UC BERKELEY

CENTER FOR LONG-TERM CYBERSECURITY

CENTER FOR LONG-TERM CYBERSECURITY
CYBERSECURITY FUTURES
2020
UNIVERSITY OF CALIFORNIA, BERKELEY
Center for Long-Term Cybersecurity

2017

ANNUAL REPORT

Contents

Initially funded through a generous grant from the William and Flora Hewlett Foundation, the Center for Long-Term Cybersecurity aims to be the world's premier research and collaboration hub dedicated to building secure digital futures. We build bridges between academic research communities, corporations, government policymakers/regulators, and civil society to envision solutions that enable the potential of digital technologies to advance and protect institutions, societies, and individuals.

Introduction

From the WannaCry virus and Equifax breach to revelations about election interference in the United States and Europe, 2017 provided nearly constant reminders about the challenge and importance of building a robust and secure world for the digital age. The past year also marked an important phase in the evolution of the UC Berkeley Center for Long-Term Cybersecurity (CLTC), as we have continued to grow and evolve in our mission to support more secure digital futures.

In 2017, we put additional building blocks in place for the Center to reach the next stage of capacity and influence. Key to that was obtaining and renovating a facility capable of housing about 30 people, for the first time allowing our core personnel and campus collaborators to work together in a shared space under one roof. We grew our staff this year, adding three CLTC researchers and two staff positions, which increased our capability both to invest in long-term projects and to respond to short-term opportunities. The Berkeley Master's Degree in Information and Cybersecurity received final approval and the first cohort of students will start in June 2018.

At the same time that we are laying a strong foundation for the future of the organization, we continued to work on the complex challenges of digital security through an integrated program of research, education, and external engagement. We allocated over $1 million in research funds; published white papers and pieces in the *New York Times* and *Washington Post*; helped get an amendment introduced to the National Defense Authorization Act; and launched our corporate membership program and external advisory committee. We remain convinced that the future of cybersecurity is one of the most important issues facing modern societies, and that the current social and political climate inside the United States adds greater urgency to our work both domestically and internationally. We have built a distinctive position as an academic research center that pays equal attention to scholarly research, policy, and corporate engagement; and we continue to develop our work under the proposition that these three ingredients—managed carefully—are compatible and synergistic.

This report reviews CLTC's accomplishments for 2017 and identifies short- and long-term goals for what lies ahead. (Please note that additional information about most of the initiatives outlined in this report—including publications—can be found at https://cltc.berkeley.edu.)

Steve Weber, Faculty Director
January 31, 2018

Betsy Cooper, Executive Director
January 31, 2018

We allocated over $1 million in research funds; published white papers and pieces in the *New York Times* and *Washington Post*; helped get an amendment introduced to the National Defense Authorization Act; and launched our corporate membership program and external advisory committee.

Research and Thought Leadership

Throughout 2017, CLTC made progress in advancing our research agenda and establishing our thought leadership on an array of issues related to cybersecurity.

BUILDING OUR RESEARCH CAPACITY

Over the past year, we focused on building out the "center of our center," i.e., growing our capacity through selective hires in four key priority research areas: machine learning and artificial intelligence, expanding the cybersecurity talent pool, exploring new regulatory and governance structures to support cybersecurity, and protecting vulnerable online populations. As detailed in our report last year, these topics were selected in part as a result of meetings with faculty members and external advisors. The fourth research area, which we added in 2017, aligns with our research initiative investigating cybersecurity resources supporting civil society, described in more detail below.

Throughout 2017, CLTC made progress in advancing our research agenda and establishing our thought leadership on an array of issues related to cybersecurity.

Early in 2017, we undertook a scoping process to determine how we could maximize our impact—through research and beyond—in these priority areas. We hired consultants to scope out possible future program priorities, complementing our own views with independent and unbiased perspectives. Brian Miller, Strategic Advisor at Public Sphere, focused on the cyber talent pipeline as a research focus; he investigated questions such as what structural factors contribute to a lack of diversity in the field and how a robust and adaptive cybersecurity workforce can grow. Charlotte Stanton, then an advisor at the AI For Good Foundation, assessed the impact that artificial intelligence and machine learning are likely to have on society and technology. Sean Brooks, who also joined CLTC as a research fellow, began investigating innovative solutions to cybersecurity governance, including (but not limited to) new institutions, incentive structures, and policy initiatives. In addition, Sean has been spearheading our efforts to establish a new program funded by the MacArthur Foundation that is focused on improving security and privacy for politically vulnerable individuals and organizations, such as journalists and political dissidents.

We continued adding to our research team in the second half of 2017: we hired Jessica Cussins, who was previously the AI policy lead at the Future of Life Institute, as a Research Fellow focused on artificial intelligence. We also hired Allison Davenport, a graduate of Pepperdine University School of Law and a licensed California attorney who will be conducting a variety of research tasks with the CLTC, with an initial focus on cybersecurity governance. Jonathan Reiber, Senior Research Fellow and (beginning in September 2017) Visiting Scholar with CLTC, also has been an active contributor in

Sean Brooks

Jessica Cussins

Allison Davenport

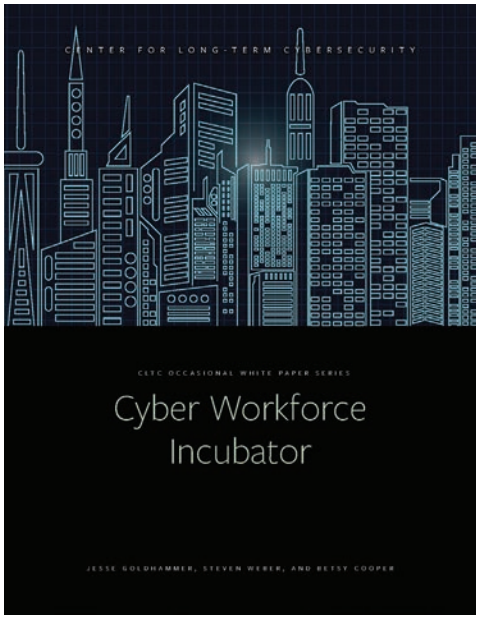
Jonathan Reiber

national and international forums related to cybersecurity and was the lead author of a new report detailing scenarios for the future of cybersecurity in Asia.

CLTC RESEARCH IMPACT

As CLTC's research staff has grown, so has our capacity to produce timely research outputs on important contemporary issues of cybersecurity. These efforts will expand in 2018 as our growing team of staff researchers begin to produce research outputs, and as we publish four white papers already in our queue, based on research done in 2017.

CYBER WORKFORCE INCUBATOR



CENTER FOR LONG-TERM CYBERSECURITY

CLTC OCCASIONAL WHITE PAPER SERIES

Cyber Workforce Incubator

JESSE GOLDHAMMER, STEVEN WEBER, AND BETSY COOPER

We published a white paper outlining the concept for the Cyber Workforce Incubator.

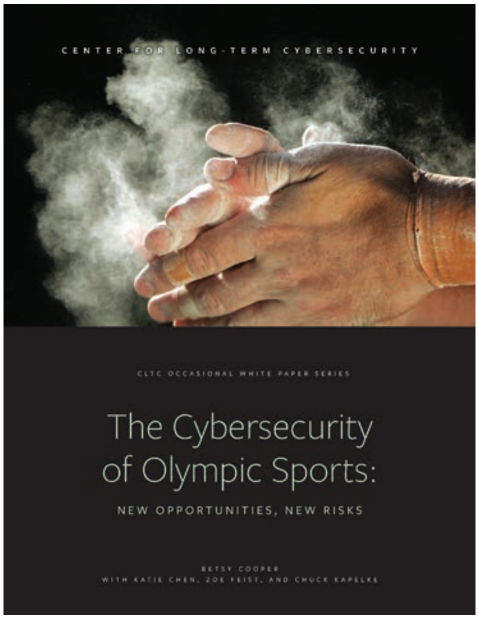
In April, Jesse Goldhammer, Senior Advisor for CLTC and Associate Dean for Business Development and Strategic Planning at the UC Berkeley School of Information, along with Faculty Director Steve Weber and Executive Director Betsy Cooper, published a white paper that outlines the workforce challenges facing the government, and details the opportunity to create a "Cyber Workforce Incubator" that could bridge industry and government by enabling top technologists from Silicon Valley to work for the federal government for one- or two-year terms. In addition to authoring the report, on April 4 the team submitted written testimony to the U.S. House of Representatives' Subcommittee on Information Technology (part of the Committee on Oversight and Government Reform); they expressed the need for the Cyber Workforce Incubator program to ensure that the Department of Defense and other agencies remain on the cutting edge of technology.

The proposal for a Cyber Workforce Incubator was featured in *The Hill*, a top U.S. political website, in an article called "Feds Face Big Obstacle in Cyber Efforts: Geography" that quoted both Weber and Cooper. In addition, Goldhammer published an op-ed in Lawfare Blog focused on the Cyber Workforce Incubator, and Cooper introduced the concept for this program at a public meeting of the

Defense Innovation Board, which is working to accelerate technology into the hands of the men and women in uniform. In the fall, Senator Kamala Harris introduced an amendment into the National Defense Authorization Act calling for a "Program on Integrating into the Department of Defense Workforce Individuals with Cybersecurity Skills Whose Services are Donated by Private Persons" based on the team's proposal. CLTC is working to have the amendment reintroduced in 2018.

