

INSTITUTE FOR SECURITY AND TECHNOLOGY **ANNUAL REPORT 2022**



IST Institute for
SECURITY + TECHNOLOGY

2022 IN REVIEW

Seven years ago, a small group of national security professionals and California-based entrepreneurs set out to establish the Institute for Security and Technology with a vision: becoming a trusted source for technical and policy solutions to emerging security threats.

Today, we are still driven by this vision. We continue to be guided by our Silicon Valley start-up roots: we are agile and adaptable, we are constantly thinking about the next, emerging technology and the risks that come with it, and we maintain a go-getter approach to tackling some of the world's toughest security and technology challenges.

Yet we are also more prolific, successful, and established than ever. In 2022, we published 21 reports, briefings, and one pagers on topics ranging from the [ransomware payment ecosystem](#) and [forecasting the AI and nuclear landscape](#) to [nuclear crisis communications](#) and [digital cognition and democracy](#). We engaged with over 3,440 people at our public-facing events and were cited in over 160 articles in the media. We testified before Congress, participated in 45 events worldwide including the [White House Counter Ransomware Initiative Summit](#), the [Review Conference on the Non-Proliferation Treaty](#), and the [Paris Peace Forum](#), and held closed-door briefings with national and international representatives on a multitude of topics.



At Verify 2022 in May, Megan Stifel sat down with Lawfare's Benjamin Wittes for a live podcast recording on cybersecurity and Ukraine. | Photo credit: Steve Fisch



In November 2022, Philip Reiner joined the World Economic Forum's Annual Meeting on Cybersecurity in Geneva, where he discussed the use of cryptocurrency as legal tender. | Photo credit: Pascal Bitz



Ransomware Task Force co-chairs gathered at IST's May 2022 event, Combating Ransomware: A Year of Action. | Photo credit: Glen Echo Group

In addition, we expanded our team, widened our network, and built out our capabilities. We forged partnerships with [Metaculus](#), the [U.S. Department of State's Bureau of Arms Control, Verification, and Compliance](#), and over [60 members of the Ransomware Task Force](#), among many others. And to keep up with our expanding project portfolio, we created three thematic pillars to conceptualize and guide our work: [The Geopolitics of Technology](#), [Innovation and Catastrophic Risk](#), and [The Future of Digital Security](#). This positions us well for 2023, as we look to keeping up our commitment to the ransomware fight and building our Applied Trust and Safety and Open-Source Software initiatives, while continuing to build bridges between national security policymakers and the artificial intelligence and other emerging tech communities.



Elizabeth Vish joined the Paris Peace Forum for a roundtable discussion on public-private partnerships in fighting ransomware threats in November 2022. | Photo credit: Krystal Kenney



At the NPT RevCon in August 2022, Leah Walker participated in a side event hosted by the UNIDIR, BASIC, and the governments of the Netherlands and Switzerland.



At the Aspen Cyber Summit in December 2022, Megan Stifel joined a panel on efforts to curb illicit uses of virtual currency and enforce know-your-customer laws.

In a year of unprecedented productivity and growth, I want to thank you, our supporters, for making this possible. This evolution was possible because of your in-kind and financial support. I extend appreciation to our board, advisory groups, subject matter experts, partners, funders, and dedicated team. *Together* we are able to design and advance solutions to the world's toughest emerging security threats. I look forward to working with you in the year ahead!

Philip Reiner,
Chief Executive Officer, Institute for Security and Technology

OUR SUPPORTERS

The Institute for Security and Technology's success would be unimaginable without the generous support of the many foundations, organizations, government entities, and individuals who are the driving force behind our work. With their contributions, we are able to continue tackling some of the world's toughest emerging security threats, from countering ransomware and researching the cognitive foundations of the disinformation threatening our democracy to proposing tangible, technical solutions to mitigate the risk of nuclear war.

