UC BERKELEY

CENTER FOR LONG-TERM CYBERSECURITY
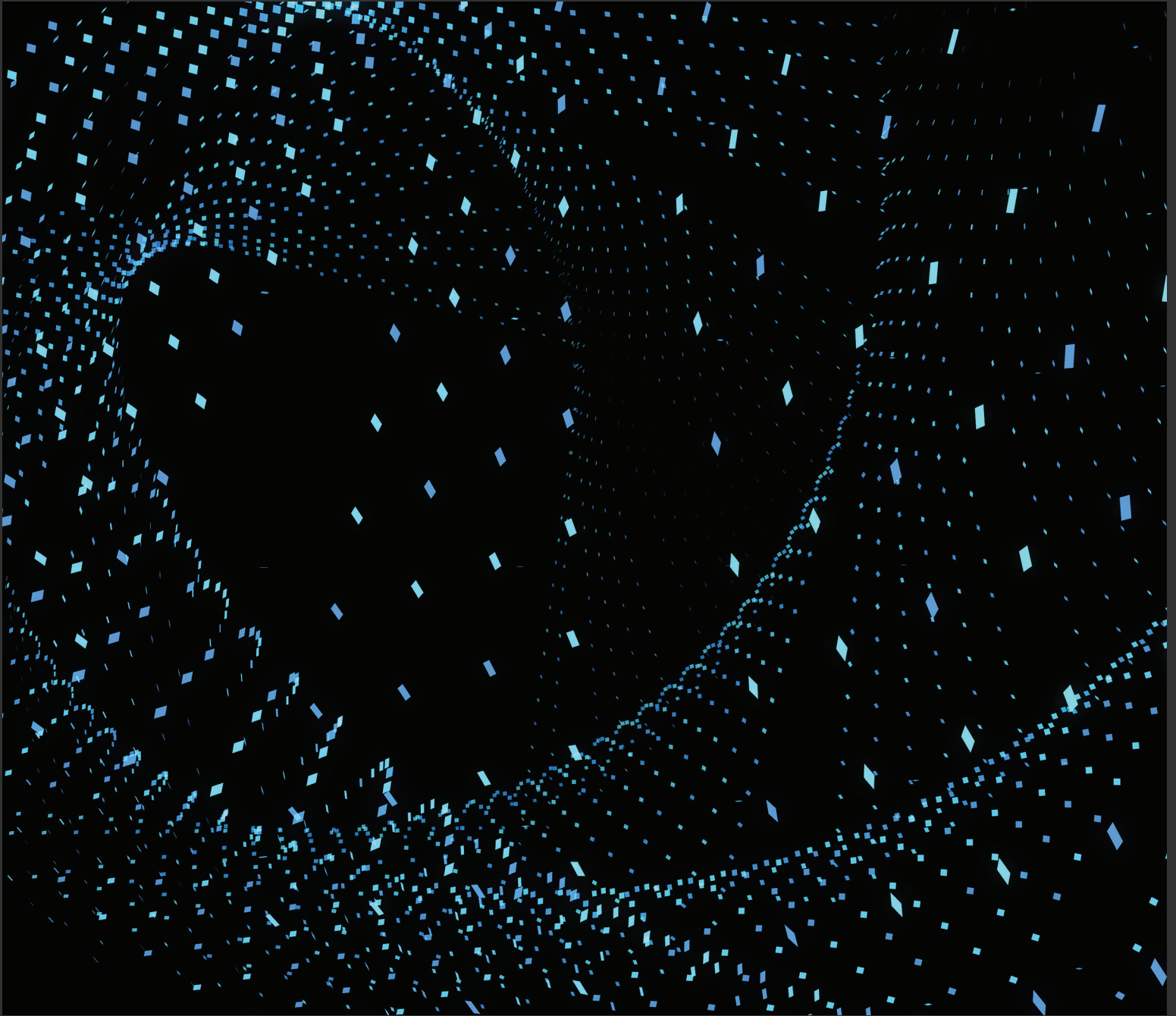
2016

ANNUAL REPORT

Table of Contents

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

For those who are unfamiliar with the Center for Long-Term Cybersecurity (CLTC), we are a research and collaboration hub housed within the University of California, Berkeley School of Information. Funded through a generous seed grant from the William and Flora Hewlett Foundation, CLTC seeks to design solutions to cybersecurity issues that arise wherever humans and digital systems interact, based on a long-term vision of the internet and its future. Working with researchers from UC Berkeley and outside organizations, we are building a diverse community of partners to advance research, technologies, and recommendations that will help governments, corporations, and individuals better prepare for the challenges of cybersecurity throughout the 21st century. We focus our work on three streams of activity: research, education, and engagement.