CYBERSECURITY OF THE OLYMPIC GAMES

Throughout 2017, CLTC pursued research focused on a unique dimension of life in the digital age: the cybersecurity of major sporting events, with a focus on the Olympic Games. In May, Steve Weber and Betsy Cooper presented preliminary findings at the National Football League's security conference. The research culminated in October with the public release of "The Cybersecurity of Olympic Sports: New Opportunities, New Risks," a report investigating how the proliferation of new technologies in major sporting events—from digital display panels in stadiums to online ticketing systems to artificial intelligence-based scoring software—opens the door to cyberattacks that could threaten public safety, diminish the fan experience, and undermine the integrity of competition.



CENTER FOR LONG-TERM CYBERSECURITY

CLTC OCCASIONAL WHITE PAPER SERIES

The Cybersecurity of Olympic Sports:

NEW OPPORTUNITIES, NEW RISKS

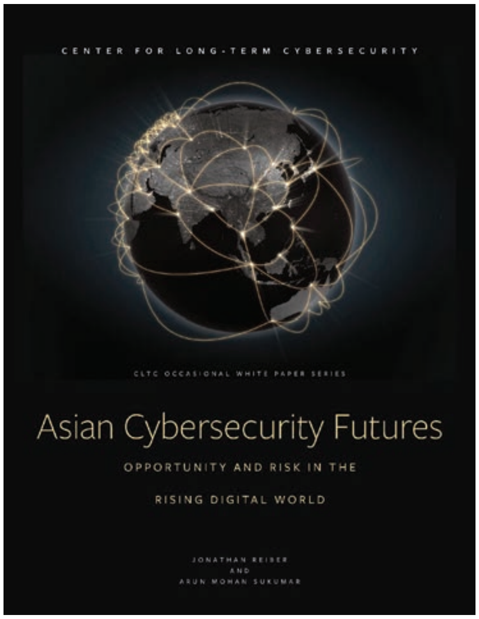
BETSY COOPER
WITH KATIE CHEN, ZOE FEIST, AND CHUCK KAPELKE

Our report on the cybersecurity of Olympic sports earned coverage from CNN, Politico, and other outlets.

To maximize the impact of this research, CLTC held a public event at Cal Stadium that included a panel with Missy Franklin, five-time Olympic medalist; Brian Nelson, General

We held a panel discussion that included Olympic gold medalist Missy Franklin and representatives from the Los Angeles 2028 Olympic Games.

Counsel for the 2028 Los Angeles Olympic Games; and Doug Arnot, Chairman of Broadstone Group, which manages security, traffic, and other logistical aspects of the Games. Both Nelson and Arnot commented that they expect to bring their findings back to inform their work in planning the Olympic Games in Los Angeles. In addition, the report garnered media attention from CNN, Politico, and a variety of international news outlets.



CENTER FOR LONG-TERM CYBERSECURITY

CLTC OCCASIONAL WHITE PAPER SERIES

Asian Cybersecurity Futures

OPPORTUNITY AND RISK IN THE RISING DIGITAL WORLD

JONATHAN REIBER
AND
ARUN MOHAN SUKUMAR

Jonathan Reiber's report explored possible futures for cybersecurity in Asia.

ASIAN CYBERSECURITY FUTURES

Since joining CLTC as a Senior Fellow in 2016, Jonathan Reiber has participated in multiple collaborations with researchers and industry officials in India and other Asian nations. In 2017, Reiber collaborated with a colleague—Arun Mohan Sukumar, head of the Technology, Society, and Security Program at the Observer Research Foundation in New Delhi—on research that led to the December release of an original report, "Asian Cybersecurity Futures: Opportunity and Risk in the Rising Digital World." This report explored diverse political, economic, and technological factors that will shape Asia's future as the region's citizens become more connected to the internet.

CLTC ACADEMIC PUBLICATIONS

In addition to publishing white papers and policy briefs, CLTC staff continue to publish academic articles in peer-reviewed publications. For example:

- In February, Steve Weber, together with Richmond Wong, a Ph.D. student in the UC Berkeley School of Information and 2018 CLTC grantee, published an essay on **First Monday**, a peer-reviewed online journal, entitled "The New World of Data: Four Provocations on the Internet of Things."

- In February, Weber, together with Jesse Goldhammer and Nils Gilman, then Associate Chancellor at UC Berkeley, published an article in **Limn**, an online scholarly journal/magazine, focused on the 2014–2015 hacks on the Office of Personnel Management (OPM).

- In April, Weber published a paper in **Business and Politics**, a journal by Cambridge University Press, entitled "Data, Development, and Growth." In the paper, Weber argued that the flow of data across borders is now a critical dimension of economic growth and development, with characteristics distinctive from flows of goods, ideas, and money.

- Weber also published a paper in the **Journal of Cybersecurity** addressing the commonly used analogy comparing cybersecurity and public health, explaining in the essay's abstract that "analogies between public health and cybersecurity are superficially appealing but fail on closer examination in two distinct ways: the 'publicness' of the goods in question, and the readiness of the relevant actors and institutions to exert and accept coercive authority."

- In October, Betsy Cooper and Weber published "Moving Slowly, Not Breaking Enough: Trump's Cybersecurity Accomplishments" in the **Bulletin of the Atomic Scientists**, which argued that the Trump administration has been slow to take action on cybersecurity—but there are still many opportunities for federally funded initiatives that could have a major near- and long-term impact in protecting our nation's digital infrastructure.

CYBERSECURITY RESOURCES FOR CIVIL SOCIETY

CLTC also received a grant from the MacArthur Foundation to explore how civil society organizations seek to secure themselves online, and to understand the landscape of existing resources available to support them. Our preliminary findings have illustrated significant gaps in the availability and sophistication of assistance to at-risk organizations, particularly those targeted for political purposes by governments or other powerful interests. CLTC has reviewed the work of more than 100 organizations providing assistance in this space, and interviewed a broad range of subject-matter experts to understand the strengths and gaps in the ecosystem of cybersecurity support for civil society, and to catalog the online threat landscape that has emerged for organizations who speak truth to power. The work culminated in a closed-door workshop with key stakeholders in October 2017. We plan to publish a white paper on the results of this work, and are also considering options about how we might best move forward with a new initiative in this space in 2018.

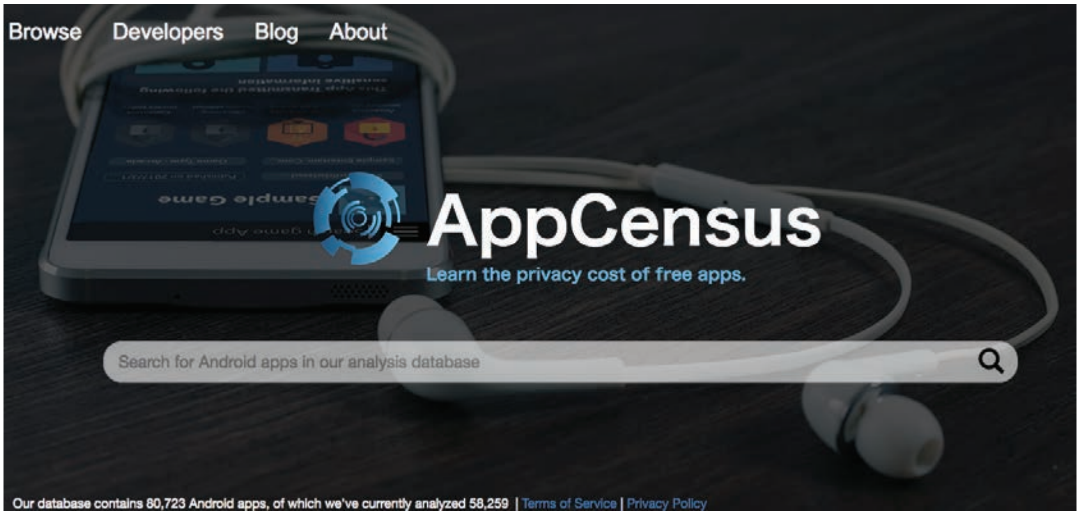
CAMPUS GRANTMAKING

In early 2017, we allocated over $1 million in funding to 28 different research initiatives. The winning proposals were chosen through review by a campus cross-disciplinary committee. Two types of grants were given: seed grants, generally below $15,000, for exploratory studies, and discrete project grants of up to $100,000, for projects with clear expected outcomes and impact potential.

The purpose of our research funding is not only to address the most interesting and complex challenges of today's socio-technical security environment, but also to grapple with the broader challenges of the next decade's environment.

The purpose of our research funding is not only to address the most interesting and complex challenges of today's socio-technical security environment, but also to grapple with the broader challenges of the next decade's environment. For example, one sponsored team is exploring a new method, based on deep neural networks, for detecting fake or manipulated videos. Another group, led by researchers from UC Berkeley's Human Rights Center, is working to identify what protocols can be put in place to protect the security of activists, legal practitioners, and human rights abuse victims as their cases are being investigated.

Below are some examples of achievements by CLTC-funded researchers that were recognized publicly in 2017:


Browse
Developers
Blog
About
AppCensus
Learn the privacy cost of free apps.
Search for Android apps in our analysis database

Our database contains 80,723 Android apps, of which we've currently analyzed 58,259 | Terms of Service | Privacy Policy

CLTC grantees developed a website to help identify apps that may violate the Children's Online Privacy Protection Act (COPPA).

