THE FUTURE OF CYBERSECURITY

REAL-WORLD SOLUTIONS

ists.dartmouth.edu
When I talk about Dartmouth being academically energized, a place of innovation and intellectual risk-taking, I think of the incredibly important work being done in the area of cybersecurity. We speak of Dartmouth as a birthplace of big ideas and bold efforts with the courage to take on some of the world’s most pressing challenges. Cybersecurity is one of those challenges.

With the number of Internet-connected devices growing exponentially, so too grows the number of information security risks. Recognizing the social and technical complexities associated with those risks, we have created an academic cluster — cohorts of world-renowned scholars — to focus on cybersecurity themes and questions that cut across disciplines, departments, and schools. And we have created the Institute of Security, Technology, and Society to help address the challenge of securing our cyber future by developing world-class information technology security, privacy, and usability solutions and educating the next generation of cybersecurity innovators.

Responding to the global challenges of cybersecurity requires rigorous research and analysis of technology and how people use it. Internationally respected in fields such as computer science, engineering, government, psychology, and sociology, I believe Dartmouth is poised to be a world leader in this space.

Philip J. Hanlon ’77
President, Dartmouth College

ISTS HISTORY & MISSION

In 2000, recognizing grave threats to the nation’s information security, an act of Congress created the Institute of Security, Technology, and Society at Dartmouth. A report from the U.S. President’s Council of Advisors on Science and Technology had recommended that a nongovernmental organization be formed to address national cybersecurity issues in an increasingly networked world. There was a national-security need for a research-and-development hub dedicated to protecting the nation’s critical infrastructures.

In a 2009 interview recalling the founding of the Institute, then-Dartmouth Provost Barry Scherr said, “Senator Judd Gregg [R-NH] took an interest in the subject and played an instrumental role in establishing the ISTS at Dartmouth. He understood the gravity of the cyber threat to the nation before many others recognized the problem, and he felt that Dartmouth, with a history of excellence in computer science and a strong interdisciplinary and collegial environment, was an obvious choice.”

The simplicity of the ISTS mission would directly guide its complex work. The Institute would be dedicated to pursuing research and education to advance information security and privacy throughout society.

Since its founding, ISTS affiliates have conducted outstanding, crucial interdisciplinary research, education, and outreach programs, involving work from 64 faculty members across every school at Dartmouth and 21 faculty at other institutions. The range of threats has increased alongside the burgeoning research: Artificial intelligence and machine learning put to malicious purpose. Foreign interference in national elections. An explosion in social media and the propagation of propaganda and misinformation. Exposed vulnerabilities in the electrical grid and financial institutions. The proliferation of unsecure wireless networks. The Institute’s scope, by necessity, has grown beyond its original mandate. Its important work not only addresses our national security. It impacts the prosperity and resiliency of societies around the world.
**V.S. Subrahmanian**  
Dartmouth College Distinguished Professor in Cybersecurity, Technology, and Society  
Professor of Computer Science; Director, ISTS  

World-renowned scholar, author, and speaker whose work in data science and cybersecurity has been used to detect bots on social media platforms, prevent rhinoceros poaching, and accurately forecast the behavior of terrorist networks. Prior to being named director of Dartmouth’s Institute for Security, Technology, and Society in 2018, co-founded the University of Maryland’s Lab for Computational Cultural Dynamics and founded its Center for Digital International Government. He has been an invited speaker at the United Nations.

**Sergey Bratus**  
Research Associate Professor of Computer Science  

Dartmouth’s “hacker-in-residence,” expert on computer security and intrusion analysis. Has published more than 100 technical papers and presentations and received numerous awards, most notably shared the 2013 BlackHat Pwnie award for Most Innovative Research.

**George Cybenko**  
Dorothy and Walter Gramm Professor of Engineering  

Pioneer in machine learning, adversarial dynamics, and cybersecurity; government advisor on boards including the Army Cyber Institute at West Point. Founding editor of IEEE Security & Privacy, the leading professional security publication.

**Dave Kotz**  
Champion International Professor, Department of Computer Science  

Prolific author and expert in privacy, pervasive computing for healthcare, and wireless networks. Previously served as interim provost at Dartmouth and as executive director of ISTS. Served on the U.S. Healthcare IT Policy Committee.