2016 was a year of significant growth for CLTC. We doubled our staff, hosted major events in the San Francisco Bay Area and Washington, D.C., funded creative research projects, and prepared to launch a master's degree program in cybersecurity. Through it all, we sought both to educate our partners about the importance of taking a longer term view of cybersecurity, and to encourage them to stretch their impact, both within and outside the university. This annual report reviews our accomplishments and defines the impacts, obstacles, and risks that remain in the long-term endeavor that we have begun. We start with some brief reflections about what has changed—and what has not.

Over the past year, we have developed a stronger strategic direction and sense of where we can make a unique contribution, which we have defined in a mission statement:

CLTC 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.

This mission statement reflects our continued belief that our center should 'nudge' society toward both a broader view of what cybersecurity means and a longer-term vision of how to approach this challenge. But it also acknowledges a shift in how we

We are fully dedicated to supporting research and education at UC Berkeley; we have now allocated over $2 million in funding to Berkeley-affiliated cybersecurity research projects, and hope to help launch a degree program within the next year.

are seeking to achieve that goal. Whereas in the past we have focused primarily on developing an academic field of cybersecurity—a goal we still think is central and continue to pursue—we now see the need to play a broader role by connecting this burgeoning academic field to companies, governments, and other institutions.

We have also begun to refine our strategy for achieving our mission. We are fully dedicated to supporting research and education at UC Berkeley; we have now allocated over $2 million in funding to Berkeley-affiliated cybersecurity research projects, and hope to help launch a degree program within the next year. But we also believe that in order to achieve our mission, we need to specialize further within the 'center of our center,' developing a deeper range of domain expertise through internal research and programming that give CLTC a unique voice and role in the global conversation about cybersecurity.

What has not changed is our ambition. CLTC aspires to be 'the' voice on long-term cybersecurity. In our first year, we took a diverse approach to achieving that goal. In our second year, we have begun to narrow our scope in order to focus on a more selective set of research, educational, and outreach activities. But exploration and innovation will remain an important part of our development as we go forward.[1]

In the sections that follow, we review CLTC's accomplishments for 2016, and identify key short- and long-term goals for the coming years.

Steve Weber, Faculty Director
January 30, 2017

Betsy Cooper, Executive Director
January 30, 2017

Organizational Development

In 2016, CLTC continued to work toward our goal of establishing a robust and self-sustaining organization by the end of 2020. We built out our administrative capacity by hiring several staff members (some part-time) to work on events and general administrative support; restructured the CLTC scientific advisory committee to better serve our needs; and established an external advisory board for ongoing corporate and government engagement. To accommodate our rapid growth, we moved into a temporary three-room office space on the UC Berkeley campus. Finding a permanent space to accommodate our growing size is a top priority.

We hired a part-time events coordinator to manage the logistics of coordinating CLTC events, which in 2016 included hosting a meeting of the White House Commission on Enhancing National Cybersecurity, as well as 11 public presentations delivered as part of our seminar series. Additionally, we brought on Kristin Lin as Special Assistant, a role that focuses on sustaining the daily operations of the Center, as well as providing support for larger research and development projects as needed. Having an additional staff member on board has allowed Executive Director Betsy Cooper to focus her attention more deliberately on the Center's long-term growth, including by developing our research and fundraising efforts.

CLTC continues to employ a part-time communications coordinator, Chuck Kapelke, who assists with events, website development and branding, video production, and copyediting. We contracted with additional consultants— including a web designer, a publications designer, and communications support —to assist with building our media presence on both coasts. And we continued to support the work of Jonathan Reiber, senior research fellow, who has been an active contributor in national and international forums related to cybersecurity.

CLTC also focused on building out our advisory network in 2016. We created a Scientific Advisory Committee consisting of all faculty grantees. We then convened a research agenda retreat that brought together 14 UC Berkeley faculty members and corporate advisors to help refine CLTC's research priorities. AnnaLee Saxenian, Dean of the UC Berkeley School of Information, and Jesse Goldhammer, Associate Dean, continue to serve as Senior Advisors and provide regular advice and support to the center.

To ensure our work remains relevant to the interests of other institutions, CLTC began to develop an External Advisory Committee, a group of six corporate executives and government leaders who represent companies like Visa, Facebook, and Uber and have committed time and resources to helping the Center think strategically about our growth plans. At the first meeting of the group in early December, the advisors established points of mutual interest and potential avenues of engagement and partnership for the year ahead.

ORGANIZATIONAL DEVELOPMENT 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, multi-disciplinary researchers focused on key issues related to the long-term cybersecurity research agenda.

Interim Goals for 2017

● Build an efficient, adequate staffing model capable of supporting the "center of the center," and hire the appropriate staff.
● Secure space adequate for in-house research.
● Build in-house research capability and stand up the in-house team.