- A group of researchers received the prestigious Internet Defense Prize—a $100,000 prize funded by Facebook—for their academic research on detecting spearphishing attacks. The paper's authors were Grant Ho, UC Berkeley; Aashish Sharma, Lawrence Berkeley National Laboratory; Mobin Javed, UC Berkeley; Vern Paxson, UC Berkeley and ICSI; and David Wagner, UC Berkeley. In addition, a system based on these researchers' work was implemented and deployed at Lawrence Berkeley National Labs and is now in use to defend against spearphishing attacks.
- Led by Serge Egelman, a team of CLTC-funded researchers from the Usable Security & Privacy group at the International Computer Science Institute (ICSI) discovered that more than 50 percent of Android apps targeted at children under 13 appear to be failing to protect data, in violation of the Children's Online Privacy Protection Act (COPPA). The researchers developed a website, AppCensus, that shows the privacy behaviors of the apps they tested. With CLTC's support, Egelman wrote an op-ed about this study that was published by "The Switch," a digital outlet of the *Washington Post*. At least one of the app developers responsible signaled it would change its practices as a result, and the study brought the issue to the attention of state and federal authorities, who in some cases have begun using the research team's tools for their investigations.
- A CLTC-funded initiative focused on improving the privacy of SQL queries was adopted for use by Uber, which received coverage in *Wired* magazine. The researchers, Professor Dawn Song, Postdoctoral Researcher Joseph Near, and Graduate Student Researcher Noah Johnson, received funding for a project focused on differential privacy, which enables general statistical analysis of data while providing individuals with a strong formal guarantee of privacy.

Ashwin Jacob Mathew was among the grantees who presented at our Research Exchange.

- Following the massive data breach at Equifax, many critics pointed out that one of the company's female security executives had a degree in music composition, suggesting she was unqualified. But an article in *Engadget*, "Why Equifax's error wasn't hiring someone with a music degree," cited research by grantees Coye Cheshire and Ashwin Mathew showing that most information security professionals do not hold a degree in a computer-science-related field—and that "degrees are the least important feature of a competent practitioner and degree programs are the least useful places to learn security skills."
- CLTC grantee Bill Marczak was among the experts who helped confirm the presence of the Pegasus malware on several phones belonging to Mexican journalists and activists. *The New York Times* profiled the research of Marczak in an article entitled "Using Texts as Lures, Government Spyware Targets Mexican Activists and Their Families," which spotlighted the use of spyware against human rights lawyers, journalists, and anti-corruption activists in Mexico.
- CLTC grantee Benjamin Jensen co-authored a piece on the *Washington Post's* "Monkey Cage" entitled, "Cyberwarfare has taken a new turn. Yes, it's time to worry." Together with Brandon Valeriano and Ryan C. Maness, Jensen, Associate Professor at Marine Corps University and Scholar-in-Residence at American University, argued that ransomware attacks represented "disruptive cyber-actions—with the apparent goals of signaling capability, disrupting normal systems and demonstrating the instability of Western democratic models." Jensen also published a piece for Monkey Cage entitled, "Five Things We Can Learn from the Russian Hacking Scandal."

RESEARCH AND THOUGHT LEADERSHIP GOALS

Goals for 2020

Develop a multi-disciplinary research and impact agenda that is directed by a vision of long-term cybersecurity, and engage in areas that emerge on an opportunistic basis where we feel we can have a distinctive or outside impact. This includes:

1) Supporting and facilitating UC Berkeley researchers in pursuing that agenda, including by strengthening the internal UC Berkeley community of researchers with an interest in cybersecurity and the digital environment; and

2) Hiring internal researchers to sit within CLTC's 'core' to pursue elements of that agenda.

Interim Goals for 2018

- Hire team members to lead on our priority research areas
- Convene at least two opportunities for CLTC grantees to share their research
- Support grantees with placing op-eds and/or receiving media coverage
- Select 2019 grantees

2017 REQUEST FOR PROPOSALS

In August 2017, we announced our third annual Request for Proposals. We received more than 50 proposals, of which 35 (including 13 renewals) were chosen to receive funding in December 2017. We publicly announced the successful projects and distributed the funding in January 2018.

CLTC 2018 GRANTEES

BELOW IS A LIST OF THE PROJECTS FUNDED BY THE CENTER FOR LONG-TERM CYBERSECURITY THROUGH OUR 2017 RESEARCH GRANT PROCESS.

- **Advanced Encryption Technologies for the Internet of Things and Data Storage Systems** | Sanjam Garg, Assistant Professor, UC Berkeley Department of Electrical Engineering and Computer Science (EECS); Daniel Masny, Postdoctoral Researcher, EECS
- **Building Decentralized Contract Systems with Strong Privacy** | Alessandro Chiesa, Professor, EECS
- **Cybersecurity Awareness for Vulnerable Populations** | Ahmad Sultan, Master of Public Policy Candidate, Goldman School of Public Policy, UC Berkeley
- **Cybersecurity Toolkits of/for the Future: A Human-Centered and Design Research Approach** | James Pierce, Adjunct Faculty, Jacobs Institute for Design Innovation, UC Berkeley; Sarah Fox, PhD Candidate, Tactile and Tactical (TAT) Design Lab, University of Washington; Richmond Wong, PhD Student, UC Berkeley School of Information; Nick Merrill, PhD Candidate, UC Berkeley School of Information
- **Deep Fairness in Classification** | Matt Olfat, PhD Student, Industrial Engineering and Operations Research Department (IEOR), UC Berkeley; Anil Aswani, Assistant Professor, IEOR
- **Enhancing Security Using Deep Learning Techniques** | Dawn Song, Professor, EECS; Chang Liu, Postdoctoral Scholar, UC Berkeley
- **Human-Centric Research on Mobile Sensing and Co-Robotics: Developing Cybersecurity Awareness and Curricular Materials** | Alice M. Agogino, Roscoe and Elizabeth Hughes Professor of Mechanical Engineering and Education Director of the Blum Center for Developing Economies; Euiyoung Kim, Postdoctoral Design Fellow, Jacobs Institute for Design Innovation in the Department of Mechanical Engineering, UC Berkeley; Matilde Bisballe Jensen, PhD Candidate, Norwegian University of Science & Technology (NTNU)
- **Malpractice, Malice, and Accountability in Machine Learning** | Joshua Kroll, Postdoctoral Research Scholar, UC Berkeley School of Information; Nitin Kohli, PhD Student, UC Berkeley School of Information
- **The Mice that Roar: Small States and the Pursuit of National Defense in Cyberspace** | Melissa K. Griffith, PhD Candidate, Department of Political Science, UC Berkeley
- **Model Agnostic Estimation of Threat Probabilities** | Venkatachalam Anantharam, EECS
- **Post and Re-trauma: Enhancing the Cybersecurity of Sexual Assault Victims on Facebook** | Hadar Dancig-Rosenberg, Associate Professor, Bar-Ilan University Faculty of Law, Visiting Professor, Berkeley Institute for Jewish Law and Israel Studies; Anat Peleg, Lecturer, Faculty of Law and Director of the Center for the Study of Law, Media, Bar-Ilan University; Roy Rosenberg, Senior Partner and Director, Economic Regulation Department, Ascola Economic and Financial Consulting LTD
- **Privacy Analysis at Scale: A Study of COPPA Compliance** | Serge Egelman, Director, Usable Security & Privacy Group, International Computer Science Institute (ICSI); Irwin Reyes, Researcher, ICSI; Primal Wijesekera, PhD Candidate, Department of Electrical and Computer Engineering, University of British Columbia; Amit Elazari, Doctoral Law Candidate, UC Berkeley School of Law, CTSP Fellow, UC Berkeley School of Information

Continued on following page.

- **Privacy Localism Conference Travel Grant Proposal** | Ahmad Sultan, Master of Public Policy Candidate, Goldman School of Public Policy, UC Berkeley
- **Probing the Ambivalence of Facial Recognition Technologies in China: An Ethnographic Study of Megvii** | Michael Kowen, PhD Student, Department of Sociology, UC Berkeley
- **Repercussions of Cyber-Security Measures in U.S. High Schools** | Anne Jonas, PhD Student, UC Berkeley School of Information
- **Responding to Emerging Protection Threats in Cyberspace** | Alexa Koenig, Executive Director, Human Rights Center; Joseph Guay, Associate, The Policy Lab; Lisa Rudnick, Principal and Founding Partner, The Policy Lab; Leeor Levy, Principal, The Policy Lab
- **Ride Free or Die: Overcoming Collective Action Problems in Autonomous Driving Governance** | Deirdre K. Mulligan, Associate Professor, School of Information, UC Berkeley, Faculty Director, Berkeley Center for Law & Technology; Adam Hill, Government Information Specialist, USDA FSIS
- **The Role of Private Ordering in Cybersecurity: Towards A Cybersecurity License** | Amit Elazari, Doctoral Law Candidate, UC Berkeley School of Law; Research Fellow, CTSP, UC Berkeley School of Information
- **Secure Internet of Things for Senior Users** | Alisa Frik, Postdoctoral Fellow, ICSI; Serge Egelman, ICSI; Florian Schaub, Assistant Professor, University of Michigan School of Information; Joyce Lee, Masters Degree Candidate, UC Berkeley
- **Security Implications of 5G Networks** | Jon Metzler, Lecturer, Haas School of Business, Associated Faculty, Center for Japanese Studies, UC Berkeley
- **Statistical Foundations to Advance Provably Private Algorithms** | Paul Laskowski, Adjunct Assistant Professor, UC Berkeley School of Information
- **Uncovering the Risk Networks of Third-Party Data Sharing in China’s Social Credit System** | Shazeda Ahmed, PhD Student, UC Berkeley School of Information