**Gene Santos**  
Professor of Engineering, Thayer School of Engineering  

Artificial intelligence expert whose work encompasses the areas of information, cognition, human factors, and mathematics. Has applied his work to insider threat and deception detection, intelligence assessment, and analysis of adversarial intent and course of action.

**Sean Smith**  
Professor of Computer Science  

Security architect who investigates how to build trustworthy systems including power grid, health care, and finance. An outstanding classroom teacher who has performed security reviews, designs, analyses, and briefings for a wide variety of public-sector clients.

**Soroush Vosoughi**  
Assistant Professor of Computer Science  

Miner and modeler of large social and information networks. Studies complex social behaviors using methods at the intersection of natural language processing, machine learning, and network science. Expert on social cybersecurity.
How will we secure the systems we depend on when it’s not just computers that are connected?

In his 2017 book The Internet of Risky Things, Sean Smith writes, “…by 2020 we will have over 25 billion networked devices embedded throughout our homes, clothing, factories, cities, buildings, and bodies. If we build this new Internet of Things the way we built the current internet of computers, we are heading for trouble: humans cannot effectively reason about security when devices become too long-lived, too cheap, too tightly tied to physical life, too invisible, and too many…” Smith, a professor of computer science and the former director of ISTS, says that part of the daunting challenge facing our digital security is
Wearable devices and advanced wireless technology have been a boon for medical professionals, patients, and for people taking control of their own bodies. “But there are a host of risks,” says professor David Kotz. “What information gets collected? Who has access to it? For what period of time? A woman probably doesn’t want everyone in Bluetooth range to know about her fertility. A doctor needs confidence that it’s actually his patient wearing the data-sending device.”

For years, Kotz’s research has focused on securing this type of confidential health-related data. But with the explosion in wearable devices, smart phones, smart cars, smart homes, and other technologies that receive, react to, and record our movements and behaviors, he and other Dartmouth researchers are working on a broader application of that work: securing personal information of all kinds.

Besides the human layer, he focuses his work on making lower-level software more secure, the layer invisible to those of us using the Internet of Things in the world. There, at the level of electrical circuits and the laws of physics, Smith works to harden the door of systems, keeping attackers out. He works, as well, to limit and contain the potential damage should the attackers get inside.

In a robust system, the power grid doesn’t go dark. Financial data isn’t stolen. A plane doesn’t fall out of the sky. The same fundamental principles apply.

In the Consumer Internet of Things, doctors remotely monitor a heart patient’s activity and stress levels in real time — invisibly and painlessly — and get far more detailed daily data than ever before possible. A small patch automatically measures and records glucose levels and delivers insulin, lessening the burdensome chore for diabetics and saving hours of time in hospital visits. A young woman wears a fertility tracking bracelet while sleeping, capturing physiological signals that track her monthly menstrual cycle, then syncs the data with a smartphone app that accurately predicts the most fertile times for becoming pregnant.
Scientists have long used games to test and measure the progress they’ve made in developing artificial intelligence. Two decades ago, IBM’s Deep Blue computer reached a significant milestone when it beat the world chess champion, Garry Kasparov. But winning at an “imperfect information” game like poker — where there’s hidden information that only one player knows — has proven to be a much higher bar for the technology. That bar was finally passed only recently. Observers in the scientific community hailed the achievement.

“But in both those arenas,” Dartmouth’s George Cybenko notes,
“the rules are fixed, and what it means to win is well defined. In the cybersecurity arena, there are no rules. And we often don’t even know what the adversaries want.”

Cybenko is a pioneer in the fields of machine learning and artificial intelligence. Thanks largely to recent advances in so-called deep learning, machine learning is revolutionizing how many problems are formulated and solved today. Open-source, high-quality software is increasingly accessible to researchers and developers. Powerful computers and the availability of big data, thanks to the cloud, are allowing machine learning on massive data sets of text, speech, and images. The ability of machines to recognize images has already surpassed that of human beings. In natural language translation, machines are approaching human capability.

Today, Cybenko, Soroush Vosoughi, and V.S. Subrahmanian are among the ISTS faculty investigating the dynamics of learning in adversarial engagements, when all participants are adapting through experience. Just one challenge among dozens: In the continual cat-and-mouse game we see in cybersecurity, it is faster and less expensive to tweak and re-deploy malware than it is to develop the defenses against malware. But the question needs to be asked: Are the adversaries’ adjustments shaping the way the defenses need to react, laying the groundwork for a more significant attack down the road when the opportunity is right?