OUR DONORS

Our donors are what make the work we do every day at IST possible. Their engagement, trust, and support are integral to our ability to achieve our mission. We extend our deep appreciation to our individual donors and to the following corporate and philanthropic entities:



craig newmark philanthropies



German Federal
Foreign Office



Meta



Swiss Federal Department
of Foreign Affairs



U.S. Department of State

DONOR SPOTLIGHT

craig newmark philanthropies

IST was honored to [announce](#) Craig Newmark Philanthropies' commitment of \$2 million through 2024 and our role in the Craig Newmark Philanthropies Cyber Civil Defense Initiative. This commitment goes towards supporting our work in the areas of counter-ransomware, the Ransomware Task Force, and information security policy.

"The focus is on developing and implementing tools and services for regular people... When individuals have their security threatened, we're all at risk. Pulling together will help secure businesses, organizations, and the country as a whole."

— Craig Newmark, Founder, Craigslist and Craig Newmark Philanthropies



IST is grateful to the William and Flora Hewlett Foundation Cyber Initiative, which generously [provided \\$1,000,000 in additional support](#) to the Ransomware Task Force in 2022. The Hewlett Foundation Cyber Initiative's contributions enable IST to continue developing tools and insights for organizations and governments to outpace emerging global security threats.

"As a Silicon Valley-based think tank with a deep understanding of Washington's policy making process, IST plays a critical bridging role while working on some of the most pressing cybersecurity issues of the day, including their vital work on ransomware. We're proud to be able to support them."

— Kelly Born, former Director, Hewlett Foundation Cyber Initiative

EXPANDING OUR IMPACT

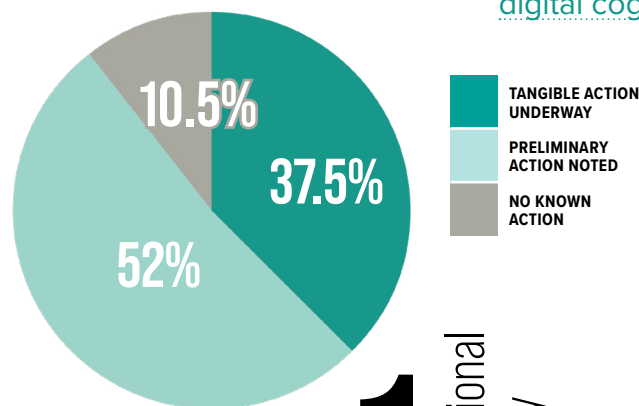
59,402 visitors

engaged with our NatSpecs blog, downloaded our reports, and read about our 3 thematic pillars on securityandtechnology.org.

21 in-depth reports

covered everything from the [ransomware payment ecosystem](#) and [forecasting the AI and nuclear landscape](#) to [nuclear crisis communications](#) and [digital cognition and democracy](#).

Since the initial release of the RTF report in April 2021, tangible progress was achieved in 18 of the 48 recommendations. Moreover, of the 48 recommendations, 43 experienced some degree of implementation.



11 public events

brought together 3,440 attendees. We hosted 39 external speakers, including Senators, authors, private sector representatives, directors of government agencies, nuclear experts, and Ransomware Task Force members.

4,187

followers on Twitter, up 106.9% since January 2021. Tweet impressions in 2022 totaled 733,000.

1

Congressional testimony

before the Senate Committee on Homeland Security.

161

articles covered the Institute for Security and Technology in media outlets nationally & internationally this year.