PROJECTS JOINTLY FUNDED WITH THE CENTER FOR TECHNOLOGY, SOCIETY & POLICY

- **Everyone Can Code? Race, Gender, and the American Learn to Code Discourse** | Kate Miltner, PhD Candidate, USC Annenberg School for Communication and Journalism, Visiting Student Researcher, UC Berkeley Center for Science, Technology, Medicine, & Society
- **Menstrual Biosensing Survival Guide** | Noura Howell, PhD Student, UC Berkeley School of Information; Sarah Fox, PhD candidate, University of Washington, Visiting Scholar, EECS; Richmond Wong, PhD Student, UC Berkeley School of Information

RENEWED PROJECTS

- **Addressing the Privacy Gaps in Healthcare** | Ruzena Bajcsy, Professor, EECS; Daniel Aranki, PhD Candidate, EECS
- **Adversarially Robust Machine Learning** | Sadia Afroz, Research Scientist, ICSI
- **Allegro: A Framework for Practical Differential Privacy of SQL Queries** | Dawn Song, Professor, EECS; Joseph Near, Postdoctoral Researcher, EECS
- **Defense Against Social Engineering Attacks** | David Wagner, Professor, EECS; Vern Paxson, Professor, EECS, and Director, Networking and Security Group, ICSI
- **Exploring Internet Balkanization through the Lens of Regional Discrimination** | Jenna Burrell, Associate Professor, UC Berkeley School of Information; Anne Jonas, PhD Student, UC Berkeley School of Information
- **Identifying Audio-Video Manipulation by Detecting Temporal Anomalies** | Alexei Efros, Associate Professor, EECS, and Andrew Owens, Postdoctoral Scholar, EECS
- **Illuminating and Defending Against Targeted Government Surveillance of Activists** | Vern Paxson, Professor, EECS, and Director, Networking and Security Group, ICSI; Bill Marczak, Postdoctoral Researcher, UC Berkeley
- **The International Coordination of Cybersecurity Industrial Policies** | Vinod Aggarwal, Senior Faculty Fellow and Professor, UC Berkeley Department of Political Science; Andrew Reddie, PhD Candidate, UC Berkeley Department of Political Science
- **NilDB: Computing on Encrypted Databases with No Information Leakage** | Alessandro Chiesa, Assistant Professor, EECS; Raluca Ada Popa, Assistant Professor, EECS
- **Secure Machine Learning** | David Wagner, Professor, EECS; Michael McCoyd, PhD Student, EECS; Nicholas Carlini, PhD Student, EECS
- **The Security Behavior Observatory** | Serge Egelman, Director, Usable Security & Privacy Group, ICSI; Alessandro Acquisti, Professor of Information Technology and Public Policy, Heinz College, Carnegie Mellon University (CMU); Lorrie Faith Cranor, Professor of Computer Science and of Engineering and Public Policy, CMU; Nicolas Christin, Assistant Research Professor in Electrical and Computer Engineering, CMU; Rahul Telang, Professor of Information Systems and Management, Heinz College, CMU
- **Stakeholder Workshop on Deterring Financially Motivated Cybercrime** | Chris Hoofnagle, Adjunct Full Professor, School of Information and School of Law, UC Berkeley; Aniket Kesari, JD/PhD Student, UC Berkeley School of Law; Damon McCoy, Assistant Professor, New York University
- **User Authentication Using Custom-Fit Ear EEG** | John Chuang, Professor, UC Berkeley School of Information

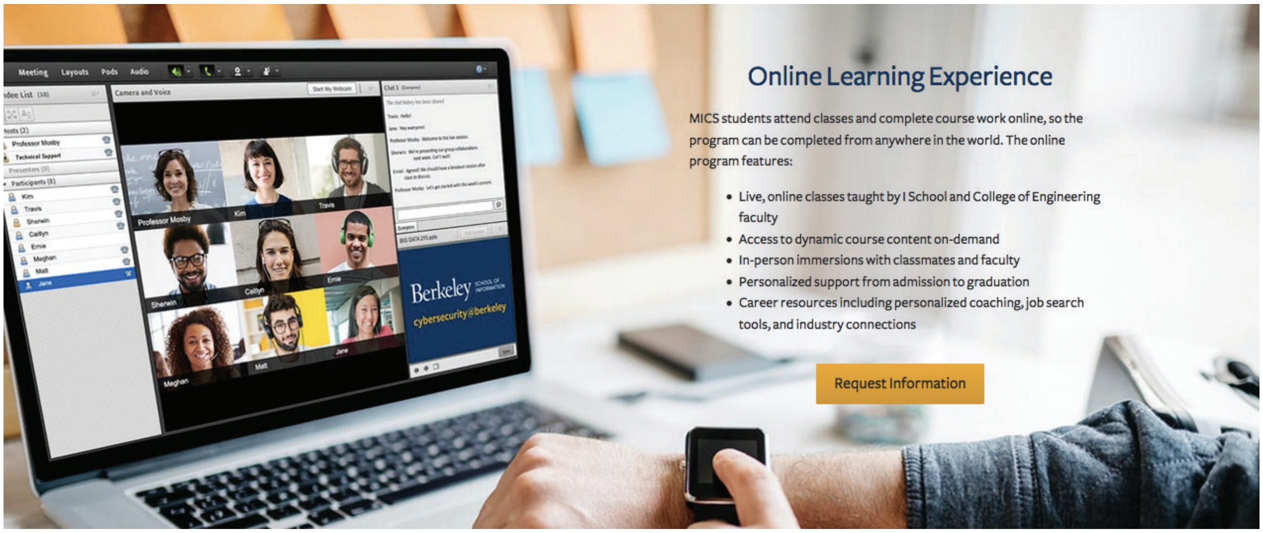
- With support from CLTC, grantees Michael Nacht and Charalampos Andreades published an op-ed in *The Hill* arguing that greater cybersecurity protections are needed to safeguard America's nuclear power infrastructure. The op-ed was grounded in a research report published by the team entitled "When to Avoid Digital Control: A Cybersecurity Case Study for Advanced Nuclear Reactors."
- In an article entitled "Antidote to Fake News: The Investigations Lab Teaches Digital Skepticism," *California Magazine* profiled CLTC Grantee Alexa Koenig and her colleagues at UC Berkeley Human Rights Center's Investigation Lab at Berkeley Law. The Investigation Lab is working to verify open-source material found on social media so that it can be used in prosecutions of war crimes and other crimes.

CLTC plays a key role in building a community of cybersecurity researchers at UC Berkeley and beyond, and in 2017 we broadened the scope of our grantee engagement.

CLTC plays a key role in building a community of cybersecurity researchers at UC Berkeley and beyond, and in 2017 we broadened the scope of our grantee engagement. We held a reception for our grantees on April 4 to celebrate their accomplishments and create opportunities for networking; in May, we hosted our bi-annual CLTC Faculty Lunch; and in September, we hosted our first annual Research Exchange, a day-long event held at the David Brower Center that created an opportunity for 2016 grantees to showcase their research projects. One of the main goals of the event was to connect members of the CLTC research community with private-sector partners, as well as public policymakers. Among those in attendance were representatives from Symantec, Kaiser, and Tanium, several of CLTC's Corporate Partners, as well as Rep. Mike Honda, who served in Congress between 2000–2017 (representing Silicon Valley in his final term). We received extremely positive feedback about this event, and CLTC will continue to provide networking and outreach opportunities for our grantees in 2018 and beyond.

Education

CLTC is committed to providing educational opportunities and programming to students on the UC Berkeley campus, as well as addressing the cybersecurity talent pipeline problem more broadly. Following is an overview of our 2017 activities in this space.



Online Learning Experience

MICS students attend classes and complete course work online, so the program can be completed from anywhere in the world. The online program features:

- Live, online classes taught by I School and College of Engineering faculty
- Access to dynamic course content on-demand
- In-person immersions with classmates and faculty
- Personalized support from admission to graduation
- Career resources including personalized coaching, job search tools, and industry connections

CLTC helped the UC Berkeley School of Information launch a new Master of Information and Cybersecurity (MICS) degree program.

CYBERSECURITY@BERKELEY: MASTER OF INFORMATION AND CYBERSECURITY (MICS) DEGREE

2017 saw an important landmark in UC Berkeley's efforts to develop a pipeline for future cybersecurity talent, as the School of Information formally announced "cybersecurity@berkeley," a new Master of Information and Cybersecurity (MICS) online degree program that will be taught by UC Berkeley faculty members. The new program, developed in partnership with the College of Engineering and in collaboration with CLTC, consists of 27 credit hours with courses focusing on both the technical and interdisciplinary aspects of cybersecurity, including cryptography, secure programming, and web security. MICS students will interact with faculty, network with other students, and gain exposure to applied research through live online classes and real-world immersion experiences. By teaching students online, the School of Information has the ability to scale the program, as it has with its companion Master of Information and Data Science program, to a greater number of students than could be accommodated on campus. The online degree program also provides added flexibility for mid-career professionals.