“I’m applying work I’ve done in machine learning for over 30 years to security problems. This is a very exciting time because machine learning is developing so rapidly and cybersecurity is in so much need of new approaches. The old approaches just aren’t working very well. It’s a technological renaissance that will have profound implications for cybersecurity.”

~ George Cybenko

// ISTS by the Numbers

483 CONFERENCE PAPERS PRESENTED

381 NUMBER OF PEER-REVIEWED JOURNAL ARTICLES PUBLISHED
Call it social insecurity in the digital age. With so much news, opinion, information, and advertising racing across our massive social networks, how’s a good citizen to know what is coming from legitimate sources? How to detect an ulterior motive? The 2016 presidential election revealed just one widespread practice of social hacking: the deliberate posting and spreading of misinformation intended to confuse voters and influence behavior. There are dozens of other examples of bad actors distorting and manipulating the free flow of information across the platforms we use every day: from fake Astroturfing. Bots. Sockpuppets. Propaganda. Censorship.

Undercover work being done at ISTS is part of the policing of the information superhighway.

I use computational methods to understand and detect propaganda. It’s a mix of computer science and social science.

~ Soroush Vosoughi
reviews on Amazon to bots sending false narratives or deceptive, personalized advertising over Twitter.

Soroush Vosoughi uses machine learning to mine and model the data appearing on social media, integrating algorithms to parse and analyze the sources and veracity of the content. As technical director of the Electome project (at the Laboratory for Social Machines at MIT), Vosoughi and a team of graduate students developed the analytics that were used to brief the moderators of the 2016 presidential debates.

A flip side to the equation: the anonymous accounts that shield identities on social media also serve as protective proxies for free speech in countries where free speech is censored. In response, repressive governments have begun using sophisticated software to analyze patterns in written communications to identify and persecute authors and activists who use such accounts. Another project of Vosoughi’s runs the language from such anonymous accounts through a translator that retains the content while changing the style, making the source impossible to identify.

The tools, says Vosoughi, come from state-of-the-art machine learning. The purpose, in his words, are “social cybersecurity.”

This is an area of deep collaboration and expertise at ISTS, including work by V.S. Subrahmanian and by George Cybenko, whose pioneering research into fake news goes back to 2002.

“"If George is the Father of fake-news detection, Soroush is the current King. Both have contributed enormously to our understanding of the psychological behaviors that drive the practice.”

~ V.S. Subrahmanian

---

**NUMBER OF PARTICIPANTS IN AN ISTS-LED SIMULATION OF A SUSTAINED CYBER-ATTACK AGAINST CRITICAL INFRASTRUCTURE IN THE U.S. PARTICIPANTS REPRESENTED FEDERAL AGENCIES, STATE AND LOCAL GOVERNMENTS, AND PRIVATE-SECTOR ORGANIZATIONS.**
For too long, cybersecurity has been the domain of hard-core computer scientists, those guys who look into the kernels of the operating systems, into the detailed structure of the routers and the very low-level code and hardware that implement devices and communications capabilities. Over the past decade, though, the nature of computing has changed dramatically. The way people communicate using computers is no longer a point-to-point phone call style operation. People can broadcast their message to the world, wirelessly, or target it for one specific individual. This new kind of sharing — with huge quantities of information flowing in all directions — is ripe for abuse.

“Deceptive or fraudulent tactics show up everywhere, from fake reviews meant to harm a product’s sales to news releases purposely distributed with misinformation to drive a particular stock price up or down!”

~ Gene Santos
swaths of data traveling across a vast number of platforms and devices — has fundamentally changed the way attackers view vulnerability and how they construct malware.

At the same time, big data and machine learning have changed the game for the defense.