26 blog posts

on our NatSpecs blog. Most popular posts of 2022:

3,402 views: [RTF Year Two: New Map; New Data: Same Mission](#)

3,329 views: [Ransomware Task Force Releases Blueprint for Ransomware Defense](#)

810 views: [Digitally Influenced Cognition: What is it, and what does it mean for democracy?](#)

554 views: [The Role of Crisis Communications in the Russo-Ukrainian War](#)

485 views: [Crypto and Web3: Anticipating Security and Regulatory Challenges](#)



[Russia arrests ransomware gang responsible for high-profile cyberattacks](#)

Kevin Collier, January 14, 2022



[World News Roundup: Ukraine Invasion](#)

Steve Kathan, March 1, 2022



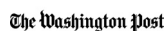
[Visual Explorer: Russian Disinformation](#)

Tina Trinh, March 16, 2022



[The Lawfare Podcast: Cybersecurity and Ukraine](#)

Benjamin Wittes, May 3, 2022



[One year ago, Colonial Pipeline changed the cyber landscape forever](#)

Joseph Marks, May 6, 2022



[What's next for a big ransomware task force](#)

Eric Geller, May 18, 2022



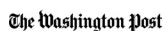
[A year after report, task force urges U.S. to keep ransomware on front burner](#)

Tonya Riley, May 20, 2022



[Ransomware Safe Havens, Reporting Inconsistencies Trouble Authorities](#)

Lindsey O'Donnell-Welch, May 24, 2022



[The government is finally tackling ransomware. More work remains.](#)

Washington Post Editorial Board, June 7, 2022



[Work Remains in Fight Against Ransomware](#)

James Rundle, June 8, 2022



[Pentagon's Office of Strategic Capital must win over Silicon Valley](#)

Leah Walker and Alexa Wehsener, December 13, 2022



[A new blueprint offers advice for businesses to protect against ransomware attacks](#)

Jenna McLaughlin, August 11, 2022



[Cyber officials from 37 countries, 13 companies to meet on ransomware in Washington](#)

Andrea Shalal, October 31, 2022



[Decoding the government's dire ransomware warnings](#)

Sam Sabin, November 18, 2022

FUTURE OF DIGITAL SECURITY

Stakeholders across the Internet want to improve its security. But no single entity coordinates efforts, implements sustainable cybersecurity, or addresses digital security market failures. IST works to fill this gap by uniting key stakeholders across industry, government, and civil society. In the last year, our work in the Future of Digital Security pillar has aimed to innovate new solutions, break down silos, and find effective methods to advance digital security, including countering the ransomware threat.

THE RANSOMWARE TASK FORCE

The Ransomware Task Force (RTF) combats the national security threat posed by the ransomware scourge with a cross-sector approach. Our 2021 report, [Combating Ransomware](#), made a powerful impact in the media, within government and private sector circles, and across the cybersecurity community; as of December 2022, 43 of the 48 recommendations had seen some degree of implementation. IST continues to lead an ongoing counter-ransomware campaign. Participants include both RTF members and other contributing partners, through the following lines of effort:

- » Cyber Insurance Roundtable
- » Cryptocurrency Working Group
- » Blueprint for Ransomware Defense Working Group
- » Ransomware Incident Response Network
- » Victim Notification Working Group
- » International Engagement Working Group

Blueprint for Ransomware Defense



In response to Action 3.1.1 of the [Combating Ransomware](#) report, which calls for the cybersecurity community to “develop a clear, actionable framework for ransomware mitigation, response, and recovery,” the Blueprint for Ransomware Defense Working Group developed the [Blueprint for Ransomware Defense: An Action Plan for Ransomware Mitigation, Response, and Recovery for Small- and Medium-sized Enterprises](#). The Working Group also released a [comprehensive tooling reference guide](#) to help evaluate progress on the implementation of data controls. The Blueprint is hosted on [CISA's Resources Page](#) and [translated into Spanish](#).



“Small businesses have paid hundreds of millions of dollars to cybercriminals in just the last year. And now a group of experts has released a blueprint full of advice on how to prepare for a possible ransomware attack.”

- Juana Summers on NPR's [All Things Considered](#)

5 webinars organized by the Blueprint for Ransomware Defense Working Group were attended by over 650 people.