TEACHING AND SEMINARS

CLTC continues to enhance and lead other cybersecurity education opportunities both on and off the UC Berkeley campus, as a way of mobilizing, motivating, and training the next generation of students who will be working in the cybersecurity field. During the Spring and Fall 2017 semesters, CLTC sponsored and ran “Info 290: Future of Cybersecurity Policy Reading Group,” a one-credit reading group in which students discussed contemporary cybersecurity policy problems. Taught by Betsy Cooper and Chris Hoofnagle, CLTC Grantee and Adjunct Professor at the School of Information, the seminar focused on future trends in technology, as well as how the economy and politics shape cybersecurity policy. Approximately 25 students attended weekly 50-minute sessions; they presented and wrote papers in response to readings that included books, policy papers, essays, academic research articles, and more.

The Center has also focused on promoting cybersecurity education at UC Berkeley through our popular Seminar Series, which in 2017 brought a range of outstanding speakers from government, academia, and the private sector.

The Center has also focused on promoting cybersecurity education at UC Berkeley through our popular Seminar Series, which in 2017 brought a range of outstanding speakers from government, academia, and the private sector. CLTC seminars are open to the public and typically include lunch; each of our seminars attracted between 25–150 attendees, and followed a standard structure that included a presentation followed by a question and answer session. CLTC is committed to making these events as accessible as possible through livestreaming and social media engagement. Presenters in our Spring Seminar Series (February–May 2017) included the following:

MIKKO HYPPONEN, a globally renowned expert who serves as Chief Research Officer of F-Secure, a European cybersecurity firm, spoke on “Fighting Organized Online Crime,” which examined major hacking cases with background on the investigations behind them.

GILAD ROSNER, founder of the Internet of Things Privacy Forum, spoke on “The Intimacy of Things: Privacy and the IoT,” looking at conceptions of the IoT, the privacy risks it implies, relevant policy frameworks, and other questions.

EMILY REID, a cybersecurity professional who formerly served as Director of Education at Girls Who Code, spoke on “The Cybersecurity Pipeline . . . Or How I Learned to Start Worrying and Love a Chicken and Egg Problem.” She discussed the challenges and potential solutions related to reducing the gender gap in cybersecurity and other tech fields.

Seminar speakers (left to right): Emily Reid, Ron Deibert, Tom Lowenthal, Ignacio Arnaldo, Sean Zadig, Camille Francois, and David Sanger

RON DEIBERT, Professor of Political Science and Director of the Citizen Lab at the Munk School of Global Affairs, University of Toronto, delivered a presentation entitled, “Cyber Espionage and Civil Society: A Silent Epidemic.” He outlined recent targeted attacks on civil society, including what those attacks look like and what might be done to mitigate them.

TOM LOWENTHAL, Staff Technologist for the Committee to Protect Journalists, delivered a talk entitled “Won’t Somebody Think of the Journalists?” A technologist and an activist who specializes in operational security and grassroots surveillance self-defense, Lowenthal outlined the importance of broad security and privacy protections in today’s media landscape.

IGNACIO ARNALDO, Chief Data Scientist at PatternEx, an artificial intelligence platform for information security, presented “AI for Enterprise Security: The Challenges From a Data Scientist’s Perspective,” an overview of how machine learning can support cybersecurity.

EDUCATION

Goals for 2020

Create a world-renowned educational program for UC Berkeley cybersecurity students.

Interim Goals for 2018:

- Successfully launch the first cohort of the MICS degree program
- Pilot the women and minorities technical training, and continue to support diversity in cybersecurity education

Our Fall Seminar Series focused on presentations aligned around a key theme: "Cybersecurity and Democracy: The Shifting Implications of Citizenship in the Digital Age." Featured presenters included the following:

SEAN ZADIG, Director, Oath (Yahoo) Threat Investigations, focused on the sophisticated (often state-sponsored) cybersecurity threats that today's institutions face, and provided an overview of how modern organizations can proactively defend themselves and their users.

DAVID DILL, Donald E. Knuth Professor in the School of Engineering and Professor of Computer Science and Electrical Engineering at Stanford University, presented on "Voting Computer Security in the Age of Cyber War," describing the potential risks of electronic tampering with election outcomes in the U.S., as well as defenses that can be put in place.

DAVID SANGER, National Security Correspondent for the *New York Times*, spoke about the decades-long evolution that ultimately led to the Russian hacks on the U.S. election in 2016, and explored the implications of those attacks for our national security and democracy. More than 150 people attended the Sanger seminar, our highest turnout to date.

CAMILLE FRANCOIS, Principal Researcher for Jigsaw/Google and an affiliate at the Berkman Center for Internet & Society, presented "Paths to Cyber Peace: Protecting Human Rights and Democracy in an Age of Cyber Conflict," which asked what the rise of powerful, state-sponsored "cyber weapons" could mean for citizens and democracies around the world.

SUPPORTING DIVERSITY IN THE FIELD

CLTC is committed to increasing diversity within the field by supporting curriculum development and programming for women, minorities, and other underrepresented groups in cybersecurity.

With support from Facebook and Kaiser Permanente, CLTC is developing a one-day technical workshop for women and underrepresented minorities in cybersecurity. Consultant Emily Reid is working with us to create a curriculum around fundamental technical concepts that will engage mid-career professionals who wish to lateral into the field. We expect to launch the final product in the spring of 2018.

In September 2017, CLTC co-hosted the "Towards Inclusive Tech" conference, in collaboration with UC Berkeley's School of Information and the Center

Women in Tech:
A Symposium on Innovation & Entrepreneurship
November 30th, 2017
UC Santa Cruz Silicon Valley Cam
Santa Clara, CA
WOMEN IN TECH INITIATIVE UNIVERSITY OF CALIFORNIA
CITRIS BANATAO INSTITUTE
Berkeley ENGINEERING
CLTC

We sponsored the Women in Tech Symposium as part of our efforts to support diversity in the field.

To move diversity in tech forward, #IPledgeTo
teach women + under-represented groups the vocabulary of Cybersecurity
#WomenInTech

CLTC Executive Director Betsy Cooper introduced the keynote speaker at "Women in Tech."

for Gender, Equity, and Leadership at Berkeley's Haas School of Business. This conference brought together leaders from the business, non-profit, and academic communities to identify the most promising research, business, and educational practices that will advance diversity and inclusion in the technology sector. Keynote speakers included Aubrey Blanche, Global Head of Diversity & Inclusion for Atlassian, and Prudence Carter, Dean of the UC Berkeley Graduate School of Education. CLTC also co-sponsored "Women In Tech: A Symposium On Innovation & Entrepreneurship," a public event that highlighted the experience of women in the tech industry.

Collaboration and Strategic Communication

CLTC continually strives to connect our research and education initiatives with the public, both domestically and internationally, and to serve as a convener of dialogue across government, academia, and the private sector. We approach collaboration through three categories: domestic collaboration, international collaboration, and strategic communications. In carefully selected situations where these are insufficient, we are also committed to undertaking direct action (for instance, through policy advocacy) to achieve our aims.

DOMESTIC COLLABORATION

Throughout 2017, CLTC undertook a wide range of efforts focused on promoting collaboration with other organizations and institutions addressing issues related to cybersecurity. These engagements helped to raise the profile of the Center and build a network of individuals we can draw upon for our programming and research initiatives.

Examples of our domestic engagements throughout the year include:

In January, Steve Weber and Betsy Cooper presented the "Cybersecurity Futures 2020" scenarios report at an event hosted by Stanford's Center for International Security and Cooperation (CISAC) and Freeman Spogli Institute for International Studies.

In January, CLTC hosted a workshop on "active defense" in conjunction with the Carnegie Endowment for International Peace. The workshop brought together a group of industry partners working across platforms and technologies to discuss a working paper authored by Wyatt Hoffman and Ariel Levite. The report, *Private Sector Cyber Defense: Can Active Measures Help Stabilize Cyberspace?*, was released in June. Steve Weber moderated the discussion.

In February, CLTC hosted a meeting of Privacy Lab, a Bay Area group dedicated to encouraging dialogue about issues related to digital privacy. The meeting included an overview of our Cybersecurity Futures 2020 Scenarios, as well as brief presentations by several CLTC research grantees, including Richmond Wong, Laurin Weissinger, Elaine Sedenberg, Sadia Afroz, Serge Egelman, and Jen King.

In March, we convened a workshop with David Robinson of Upturn, co-author of "Accountable Algorithms," a law review article that parses the risks and opportunities associated with using machine learning tools in the criminal justice system. CLTC-affiliated faculty and grantees gathered for a deep-dive conversation.

Also in March, we partnered with the EastWest Institute to host the Global Cyberspace Cooperation Summit VII. This event brought together more than 200 leading policymakers, business leaders, and technical experts from over 30 countries

Martin Giles, now of the MIT Technology Review, and former Congressman Mike Honda, on a panel co-hosted with the Center for Strategic and International Studies (CSIS).

to discuss and find policy solutions concerning the most pressing security issues in international cyberspace. Featured speakers included Peter Altabef, President and CEO of Unisys; Marina Kaljurand, former Foreign Minister of Estonia and Chair of the Global Commission on the Stability of Cyberspace; and Francis Fukuyama, Senior Fellow at Stanford's Freeman Spogli Institute.