In 2015, V.S. Subrahmanian published the groundbreaking Global Cyber-Vulnerability Report, an analysis of more than 20 billion reports generated by 4 million computers in 44 countries, detailing risk on an unprecedented scale. He has pioneered methods, as well, of deception and deterrence. “Most people try to build firewalls and keep attackers out,” he says. “We know that works only to some extent.” A part of the work at ISTS by Subrahmanian, George Cybenko, Gene Santos, and others focuses on how to handle adversaries who have already penetrated a system. “For instance,” says V.S., “how can we impose costs on attackers who have breached the security system of a Lockheed Martin, say, even when we don’t know who those attackers are? We’ve developed one defense that creates multiple versions of the same documents, so the people attempting to steal intellectual property now don’t know what they’ve got, and to figure out what’s important will cost them significant time and money trying.” Another tactic is to generate “fake scans” that deliver multiple results to an adversary looking for a location within a system. Someone might know the crown jewels they’re trying to steal are in New Hampshire, for example. But when they try to locate them, fake scans point them in several different places, to Hanover and Manchester and Portsmouth and Keene. They may end up stealing the crown jewels, but the fake results will have frustrated and delayed them, perhaps at great cost. Or may even keep them from trying further.
Say you’re a CEO and you need to make a tough call about transparency in your annual report. Or, maybe more consequentially, say you’re in a position high up in the U.S. military or state department, and you’re studying intelligence about what Iran is really thinking about nuclear weapons. You’ll likely have advisors with points of view, armed with arguments. But how will you know if they’re arguing in good faith?

Gene Santos has been given transcripts of sensitive, private conversations like those, to add to the hundreds and thousands...
of other conversations he’s parsed and entered into computer models. His models reveal patterns: variations from previous conversation, advice glaringly inconsistent with what the models would predict, outlying signals that raise flags. In some cases, he’s been given tables showing the sources that arguments were built on, enabling even deeper research: uncovering lines of reasoning built on false information; arguments revealing weak links from having been constructed backwards from a favored conclusion; evidence suggesting deceptive tactics or even malicious intent.

“What we sell is not meant to influence decisions,” he says. “It’s research meant to reveal consistency or inconsistency over time. To get at the question, When is it opinion? When is it fact? And then get below that for the most likely reason why.”

In addition to Santos, others at ISTS are probing facets of truth and verification, including Sean Smith, George Cybenko, and V.S. Subrahmanian.

“During the big East Coast black-out emergency in 2003, the mobilization effort involved massive amounts of sensitive information being shared through all kinds of telephone calls across companies and industries, even international boundaries. Afterwards, I analyzed thousands of pages of transcripts to try and find out how humans decided who and who not to trust.”

~ Sean Smith

AMOUNT OF THE ANONYMOUS 2015 GIFT TO ENDOW THREE FACULTY POSITIONS IN CYBERSECURITY AS PART OF DARTMOUTH PRESIDENT PHILIP HANLON’S CLUSTER INITIATIVE TO ENCOURAGE MULTIDISCIPLINARY RESEARCH AND PEDAGOGY. PROFESSOR V.S. SUBRAHMANIAN WAS THE FIRST FACULTY MEMBER RECRUITED.
In a 2008 paper, Sergey Bratus laid out an unusual argument for re-orienting the way software engineers build secure systems: look for a deeper methodology behind the approaches used by hackers who try to exploit them; don’t dismiss hacking as a bag of random tricks. In “What Hackers Learn That the Rest of Us Don’t,” Bratus outlined the effective traits of the hacker community, such as its special ways of deep analysis, reverse engineering, testing and modifying software and hardware, and looking across entire computing environments beyond their convenient layers.

In a word, I believe that state-of-the-art hacking is already a distinct discipline of computer science, even though not formally recognized as such.

~ Sergey Bratus
of abstraction that are the basis of the traditional curricula. Most of those practices would be expensive, time-consuming luxuries in the often-siloed, deadline- and efficiency-driven world of commercial IT. When putting together his syllabus for his course on computer security, Bratus realized that the source dealing not just with exploitation techniques but with the widest range of background topics in systems and networks were the electronic hacker magazines Phrack (http://phrack.org) and Uninformed (http://uninformed.org). He made them required reading.

Bratus is quick to distinguish hackers. He describes white hats as ethically opposed to causing harm to the users of computer systems. Along with gray hats — those who are willing to skirt or break existing laws in the greater service of warning the vulnerable while minimizing the damage — white hats publish their research and techniques in security-related public conferences and journals, just as Bratus himself has done. Black hats act for personal gain, with no regard for the harm or damage their actions cause. They’re the ones who have given “hacking” a bad name, which is unfair and detrimental to the society that increasingly depends on computers and needs them to be trustworthy. Imagine chemistry being associated with poisoning, locksmithing with burglaries, or rhetoric with lying. When a useful branch of knowledge gets popularly associated with its abuses, everyone loses.