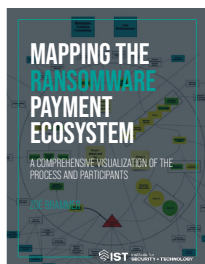
1. Tips and tricks for building your cybersecurity foundation
2. Building resilience in the face of a ransomware attack
3. Protecting your organization from access control gaps, misconfigurations, and outdated software
4. Containing and recovering from ransomware attacks
5. Cyber resilience and insurance innovation

40

actionable Safeguards taken from the CIS Controls were carefully selected for their ease-of-implementation and effectiveness for inclusion in the Blueprint.



Mapping the Ransomware Payment Ecosystem



[Mapping The Ransomware Payment Ecosystem: A Comprehensive Visualization Of The Process And Participants](#) develops an understanding of the actors, stakeholders, processes, and information involved in the ransomware payment ecosystem. It maps the entities involved and information produced at each point in the payment process. In future work, IST will analyze how each entity could leverage its position to better observe and affect the ransomware payment cycle. We will outline potential pathways and limitations in their abilities to add friction to the ongoing use of ransomware, including through the payment process.

Cyber Incident Reporting Framework



The Ransomware Task Force called for a “standard format for ransomware incident reporting” to respond to ransomware attacks more effectively. The [Cyber Incident Reporting Framework](#), submitted to inform a CISA request for information, recommends guiding principles and a structure for incident reporting. In response to feedback that similar guidance could be useful worldwide, the [Cyber Incident Reporting Framework: Global Edition](#) considers what conditions should be in place to make a reporting mandate effective and harmonizes suggested definitions with existing global regulations.

10 organizations

came together to provide input regarding cyber incident reporting.



In November 2022, Megan Stifel and Zoë Brammer highlighted the Framework at the United Nations Office of Drugs and Crime Ad Hoc Committee.



“We believe that CISA should maintain broad coverage for the reporting requirement, define significant cyber incidents to only encompass instances when real harm has occurred, and follow a set of principles (such as allowing for updates) in developing the regulation.”

- Megan Stifel & Michael Daniel in *The Hill*, [“Cyber incident reporting isn’t the problem — ignorance is”](#)

Ransomware Task Force Steering Committee

In 2022, we hosted the first two meetings of the Ransomware Task Force Steering Committee, which consists of senior stakeholders and experts that approach the RTF from an objective, ecosystem-wide perspective. They provide high-level support, help drive outcomes, and ensure the effectiveness of ongoing work.

10 Ransomware Task Force Steering Committee members

Daniel Barriuso, *Banco Santander*
Raj De, *Mayer Brown*
Craig Froelich, *Bank of America*
Royal Hansen, *Google*
Amy Hogan-Burney, *Microsoft*

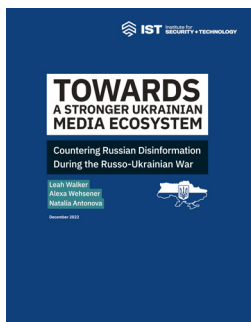
Sandra Joyce, *Mandiant*
Christopher Krebs, *Krebs Stamos Group*
Ciaran Martin, *University of Oxford*
Wendy Nather, *Cisco*
Jai Ramaswamy, *Andreessen Horowitz*

GEOPOLITICS OF TECHNOLOGY

21st century technology is shaping the outcomes of global conflicts, democratic norms and systems, and rising authoritarian power, as well as transforming global power dynamics and international conflicts. In 2022, IST worked to help governments, private companies, and civil society understand these effects, and devised plans, policies, and products that bolster collective resilience to technological change.

SUPPORT FOR CIVIL SOCIETY IN UKRAINE

Towards a Stronger Ukrainian Media Ecosystem



IST began supporting U.S. Embassy, Kyiv in 2021 to develop strategies to combat Russian disinformation and improve the digital safety of Ukrainian civil society and media. When Russia launched its invasion, the nature of the project shifted from preparation to response. IST, in partnership with VAST-OSINT Technologies, conducted real-time analysis of the Russian disinformation campaign during the ongoing war and of the tools most useful to Ukrainian media professionals. [Towards a Stronger Ukrainian Media Ecosystem](#) identifies six key themes of Russian information warfare across Ukraine's media ecosystem, each advanced by numerous supporting narratives.