On April 11, CLTC hosted a panel of technology experts—including members of the Center for Strategic and International Studies (CSIS) Cyber Policy Task Force—to discuss recommendations for the Trump administration. The event included two discussion panels, one featuring members of the CSIS Task Force's West Coast Cohort, and another that convened discussants from across sectors. Held at Berkeley's Bancroft Hotel, panelists included Sameer Bhalotra, Co-founder and CEO at StackRox; Nils Gilman, Associate Chancellor, UC Berkeley; Davis Hake, Adjunct Fellow at CSIS; Martin Giles, Partner at Wing Venture Capital; Former Congressman Mike Honda; Ellen Richey, Vice Chairman, Risk & Public Policy for Visa Inc.; Chris Riley, Head of Public Policy at Mozilla; and Nico Sell, Co-founder and CEO of Wickr. The panel covered some of the far-reaching challenges facing decision-makers as they implement cybersecurity policy, including the need to balance the responsibilities of the public and private sectors, work with companies to encourage strong privacy for consumers, and understand the motivations of foreign nation-states in the shared task of establishing standards.

In June, Betsy Cooper spoke on a panel at the World Economic Forum's Industry Strategy Meeting, held in San Francisco. Her panel, "Catch Me If You Can: Future-Proofing Tomorrow's Economy," tackled the question, "How can business work with government to anticipate and shape the social, political, and economic impacts of the Fourth Industrial Revolution?"

In June, Steve Weber delivered a keynote at the 2017 Cloud Identity Summit, in Chicago. In his presentation, titled "On Matters of Identity and Security," Dr. Weber and IBM veteran Irving Wadlawsky-Berger discussed the past, present, and future of digital identity and security.

In July, House Democrats introduced the "New Collar Jobs Act," which would increase funding for cyber scholarships and introduce tax breaks for companies providing cybersecurity training; it would also provide student debt relief for graduates entering the cybersecurity workforce—an idea that CLTC had presented in our 2016 report on *Cybersecurity Policy Ideas for the New Presidency*.

Throughout 2017, CLTC undertook a wide range of efforts focused on promoting collaboration with other organizations and institutions addressing issues related to cybersecurity.

In July, when the National Institute of Standards and Technology (NIST) issued a request for information (RFI) to gain public input about how to educate and train a new generation of cybersecurity professionals, CLTC responded with a letter outlining a variety of ideas and recommendations. Our letter encouraged lawmakers to explore "policy solutions that may not reflect the traditional way that things are done within the Beltway," and highlighted diverse approaches the government could take in key areas outlined in the RFI, including research, metrics, and data; education; and policy solutions.

On October 19, NIST hosted the IoT Cybersecurity Colloquium to convene stakeholders from across government, industry, international bodies, and academia. CLTC visiting scholar Gilad Rosner, founder of the Internet of Things Privacy Forum, spoke on the IoT privacy threat landscape and offered a preview of work to come.

In November, Betsy Cooper led a session at the annual Techonomy conference titled, "The Cybersecurity of Sports: How Technology Interferes With Game Integrity and Fan Safety." Cooper discussed myriad ways that new technologies are challenging the security of sports and integrity of the game, drawing from our latest report.

CLTC Executive Director Betsy Cooper at the World Economic Forum Industry Strategy Meeting 2017

INTERNATIONAL COLLABORATION

CLTC has also pursued thoughtful international collaborations in keeping with our research priorities. Most prominently, throughout the year, we worked alongside the World Economic Forum (WEF) for a project focused on the "Future of Cybersecurity." We partnered with the WEF's Global Future Council on Cybersecurity to develop a set of scenarios that portray a landscape of 'cybersecurity futures' designed to stress and stretch trade-offs in objectives and values that will appear in the near future.

- Phase I of this project, completed in 2017, involved developing a set of core scenario prompts, designed to elicit meaningfully different points of view in different parts of the world about the future of cybersecurity.
- Phase II of this project will involve taking these scenarios to 3–5 workshop locations around the world, to potentially include Singapore, London, Dubai, and Washington, DC, in 2018. The goal of the workshops is to elicit fundamental differences in how people parse, think about, evaluate, and develop potential responses to the kinds of challenges that the scenarios portray. What choices need to be made? What values do the scenarios invoke most intensely? How would the world be seen from a risk and opportunity perspective?

COLLABORATION GOALS

Goals for 2020

- Domestic Collaboration: Identify a handful of key government and private-sector strategic partners and develop a concrete agenda for joint, high-impact projects in areas of our research and impact agenda.
- International Collaboration: Establish selective key 'nodes' of international cooperation in our core areas of impact, with ongoing research projects and a strong agenda for partnership.

Interim Goals for 2018

- Continue to identify strategic partnerships in our newly identified priority areas (artificial intelligence and machine learning; cyber talent pipeline; governance regimes; protecting vulnerable people online) and develop those partnerships to be productive and mutually beneficial

Laurin Weissinger

Frank Smith

CLTC participated in other international engagements as well. In June, CLTC Faculty Director Steve Weber spoke at the academic component of Cyber Week, an annual cybersecurity conference held at Tel Aviv University, in Israel. UC Berkeley Professor and CLTC Affiliated Faculty Member Dawn Song also presented at this conference, speaking on a panel about research and development in artificial intelligence. The Cyber Week conference featured prominent speakers like Israeli Prime Minister Benjamin Netanyahu; Rob Joyce, the White House's Special Assistant to the President, Cybersecurity Coordinator; and former New York mayor Rudolph Giuliani.

Using the communications strategy we developed in 2016 as a strategic framework, we have continued to raise awareness in the public about our work and cybersecurity issues broadly.

CLTC also engaged with international institutions by inviting scholars from abroad to work with us on the UC Berkeley campus. In Spring 2017, CLTC was honored to welcome two scholars from international institutions, who participated in CLTC events and delivered workshops focused on their research.

LAURIN WEISSINGER, from Cyber Security Oxford and the Extra-Legal Governance Institute, worked on developing novel methods for assessing cyber risk within organizations, in part by using network analysis to identify which individuals are most at risk for a cyberattack, based on factors such as their access to high-value data and their relationships to other people. He is also investigating how buyers and sellers assess each other's trustworthiness in online markets for illicit goods (such as Silk Road).

FRANK SMITH, a senior lecturer with the Centre for International Security Studies at the University of Sydney, spent his time with CLTC examining the potential impact of quantum technologies—including quantum computing and cryptography—on international security. His research is part of a larger, Carnegie-funded project called "Peace and Security in the Quantum Age," which considers, for example, what would happen if a government were to build a quantum computer that could unscramble even the most sophisticated encryption.

Both scholars delivered workshops for members of the UC Berkeley community and engaged with other researchers during their visits.

STRATEGIC COMMUNICATIONS

Using the communications strategy we developed in 2016 as a strategic framework, we have continued to raise awareness in the public about our work and cybersecurity issues broadly. Following are updates on our communications work in key areas:

Social Media: CLTC has continued to grow our presence on Twitter and Facebook, channels we use to report out on upcoming events, report releases, and other news. We had more than 1135 Twitter followers by year's end. We also established an account on LinkedIn and have begun to use that channel for outreach to professional communities. We hired student assistants to help us with our social media, particularly with Facebook, which has the potential to help us better connect with UC Berkeley students.

Media Relations: CLTC has continued to grow our media presence, both through direct relationships with reporters and by contracting with outside media consultancies to boost our engagements. In 2017, we continued to work with Glen Echo, a Washington D.C.-based firm, which has played a key role in helping the Center deliver our message to key audiences, including policymakers. We regularly disseminate press releases around key events, and we also made an effort in 2017 to make direct pitches to place op-eds in a variety of publications. As a result, CLTC and our grantees have earned media coverage in the *New York Times*, *New Yorker*, CNN, *Washington Post*, *Foreign Policy*, *The Guardian*, and other outlets (see sidebar). We are continuing to explore new avenues for gaining exposure for our grantees.

Weekly Newsletters: We have continued to release weekly newsletters to engage our community of supporters; our newsletters include CLTC news, event announcements, job listings, internships, academic opportunities, and more. We refined the look of our newsletter throughout the year and now have more than 1000 subscribers.

Quarterly and Annual Reports: In addition to releasing a public version of our annual report, which provides an overview of the Center's progress and achievements and our goals for the future, we began producing quarterly newsletters specifically designed for our external community of supporters. These reports are intended to share highlights and keep key stakeholders engaged in our progress.