“If you’re defending yourself against attackers,” says Bratus, “it only makes sense that you learn what the best of the attackers know, and how they know it. After you do, you will see your systems in a very different light.”

Being much indebted to the hacker community for many things I learned from its amazingly rich sources, I’ve tried to describe some trends in the hacker learning experience (sometimes called the “hacker curriculum”) that distinguish it from the typical experiences of traditionally trained developers and CS students. We use many principles of this hidden curriculum in our teaching of Computer Security at Dartmouth.”

~ Sergey Bratus
David Kotz is the Champion International Professor of Computer Science at Dartmouth College. He previously served as Dartmouth’s Interim Provost and Associate Dean of the Faculty for the Sciences, as the Executive Director of the Institute for Security Technology Studies, and on the US Healthcare IT Policy Committee. He has published more than 200 refereed papers, obtained more than $67M in grant funding, and mentored nearly 100 research students. An in-demand speaker and presenter at academic conferences and in corporate settings, he has also served as a technical consultant for industry and an expert witness in patent and intellectual-property cases.  

For more information see cs.dartmouth.edu/~dfk

Questions posed in the Abstract for “Challenges to ensuring human safety throughout the life-cycle of Smart Environments,” by David Kotz and Travis Peters, 2017: How does an occupant identify and decommission all the Things in an environment before she moves out? How does a new occupant discover, identify, validate, and configure all the Things in the environment he adopts? When a person moves from smart home to smart office to smart hotel, how is a new environment vetted for safety and security, how are personal settings migrated, and how are they securely deleted on departure? When the original vendor of a Thing (or the service behind it) disappears, how can that Thing (and its data, and its configuration) be transferred to a new service provider? What interface can enable lay people to manage these complex challenges, and be assured of their privacy, security, and safety?

His seminal contributions to the field of cybersecurity include advances in signal processing, neural computing, parallel processing, and computational behavioral analysis. His research in the late 1980s proved that simple neural networks could solve any computational problem, an area of resurgent interest with Facebook, Google, Microsoft, and others now making big bets on A.I. advances based on neural networks. His groundbreaking work in the early 2000s was the first to expose the now commonly understood concept of fake news.

For more information see dartmouth.edu/~gvc

Cybenko has become increasingly interested in finding applications for his work. With colleague Vincent Berk, he cofounded a company called FlowTraq, which uses proprietary algorithms to analyze the network traffic of firms in order to create a “behavioral fingerprint” that can then be used to identify potential security breaches. “Academic journals are graveyards for ideas,” Cybenko says, despite having served as editor-in-chief of several journals. “People have written papers about thousands of good ideas in the field of cybersecurity, but unless a Microsoft or Symantec picks them up and makes a product out it, your idea will remain a paper.” – from “Hacking the Hackers,” by Michael Blanding
Eugene “Gene” Santos, Jr., is Professor of Engineering at Thayer School of Engineering. His work on artificial intelligence intersects the areas of information, cognition, human factors, and mathematics. His current focus includes dynamic human behavior, computational intent, and decision-making with an emphasis on learning nonlinear and emergent behaviors and decisions. He has applied his work to a number of areas involving cybersecurity, including insider threat and deception detection, intelligence assessment, and adversarial intent and course of action analysis. He has advised or served on US Department of Defense and Intelligence Community committees and numerous federal agencies and working groups. He is currently appointed to the State of Vermont Taskforce on AI and is a 2019 Public Voices fellow of the OpEd Project.  

For more information see engineering.dartmouth.edu/people/faculty/eugene-santos-jr

In his own words: “How do people make their decisions and take action? I want to explain the basis for why people do what they do. Our influences aren’t deterministic. You can’t say a cultural experience will always produce a particular outcome, but influence can make an outcome more or less likely. I try to capture those elements of what’s more likely and what’s less likely. That gives me a baseline. Then once I see an action, I can go back through the influence structure, including what people have told me about their beliefs, their demographics, and their personal history, to see how they got from their background to their final action. At this point the only way to understand a complex system is to reverse engineer it. To understand the system is to dissect it.”

Sean Smith was director of ISTS from September 2015 to April 2018. Before coming to Dartmouth in 2000, he fought postal meter fraud with the US Postal Inspection Service; performed security reviews for Los Alamos National Laboratory, and designed security architecture at the IBM T.J. Watson Research Center. He has published more than 100 refereed papers and has written three books, including The Internet of Risky Things (2017). His security architecture is used in thousands of financial, e-commerce, and rights managements installations world-wide.  