Practical guides to digital safety, verifying information, and debunking propaganda



With the ongoing Russian attack on Ukraine, IST provided practical support to those covering Russia's war in Ukraine. [Towards a Safer Ukrainian Media Ecosystem and Civil Society](#) introduces readers to some of the best tools and practices for identifying and combating disinformation disseminated via videos, images, and Telegram channels. [Digital Safety Training for Ukrainian Journalists and Civil Society](#) provides practical tips to safeguard digital activities and improve digital hygiene. Both were translated into Ukrainian.

TECHCRUNCH

"Russian actors have deployed a vast array of techniques for "active measures" to confuse, sow doubt, and delegitimize basic democratic institutions. The mercenaries and clandestine agents Russia is deploying into Ukraine have honed their skills in hybrid battlespaces abroad, using a mix of...deniable influence operations and offensive cyber actions."
- Philip Reiner in *TechCrunch*, ["How the conflict in Ukraine threatens US cybersecurity"](#)

1,602 Russian & Ukrainian domains

were scraped between 1/4/2022 and 3/15/2022. Using unsupervised machine learning, VAST-OSINT grouped the 36,000 stories into most similar clusters for the [resulting analysis](#).

11

specific OSINT tools and strategies were offered in the [Towards a Safer Ukrainian Media Ecosystem and Civil Society](#) guide, ranging from YouTube filters and AI-generated image detection to photo shadow analysis and Telegram channel research.



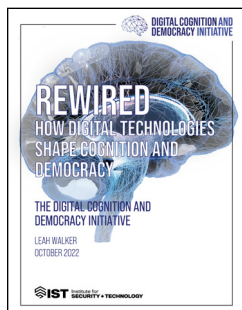
STRATEGIC BALANCING INITIATIVE (SBI)

For the United States to succeed in today's techno-industrial competition, the government and private businesses will need a shared understanding of the challenge, a clear-eyed sense of what is at stake, and knowledge of the tools we already have. SBI seeks to examine the public and private sectors' approaches to this competition, identify ways to align those efforts, and drive future economic, technological, and security stability. In 2022, we launched Phase I by creating a "baseline" analysis of capital vulnerabilities, manufacturing and hardware competitiveness, and existing government financial tools to share with key stakeholders.

DIGITAL COGNITION & DEMOCRACY INITIATIVE (DCDI)

Over the last two years, we have been exploring a key question: How are digital technologies affecting our cognitive capabilities in a way that makes us more susceptible to disinformation, affective polarization, and anti-democratic behavior? In 2022, the DCDI team released the culmination of its efforts thus far: seven papers that explore the effects of digital technologies at the individual, cognitive, and societal levels. Thank you to Craig Newmark Philanthropies, the DCDI Advisory Board, DCDI coalition members, and the DCDI team for their support in making this research possible.

Rewired: How Digital Technologies Shape Cognition and Democracy



This analytical report takes an escalating three-tiered approach: examining how effects of digital technologies on cognitive processes then affect the individual and society. To develop a model for understanding these effects, [Rewired: How Digital Technologies Shape Cognition and Democracy](#) proposes a Framework on Techno-Cognitive Risks that identifies the precise elements of digital technologies that may lead to areas of concern or vulnerability from the fundamental cognitive level up to the societal level. It is through the identification of these specific risks within these technology-driven domains that focused efforts can work to mitigate the threats to democracy we see today.

Tech Policy Press

"As we discovered in our research on digital cognition, the U.S. desperately needs to help voters grapple with the information overload, emotional manipulation, and shortcuts in reasoning that digital tools provoke."