STRATEGIC COMMUNICATIONS GOALS

Goals for 2020

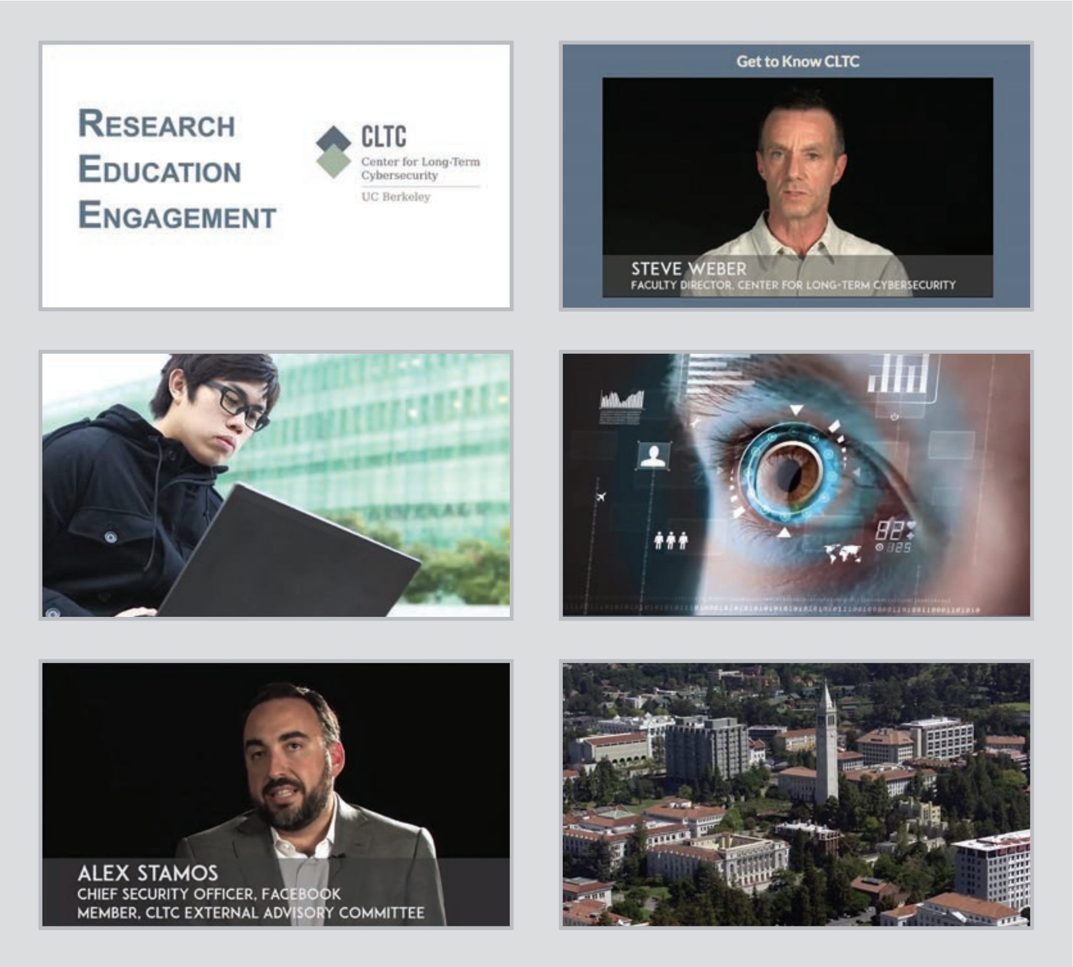
Execute Strategic Plan for Communications, as laid out in 2016.

Interim Goals for 2018

- More robustly engage decision makers (both in and out of government) to influence cyber governance models, including regulations, standards, and/or legislation
- Continue to grow a community of corporations, foundations, NGOs, and other partners who support and draw upon our work
- Increasingly raise public awareness about CLTC through a wide range of media channels, making the center the "go-to" source for information about future-oriented cybersecurity questions
- Increase on-campus interest in CLTC events and resources
- Consistently improve our internal communications work and strategy, based on audience reception and other metrics

Enhancements to the CLTC Website: Throughout the year, we worked with our web development partner, Kanopi, to enhance our website with new features, including social media links, improved design functionality, and added pages (to showcase our Corporate Membership Program, EAC, and other programs). We also began developing a robust jobs page on our web site that will allow users to search for jobs and internships, and potentially will allow external organizations to post cybersecurity jobs listings on our site.

Overview Video: In Spring 2017, we released a short video produced to provide unfamiliar audiences with an overview of our mission and activities. The video includes interviews with CLTC leaders and affiliated researchers, and is designed to convey a "nutshell" overview in roughly four minutes.


RESEARCH
EDUCATION
ENGAGEMENT
CLTC
Center for Long-Term Cybersecurity
UC Berkeley
Get to Know CLTC
STEVE WEBER
FACULTY DIRECTOR, CENTER FOR LONG-TERM CYBERSECURITY
ALEX STAMOS
CHIEF SECURITY OFFICER, FACEBOOK
MEMBER, CLTC EXTERNAL ADVISORY COMMITTEE

We produced a short video to provide an overview of our mission and activities.

MEDIA HIGHLIGHTS

CLTC received coverage in dozens of media outlets in 2017, including the *New York Times*, *Washington Post*, CNN, *Slate, Quartz, Foreign Policy*, *Guardian*, and other outlets. Below are some highlights from our media exposure:

- In February, Betsy Cooper published an op-ed in **The Hill** entitled, "Cyber executive order a reasonable step forward, yet more remains to be done." In addition, CLTC's report on recommendations for the Trump Administration was highlighted in a story in **Security Policy and the Law**, and Cooper was interviewed for an article in **The Hill**, focused on President Trump's executive order on cybersecurity.

- In March, Steve Weber published an essay in **Christian Science Monitor's Passcode** focused on using scenarios as a useful tool for approaching the cybersecurity challenge. In the essay, "Want to fix cybersecurity? Think about worst-case scenarios first," Weber argued that "good policy will need to consider not just one but a set of scenarios in order to design in advance interventions and incentives that will succeed—or at least not make the security situation worse—across the evolving landscape of possibilities."

- CLTC Senior Fellow Jonathan Reiber was a guest on South Africa's **POWER FM**, a radio talk show, along with journalist and TED Talks presenter Toby Shapshak. Their conversation, hosted by Iman Rappetti, spanned a range of topics, including cyberdefense, the role of the Internet in politics, and social media. Reiber spoke about the Russian hack, Trump's tweets, and the shape of our political and cyber world.

- In May, following the WannaCry Ransomware attacks, Weber and Cooper published an op-ed in the **New York Times**: "Digital Insecurity Is the New Normal" highlights the themes outlined in CLTC's scenario, "The New Normal," which depicts a future in which people retreat to non-digital technologies as cyberattacks become more widespread.

- In a May 15 article by Tim Starks of **Politico**, "Trump Confronts Global Cyber Crisis with a Staff Marked by Vacancies," Steve Weber noted that the WannaCry attack might motivate Trump's administration to fill key leadership positions related to cybersecurity.

- Betsy Cooper was among experts interviewed for a June piece by Charlie Mitchell of the **Washington Times**, "Trump's cyber policy remains 'to be determined,'" focused on the Trump administration's executive order on cybersecurity. She noted that the executive order shows that cybersecurity is a high priority, "but it doesn't really set a policy direction for the new administration. It calls for a series of reports, and that suggests the administration is still deciding whether to continue on the Obama path or take a new approach."

- In June, Steve Weber, together with CLTC Communications Coordinator Chuck Kapelke, published an article on the **Lawfare** blog outlining how the directives in President Trump's executive order on cybersecurity could be used by any institution to prepare for and defend itself against a cyberattack.

- In August, Senior Advisor Jesse Goldhammer was interviewed by Denisse Moreno of the **International Business Times**, in a piece focused on skills needed for a cybersecurity career. Goldhammer noted that there are opportunities not only for "folks with technical skills" but also for those with "complementary capabilities, such as sales, marketing, HR, finance, etc."

- In October, our report on the cybersecurity of the Olympics received coverage from major outlets like CNN and **Agence France Press** (whose syndication allowed the story to travel to nations around the world). On November 4, the **Guardian** wrote an article entitled "Cracking the Vault: Artificial Intelligence Judging Comes to Gymnastics," which featured the CLTC report.

- In November, CLTC Faculty Director Steve Weber was interviewed by **California Magazine** on the risk of war with North Korea and the relationship between Kim Jong-un and Donald Trump.

- In November, Deirdre Mulligan, co-director of the UC Berkeley Center for Law and Technology and CLTC-affiliated professor at the UC Berkeley School of Information, and Stefan Savage, a 2017 MacArthur Foundation "Genius" grant recipient and a professor at UC San Diego, were interviewed in a fireside chat for "**Enigman Interviews**." The conversation was focused on "connected cars," a topic on the forefront of cybersecurity and the "cyberphysical dilemma."

- In November, after the Sacramento Regional Transit experienced a cyberattack shutting down its website and gaining the attention of the Department of Homeland Security, the **Sacramento Bee** spoke to Betsy Cooper for input on the story.

- In November, **Foreign Policy** published "Where's the 9/11 Commission for Russia's Election Attack?" authored by Jonathan Reiber and Vikram J. Singh, senior advisor for national security, democracy, and technology at the Center for American Progress.

- In November, **The New Yorker** featured CLTC-affiliated faculty member Doug Tygar's Cyberwar course in "At Berkeley, a New Generation of 'Ethical Hackers' Learns to Wage Cyberwar." Tygar is a professor in computer science and information management with a research interest in privacy and security. CLTC Student Assistant Jobel Kyle Vecino, a student in the course, was also featured.

- In December, **Slate** published an op-ed by CLTC Grantee Rena Coen focused on digital marketers' use of "inference," connecting dots of data to make estimations about individual consumers to send them more targeted marketing. CLTC's communications team played a direct role in drafting and placing this piece.