For more information see cs.dartmouth.edu/~sws/cv

Most users aren’t even sure what services their machines are happily offering to anyone who queries on the Internet. Current best security practices dictate that one make sure to install all the latest security patches and updates for the OS and the applications and to disable all unnecessary network services. The vexing thing is that these actions do not guarantee a system free of vulnerabilities. Indeed, almost the opposite is true: We can guarantee, with extraordinarily high confidence, that serious vulnerabilities exist, but that neither the defenders nor, we hope, the attackers have discovered them yet.  

~ from The Craft of System Security (2007)
Soroush Vosoughi
Assistant Professor of Computer Science

**FORMER APPOINTMENTS:** Fellow at Harvard’s Berkman Klein Center for Internet & Society; Postdoctoral Associate at MIT Media Lab; Technical Advisor to Cortico, a nonprofit dedicated to fostering constructive public conversation.

**CURRENT APPOINTMENT:** Affiliate, Harvard’s Berkman Klein Center for Internet & Society.

**EDUCATION:** S.B., MIT (2008); M.S., MIT (2010); Ph.D., MIT (2015).

**CURRENT RESEARCH INTERESTS:** Machine Learning, Computational Linguistics and Natural Language, Propaganda Detection, Privacy Protection.

The most recent addition to the ISTS team, Soroush Vosoughi comes from the Media Lab at MIT, where he headed up the largest-ever study of false news. His research focuses on mining and modeling large social and information networks and developing analytical methods in information, data, and network science. He applies these methods to address urgent societal challenges. In his current research, he is using computational methods to study privacy and propaganda on social networks.  

Electome used its machine learning algorithms to measure all political conversation on topics including guns, immigration, terrorism, jobs, racial issues, seniors and Social Security, the economy, and education.

Vosoughi said Electome also took pains to follow the political conversation in real time in order to make its issue categories as precise as possible. “Since the conversation around the election is very dynamic and new terms and phrases are brought into the conversation constantly, our system automatically re-trains itself once a week so that it is aware of the most up-to-date terms and phrases,” he said.


V.S. Subrahmanian
Dartmouth College Distinguished Professor in Cybersecurity, Technology & Society  
Professor of Computer Science; Director, ISTS

**AWARDS:** National Science Foundation National Young Investigator Award; Distinguished Young Scientist Award from the Maryland Science Center/Maryland Academy of Science.

**EDUCATION:** M.Sc. (Tech.) Computer Science, Birla Institute of Technology and Science, India (1985); M.S. and Ph.D. in Computer Science, Syracuse University (1987, 1989).

**PAST APPOINTMENTS:** US-India (Track 2) Strategic Dialogue; India-Israel (Track 2) Forum; US Air Force Science Advisory Board (ad hoc); US Department of Defense (DARPA’s Executive Advisory Council).

**CURRENT RESEARCH INTERESTS:** AI, Probabilistic & Statistical Inference, Predictive Modeling for Cybersecurity & Counterterrorism Applications, Managing Huge Databases w/ Spatial, Temporal, Multimedia & Uncertain Information.

V.S. Subrahmanian joined Dartmouth in 2017 from the University of Maryland, where he built a career over three decades as a computer science professor and director of the University of Maryland Institute for Advanced Computer Studies. He is a fellow of the American Association for the Advancement of Science and the Association for the Advancement of Artificial Intelligence.


Subrahmanian has applied his work to an extraordinary range of subjects, from improving airline profitability through machine learning to identifying bad actors on social media to understanding behaviors of rhinos and poachers in South Africa. He developed the first data-driven computational predictive models of terrorist groups and some of the first ways of reshaping terrorist networks.