- Zoë Brammer and Philip Reiner in *Tech Policy Press*, ["Democracy Gone Digital: The Election Season Online"](#)

6 foundational analyses



At the cognitive level, three papers dive into the processes of [memory](#), [attention](#), and [reasoning](#), examining how each process is affected by digital systems. The final three papers explore the effects of digital systems at the individual level, focusing on [critical thinking](#), [trust](#), and [emotions](#).

12

techno-cognitive risks were identified and categorized into 4 areas of concern: gamification; information overload; unnaturally immersive experiences; and lack of friction.

INNOVATION & CATASTROPHIC RISK

Nuclear weapons, artificial general intelligence, climate change, and synthetic biology all introduce threats that human civilization may not be able to survive. In some cases, emerging technologies can make us safer; in others, they present existential risks. IST's work in 2022 focused on technical ways to reduce cataclysmic risk.

THE CATALINK INITIATIVE

CATALINK is an internationally-driven, secure, resilient communications solution that has the potential to avert catastrophes amidst rising tensions between adversaries. In 2022, IST focused on furthering its technical development and design; building diplomatic consensus and understanding of the need for CATALINK; and increasing public understanding of strategic and nuclear risk reduction. We are grateful to the German Federal Foreign Office and the Swiss Federal Department of Foreign Affairs for their support of this initiative.



In August 2022, the CATALINK team [traveled to the 2022 NPT Review Conference](#), where they participated in sessions, engaged with governmental organizations, and held a side event on taking forward nuclear risk reduction.

18 existing points of failure in crisis communications

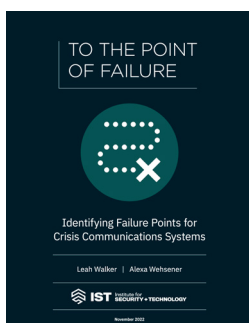
identified in our report [To the Point of Failure](#), which groups points of failure into operational, adversarial, accidental, and institutional categories.



"What's interesting about NC3 is that... where you can actually show that your systems are reliable and resilient and that they do the things they are supposed to do, that is actually inherently stabilizing."

- Philip Reiner on Future of Life Institute's podcast, ["Philip Reiner on Nuclear Command, Control, and Communications"](#)

To the Point of Failure: Identifying Failure Points for Crisis Communications Systems



Nuclear crisis communications and other diplomatic communication systems reduce nuclear risk by increasing transparency and predictability in state actions and intentions, while combating miscommunication. Failures in those communication systems can eliminate their ability to reduce risk, and may, in fact, increase the risk of war. [To the Point of Failure](#) assesses operational, adversarial, accidental, and institutional failure points in existing nuclear crisis communications. These existing points of failure are cemented by the increasing complexity of today's strategic environment and the additional risks it creates for reliable crisis communication use.

Atlas of Crisis Communications: Nuclear States



This atlas is part of IST's efforts to reinvigorate nuclear crisis control through research aimed at identifying practical nuclear risk reduction gaps. [Atlas of Crisis Communications](#) maps all existing hotlines between nuclear weapons states. It explains the use cases under which each hotline is employed, differentiates between bilateral and multilateral hotlines, and explains the unique historical circumstances that led to each.

Playing Telephone: Hoax Calls and the Insecurity of Leader to Leader Communications

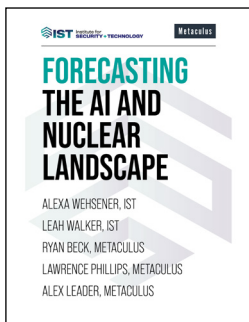


IST created a database of prank calls to world leaders as part of our efforts to understand the need for a secure, leader-to-leader communications system that can be trusted. [Playing Telephone](#) unpacks the security risks posed by hoax calls and identifies the novel technological developments that make them all the more concerning. It presents a map of known hoax calls that tracks perpetrator aliases, the leader who was targeted, and the communication method used. It concludes that international leaders and politicians must recognize the numerous parties interested in accessing their communications and the inherent vulnerabilities in the existing leader to leader communication regime.

