the quality, reliability, and security of communications in crisis; and CBMs that encourage education and training for policymakers, decision makers, and diplomats on AI knowledge and sharing of best practices across the public and the private sectors.

2023 Financials

FY 2023 REVENUE



Non-Government Grants **86.6%**	$3,377,397
Contributed Income **5.6%**	$220,062
Government Grants **0.6%**	$23,562
International Government Grants **4.7%**	$184,415
Sponsorship Income **0.3%**	$10,000
Management Fee Income **0.9%**	$34,990
Other **1.3%**	$49,316
Total	$3,899,742

FY 2023 EXPENSES

Program **73.4%**	$1,959,078
Administrative **26.2%**	$700,212
Fundraising **0.4%**	$9,930
Total	$2,669,219

* Graphs and tables include IST 2023 operational financial data. For further information and analysis please refer to forthcoming 2023 audited financials.

ISTeam

In March 2024, members of the IST team gathered in the San Francisco Bay Area for the annual team offsite.

While at the offsite, team members presented their work, discussed opportunities for cross-project collaboration, and aligned on IST's mission and values.

BOARD OF DIRECTORS

Michael McNerney
IST Board Chair

Andrew Boyd

Major General (retired) Robin L. Fontes

Suriya Jayanti

Katherine Johnson

Jason Kichen

Adean Mills Golub

T.J. Rylander

Eli Sugarman

LEADERSHIP

Philip Reiner
Chief Executive Officer

Megan Stifel
Chief Strategy Officer

Steve Kelly
Chief Trust Officer

About IST

The Institute for Security and Technology unites technology and policy leaders to create actionable solutions to emerging security challenges. Uniquely situated on the West Coast with deep ties to Washington, DC, we have the access and relationships to unite the best experts, at the right time, using the most powerful mechanisms.

Our portfolio is organized across three analytical pillars:

- **Geopolitics of Technology**: Anticipating the positive and negative security effects of emerging, disruptive technologies on the international balance of power, within states, and between governments and industries;
- **Innovation and Catastrophic Risk**: Providing deep technical and analytical expertise on technology-derived existential threats to society;
- **Future of Digital Security**: Examining the systemic security risks of societal dependence on digital technologies.

IST aims to forge crucial connections across industry, civil society, and government to solve emerging security risks before they make deleterious real-world impact. By leveraging our own expertise and engaging our trusted networks, we offer a unique problem-solving approach with a proven track record.

OUR VALUES

Trustworthiness: We earn trust and confidence through openness, transparency, collaboration, and consistent follow through.

Integrity: We promote the public interest over self-advancement, holding ourselves and our work to the highest standards.

Inclusion: We confront the most pressing security and technology challenges by harnessing diverse perspectives and experiences.

Resilience: We embody flexibility and adaptability in everything we do – surging, resting, pivoting, and scaling to meet today's mission needs, while maintaining readiness for tomorrow's.


IST
Institute for
SECURITY + TECHNOLOGY