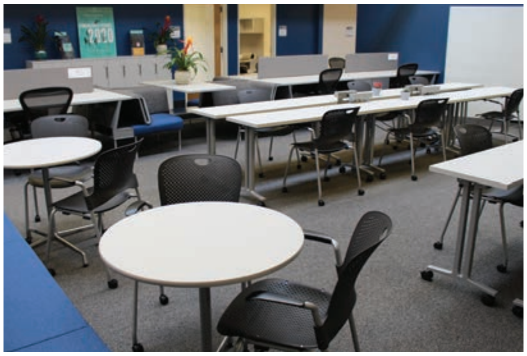
Organizational Development and Fundraising

Throughout 2017, the Center for Long-Term Cybersecurity made important progress toward our long-term goal of becoming a robust and self-sustaining organization by the end of 2020. The growth of our team during the past year reflects our evolution as an organization: we hired in-house researchers and additional staff; we enlisted student researchers, visiting scholars, and external service providers to support our work; and we have continued to expand our communications, events, and administrative functions while formalizing our relationships with external partners through the External Advisory Committee and the Corporate Membership Program.

A NEW PERMANENT HOME FOR CLTC

Given our rapid growth, CLTC has moved twice since our founding in 2014, and so we are pleased to report that, in Fall 2017, after an extensive search, we found a space to serve as our permanent home. We are now located in Hearst Field Annex, Building B, an accessible, one-story building located near Bancroft Avenue on the southern edge of the UC Berkeley campus. We moved into this new space in September and spent the fall renovating and acquiring furniture, some of which was generously provided at a discount by Herman Miller—the world renowned furniture design company—as part of their Future of Work research program.

This space has several key advantages. Most importantly, we will able to support our growing team, as we can accommodate up to 15 permanent staff members working on site, as well as 20+ students and faculty from our grantee research teams and master's degree program. The space also has an open floor plan, kitchen, and access to an



We moved into a permanent home on the UC Berkeley campus.

outdoor courtyard, all of which represent benefits for our team members. Additionally, we are housed directly adjacent to UC Berkeley's new Data Science program, which will yield productive collaborations. We celebrated our new home with an open house for grantees and other "friends of the Center" in January 2018.

COMMUNICATION, EVENTS, AND ADMINISTRATIVE CAPACITY

In addition to growing our core research team, CLTC has continued to carefully build a small expert staff for administration, communication, and events planning. Toward the end of the year, we bid farewell to Kristin Lin, who is pursuing a career in digital media production, and we hired a new Special Assistant, Matthew Nagamine, a recent UC Berkeley graduate who previously worked for UC Berkeley's Social Science Matrix. Matt has smoothly transitioned into his role working directly alongside Betsy Cooper, and he quickly took on a variety of tasks, from handling procurement and development to managing the Corporate Membership Program.

We have continued to evolve our communications team, which now comprises multiple team members, including part- and full-time employees and external consul-

Caitlin Appert-Nguyen

Chuck Kapelke

Kristin Lin

Matthew Nagamine

Denise Simard

Rachel Wesen

tants. Our part-time communications coordinator, Chuck Kapelke, continues to assist with web content, video production, copy editing, and other tasks, and in 2017, Chuck took on the task of helping our grantees with drafting and placing op-eds related to their work. We established the position of Digital Communications Strategist, who is responsible for social media management, web content and newsletter writing, digital marketing strategy, and more. Caitlin Appert-Nguyen filled this role on a 50% basis (splitting her time with the School of Information); after she transitioned to work at the School of Information full time, we hired Rachel Wesen to take over this position and serve dually as our events coordinator (replacing Denise Simard), starting in early 2018. We also hired two student assistants, Jobel Vecino and Ruby Aujla, who helped with our social media, campus engagement, newsletter, and other functions.

Beyond our team on campus, we continued to work with a variety of external service providers offering specialized communications services, such as web site design, publications design, and media relations; we have sustained our partnership with Glen Echo Communications, a Washington D.C. firm that supports us with outreach to the media (e.g. placing articles and op-eds) and engaging policymakers, and we continue to work with Kanopi Studios for web design.

EXTERNAL ADVISORY COMMITTEE

In November 2017, we publicly announced our External Advisory Committee (EAC), a group of corporate executives charged with helping the Center advance our research and educational agendas by providing perspectives from industry and other domains. The committee, which held meetings throughout the year, includes: Sameer Bhalotra (co-chair), StackRox; Ellen Richey (co-chair), Visa; Gilman Louie, Alsop Louie Partners; Jim Routh, Aetna; Ted Schlein, Kleiner Perkins Caufield & Byers; Raj Shah, Defense Innovation Unit Experimental (DIUx); Alex Stamos, Facebook; Joe Sullivan, Uber; and Maggie Wilderotter, from Wilderotter Vineyard. We are grateful that these members have committed time and resources to help the Center think strategically about our growth plans and programs.

The EAC played a meaningful role in helping us shape the curriculum and program structure for the School of Information's Master of Information and Cybersecurity degree; we convened two industry input meetings to scope out how companies currently address the cybersecurity skills gap and to understand how the degree can best provide support and preparation to students. We will continue to convene meetings with the EAC throughout 2018.

FUNDRAISING

In 2017, CLTC was able to meet its fundraising goals through a variety of sources for funding, including significant corporate contributions, a scoping grant from the MacArthur Foundation, and a cy pres award from a legal settlement.

FUNDRAISING GOALS

Goals for 2020

By 2020, we aspire to have a robust center that will at a minimum include a strong administrative structure, including in-house, multidisciplinary researchers focused on key issues related to the long-term cybersecurity research agenda, and a robust fundraising model.

Interim Goals for 2018

- Complete the renovation of our permanent space
- Continue hiring researchers to build sustainable programs in our four priority research areas
- Further build and refine our staffing in admin, communications, and events, while hiring other strategic positions focused on development, program management, and other roles
- Match or exceed 2017 fundraising, and hire a major gifts officer

Our Research Exchange brought together CLTC grantees with private-sector partners and policymakers.

As the Center prepares looks toward the second half of our grant period, we have started to think more strategically about what it would take for CLTC to be self-sustaining by 2020, including by envisioning creative and robust funding models. The Center laid the groundwork for part of this strategy in August, when we launched our Corporate Membership Program, which is designed as the primary avenue for companies to engage with the Center on research and other forms of collaboration. Companies can engage with CLTC as Associates, or they can sign on as Partners for more tailored, in-depth engagement. Six companies signed on as the program's inaugural members: Facebook, Inc.; Huawei Technologies Co., Ltd.; Kaiser Permanente; Qualcomm Technologies, Inc., a subsidiary of Qualcomm Incorporated; Symantec Corporation; and Tanium. Microsoft and Hewlett Packard have since committed to joining.

Together with the UC Berkeley School of Information, we continue to seek a Director of Major Gifts to help design a major gifts program for both institutions. The successful candidate will be charged with helping design and implement a comprehensive campaign that will address immediate fundraising needs as well as future goals. The successful candidate will be responsible for developing and implementing strategies for cultivating, soliciting, and stewarding major gifts prospects.

The Way Forward

CLTC is now well positioned to expand our research and policy impact in 2018. Our goal remains to refine our role and elevate our voice in the scientific and policy conversations about a broad array of issues related to cybersecurity as we have defined it. With our new space and staff researchers, as well as a growing community of cybersecurity researchers and students at Berkeley, we are in a strong position to continue to expand our impact and raise the profile of the center in 2018.

Organizational growth brings new challenges. Especially in a volatile and uncertain political environment, we need to remain nimble and responsive; it is imperative to jump in quickly to have a voice in the public conversation about some unfolding events and to do so responsibly and selectively. As a future-oriented center, we also are careful not to let contemporary pressures outweigh long-term thought and planning.

As we continue to grow, we will work harder to serve as effective partners to our community of researchers. We are dedicated to supporting and elevating the work of our grantees, and we are excited to build on the model of our successful Research Exchange as another means of deepening a cybersecurity community at Berkeley that includes faculty, post-docs, students, and staff. We will press forward to further integrate the Berkeley campus work with industry, government, philanthropy, and media partners. The range, depth, and significance of cybersecurity issues that will emerge in 2018 and beyond demand the kind of integrated, multidisciplinary, and cross-sectoral approach that we have devoted much of our effort to facilitating.

We are dedicated to supporting and elevating the work of our grantees, and we are excited to build on the model of our successful Research Exchange.

One significant change since we launched CLTC is that ‘cybersecurity’—not long ago a niche and specialized area of research—has emerged as a major public concern for firms, governments, and societies. Issues around commerce and data, around privacy, around information operations up to and including warfare, around distributed ledgers and ubiquitous sensing and computing, and of course around machine learning and artificial intelligence, have become central to the way people and organizations think about and experience what it means to be secure. In 2018, we expect even more attention to these important issues, and we have every intention of providing more factual underpinnings and reasoned commentary to these debates as they move forward. We will also continue to point attention to the future just over the horizon—with strategic foresight that informs research and policy work aimed at getting ahead of the problem set when possible. The digital environment moves too quickly to do otherwise, and we see no signs of that trend slowing down.

Contact Information

Visit our website, sign up for our newsletter, and follow us on Facebook and Twitter for updates on our programs and activities.

Center for Long-Term Cybersecurity
cltc.berkeley.edu
@CLTCBerkeley
cltc@berkeley.edu
(510) 664-7506

CLTC

Center for Long-Term Cybersecurity

UC Berkeley

Center for Long-Term Cybersecurity
cltc.berkeley.edu
@CLTCBerkeley