ARTIFICIAL INTELLIGENCE & ADVANCED COMPUTING

Advances in AI-related technologies have the potential to significantly disrupt patterns of commerce, governance, and war. In 2022, IST explored the integration of AI into nuclear command, control, and communications systems and its implications for strategic stability risks. As part of this work, [IST partnered with Metaculus](#), a community forecasting platform designed to generate ML-optimized collective intelligence on topics of global importance.

Forecasting the AI and Nuclear Landscape



This report, the product of collaboration between IST and Metaculus, aims to assess the risks of escalation between the U.S. and China, including by the integration of AI into NC3. We developed questions across three categories: AI-nuclear integration, measures of US-China tensions, and nuclear use. Drawing on subject-matter expertise, the Pro Forecasters explored the probabilities of each scenario and the drivers behind each trend, focusing primarily on a five-year forecasting horizon. [Forecasting the AI and Nuclear Landscape](#) provides a valuable starting point for quantifying the risks and opportunities in the AI and nuclear landscape.

OUR VALUES

IST committed to incorporating its Diversity, Equity, and Inclusion strategy into all aspects of our work, from hiring practices to organizational policies and external engagement. We are driven by a firm belief that our work to tackle emerging security risks must start with a commitment to diversity, equity, inclusion, and belonging for all.

DIVERSITY, EQUITY, INCLUSION, AND BELONGING STATEMENT

The Institute for Security and Technology (IST) affirms that the inequalities and injustices that affect any of us inevitably affect us all. The very essence of community strength—and security—begins with embracing and appreciating the benefits our differences bring.

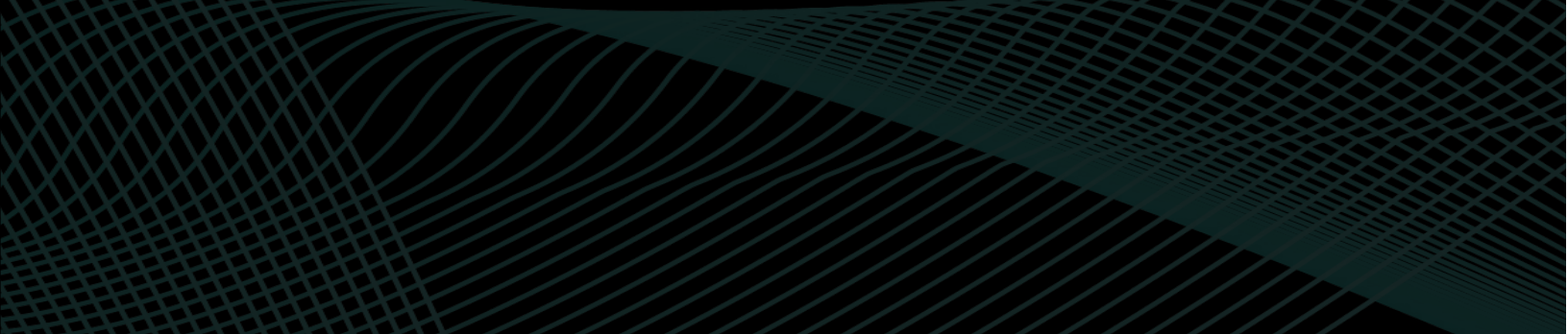
Whether it be structural inequality, systemic racism, or unequal access to personal and professional opportunities, such phenomena make for ineffective organizations and jeopardize security at all levels, from individual to international.

Knowing this, we strive to make the following principles of diversity, equity, and inclusion as integral to our daily work as they should be to the broader security spaces we aim to improve.

Systemic issues of inequality must be confronted on a daily basis, which begins with exploring how narratives, norms, and unconscious biases impact the presence of under-represented voices within our own networks and those of our partners.

We commit to continuing to incorporate diverse perspectives in our planning and research, and to actively seeking participation from those outside of traditional channels to help us gain a clearer view of the professional fields in which we engage.