**In his own words:** “When I speak about cybersecurity, I speak of its three M’s: It is multi-disciplinary. Multi-stakeholder. Multi-national. You can’t be successful if you’re looking at just one aspect. That’s one reason we are so effective at Dartmouth.”
Ambassador Daniel Benjamin

Ambassador Daniel Benjamin is the Norman E. McCulloch Jr. Director of the John Sloan Dickey Center for International Understanding. Prior to joining the Dickey Center in 2012, Daniel Benjamin served as Ambassador-at-Large and Coordinator for Counterterrorism at the U.S. State Department. ▶ DICKEY.DARTMOUTH.EDU/PEOPLE/DANIEL-BENJAMIN

Professor Andrew Campbell

Professor Andrew Campbell is an experimental computer scientist working in mobile computing. His research interests include using embedded sensors and machine learning on phones and wearables to infer human behavior with applications to health, particularly mental health sensing. ▶ CS.DARTMOUTH.EDU/~CAMPBELL

Professor Amro Farid

Professor Farid leads the Laboratory for Intelligent Integrated Networks of Engineering Systems (LIINES) and has made active contributions to the MIT-Masdar Institute Collaborative Initiative, the MIT Future of the Electricity Grid Study, and the IEEE Vision for Smart Grid Controls. Professor Farid’s research interests include: intelligent energy systems; sustainability, resilience, and reconfigurability; integrated control, automation, and information technology; smart power grids; energy-water nexus; transportation electrification systems; industrial energy management and demand response. ▶ ENGINEERING.DARTMOUTH.EDU/PEOPLE/FACULTY/AMRO-FARID

Professor Adam Kleinbaum

Adam Kleinbaum is an Associate Professor in the Strategy and Management area at the Tuck School of Business at Dartmouth. Professor Kleinbaum’s research interests include: the origins and evolution of social network structure; the neuroscience of social networks; and organizational consequences of social network structure. ▶ FACULTY.TUCK.DARTMOUTH.EDU/ADAM-KLEINBAUM

Professor Charles Palmer

Professor Charles Palmer is an Adjunct Professor in the Computer Science department at Dartmouth College. Professor Palmer is also a Distinguished Research Staff Member at IBM’s Thomas J. Watson Research Center where he has been working in security and privacy. ▶ WEB.CS.DARTMOUTH.EDU/PEOPLE/CHARLES-C-PALMER

Professor Daniel Rockmore

Professor Rockmore is the William H. Neukom 1964 Professor of Computational Science and Dartmouth College’s Associate Dean for the Sciences and Director of the Neukom Institute for Computational Science. Professor Rockmore’s research interests include: complex systems, network analysis, machine learning, cultural evolution, group theoretic transforms. ▶ CS.DARTMOUTH.EDU/~ROCKMORE

Professor Benjamin Valentino

Benjamin Valentino is an Associate Professor of Government at Dartmouth College. His research interests include the causes and consequences of violent conflict and American foreign and security policies. He is also the faculty coordinator for the War and Peace Studies Program at Dartmouth’s Dickey Center for International Understanding. He is currently working on several research projects focusing on public opinion on the use of force, civilian and military casualties in interstate wars, and developing early warning models of large-scale violence against civilians. ▶ SITES.DARTMOUTH.EDU/VALENTINO

Professor Peter Winkler

Professor Peter Winkler is the William Morrill Professor of Mathematics and Computer Science. Professor Winkler’s research interests include: discrete mathematics and the theory of computing; probability theory and applications. ▶ MATH.DARTMOUTH.EDU/~PW/CV.PDF
“The ISTS was the highlight of my undergraduate academic experience at Dartmouth. At the Trust Lab, I met some of the smartest and most thoughtful members of the information security community, and was given the opportunity to work with world-class researchers on projects in healthcare and embedded systems security. I learned so much from my time at the ISTS; I would not be involved in Information Security today if not for my time there.” ~ Samuel Tan, Dartmouth Class of 2014

“The Dartmouth Cybersecurity Initiative, a collaboration of the Trust Lab and ISTS, allowed me to get rare hands-on experience with real problems on real systems while still in school. I continually look to hire people who have had similar experiences today.” ~ Ryan Spears, Co-Founder and Managing Partner, River Loop Security

“ISTS provides a critical link between industry and researchers to help solve society’s challenges in securing critical infrastructure. Researchers get access to real world problems in complex environments, and industry gets access to the latest theoretical thinking.” ~ Dave Safford, Senior Principal Engineer, GE Research

ists.dartmouth.edu

Email: info.ists@dartmouth.edu
LinkedIn.com/company/ists_dartmouth
Facebook.com/ists.dartmouth
Twitter.com/ists_dartmouth

SUDIKOFF LABORATORY . 9 MAYNARD STREET HANOVER, NH 03755 USA (603) 646-0700