Identity cannot be bound by anyone else's terms. We recognize that each individual has their own background, ideas, voice, and a valuable impact to be respected in any room, but that too often, cultural expectations narrow sharply those perspectives.



We honor that individuals experience workplace culture differently. As a team we commit to open dialogue to understand one another, without invalidating one another if our own experience is not the same.

Uneven access to opportunities contributes to unequal and ineffective systems. We recognize that improved access creates a more level playing field, which in turn creates a more effective and more secure field for everyone.

We commit to actively providing resources and facilitating access for all team members, partners, associates, and community members, regardless of rank or position.

When empowered by these principles, we believe we will be better positioned to identify security risks and design more effective solutions. As our learning evolves, we will continue to be introspective on these beliefs, review our principles regularly, and share our successes and failures with our team, partners, and community members.

VALUES IN ACTION: STRATEGIC GOALS

Culture

Ensure the team supports a series of patterns to enable an inclusive culture. Leadership promotes the vision and strategy by taking actions to increase diversity and equity across all levels of the organization and maintain an inclusive work environment.

Consistency

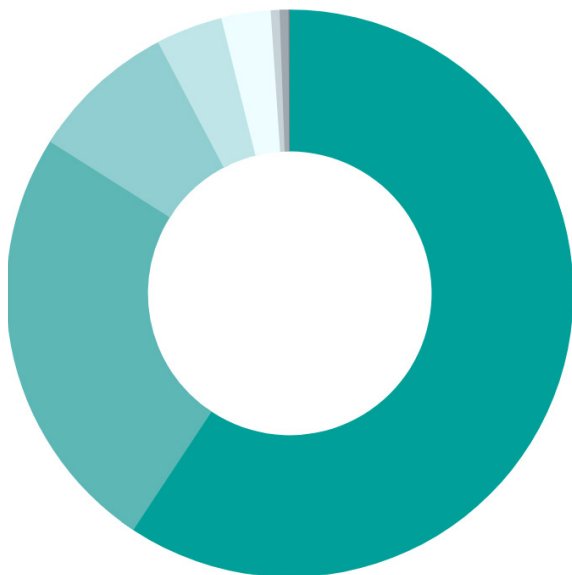
Mature IST's strategy to improve the consistency of desired outcomes by assessing and strengthening policies and procedures.

Community

Encourage inclusion and diverse perspectives in IST's internal projects and external stakeholder engagement; uphold community-level commitments; and foster mentorship within the space.

2022 FINANCIALS

FY 2022 REVENUE



Non-Government Grants	59.1%	\$2,719,500
Fiscal Sponsorship	24.6%	\$1,132,738
Contributed Income	8.3%	\$385,593
Government Grants	3.8%	\$175,028
International Government Grants	2.8%	\$129,522
Sponsorship Income	0.5%	\$25,000
Management Fee Income	0.5%	\$25,000
Other	0.07%	\$3,329
Total		\$4,595,710

FY 2022 EXPENSES



Program	65.2%	\$1,729,574
Fiscal Sponsorship	24.8%	\$657,738
Administrative	6.2%	\$164,505
Fundraising	3.8%	\$101,890
Total		\$2,653,707

* Graphs and tables include IST 2022 operational financial data. For further information and analysis please refer to forthcoming 2022 audited financials.

BOARD AND TEAM

BOARD OF DIRECTORS

Michael McNerney, *Board Chair*

Robin Fontes

Katherine Johnson

Jason Kichen

Adean Mills Golub

T.J. Rylander

Eli Sugarman

LEADERSHIP

Philip Reiner, *Chief Executive Officer*

Megan Stifel, *Chief Strategy Officer*

Alice Hunt Friend, *Vice President for Research and Analysis*



INSTITUTE FOR SECURITY AND TECHNOLOGY
www.securityandtechnology.org

info@securityandtechnology.org

Copyright 2023, The Institute for Security and Technology