Research and Thought Leadership

CLTC achieved several milestones in our research agenda this year. We released the Cybersecurity Futures 2020 report, featuring five scenarios for the future of cybersecurity; hosted sessions across the world to engage with the scenarios; and issued a second request for proposals. Going forward, we intend to develop a multi-disciplinary research and impact agenda that is directed by a vision of long-term cybersecurity, to supplement the research we are already supporting on campus.

SCENARIOS FOR CYBERSECURITY FUTURES

After months of research and interviews, the Center released *Cybersecurity Futures 2020*, a major report detailing five possible scenarios for how cybersecurity and humans' relationship to technology could evolve over the next four years. The report's release event, which took place at the National Press Club in Washington, D.C., attracted over 120 attendees, and featured a panel of technology luminaries, including Ed Felten, U.S. Deputy Chief Technology Officer, Phyllis Schneck, U.S. Department of Homeland Security's chief cybersecurity official, and Nathaniel Fick, CEO of cybersecurity company Endgame.

> Going forward, we intend to develop a multi-disciplinary research and impact agenda that is directed by a vision of long-term cybersecurity, to supplement the ressearch we are already supporting on campus.

Since the report's release, the scenarios have had significant impact on the thinking of public and private officials, both here and abroad. CLTC leaders presented the scenarios at universities, conferences, companies, and government agencies across the country and world. Faculty Director Steve Weber used the scenarios as the basis for his annual Carnegie-funded New Era Foreign Policy conference, focusing on the 'public goods' aspects of the scenarios. The *Wall Street Journal* covered a panel at the RSA security conference at which Weber and Executive Director Betsy Cooper presented the scenarios to an overflow crowd of 500 people over two sessions. Senior Advisor Jesse Goldhammer and Cooper also presented the report to senior international government officials in a closed-door session at the RSA conference. Senior Fellow Jonathan Reiber incorporated the scenarios into several talks that he gave in India and China.

In keeping with our commitment to encourage cross-sector dialogue, the Center has also given workshops on scenarios at the Council on Foreign Relations; to companies like Dropbox and SanDisk; and to a California Supreme Court Justice and his staff. These presentations and talks have allowed CLTC to engage substantively with over 20 organizations over the course of 2016. Feedback from participants, as well as continued interest many months after the report's release, suggest that the scenarios have begun to nudge the debate over cybersecurity toward a more future-oriented perspective.

2016 GRANTEE ACTIVITIES

In addition to wrapping up the scenarios report, the Center also invested more than $900,000 in research funding to support 22 projects across the UC Berkeley campus. The first class of CLTC grantees worked on such issues as how organizations can better detect spear-phishing cyberattacks; how neural signals could be used as a method of online authentication; and how at-risk activists and NGOs can better protect their digital activities from state-level surveillance. We are proud of the impact we have made through our support of Berkeley research: while much of the work is ongoing, CLTC-funded research has already resulted in publications, conferences, and even several usable tools and applications. To the right, we have highlighted several examples of the kind of work and impact that came out of CLTC-funded research in 2016.

FUTURE RESEARCH AGENDA

CLTC also began to hone our research agenda for the next few years, initially selecting six focus areas based on conversations with advisors and corporate partners, including the Center's two advisory boards.

THE SIX FOCUS AREAS WE STARTED WITH WERE:

1️⃣ **Cyber risk**, including incentives to improve security and cyber insurance;
2️⃣ Security implications of the **Internet of Things**;
3️⃣ Security implications of **machine learning and artificial intelligence**;
4️⃣ Innovative approaches to the problems of **identification and authentication** beyond conventional passwords;
5️⃣ Addressing the '**talent pipeline problem**' for cybersecurity, both by expanding the number of qualified cybersecurity professionals and increasing their diversity; and
6️⃣ New approaches to the **regulatory landscape of cybersecurity**, including improved design of public, private, and mixed institutions.

These core areas helped guide our grant-making decisions for the second grantee cohort, which was announced in January 2017. The Center conducted a thorough and extensive review process to select our 2017 grantees, with a first-round review by fifteen experts from a variety of relevant domains. The Center is grateful for the generous time and thought that these reviewers contributed to the decision-making process.

As a result of our 2016 Request for Proposals, the Center allocated almost $950,000 to support 29 research projects across the UC Berkeley campus in 2017. Our second grantee cohort reflects a wider range of disciplines engaging with cybersecurity, and includes faculty members and researchers from law, public policy, business, psychology, and sociology, in addition to computer science and information science.

2016 GRANTEE ACTIVITIES

CLTC grantee **BILL MARCZAK**, supported by fellow grantees **NICK WEAVER** and **VERN PAXSON**, discovered *Stealth Falcon*, a campaign of targeted spyware attacks carried out by a sophisticated operator (likely the United Arab Emirates government) against Emirati journalists, activists, and dissidents. These researchers also discovered the first known iPhone remote jailbreak employed for malicious ends. As a result of this discovery, Apple quickly released an iOS patch to hundreds of millions of users worldwide. The researchers' findings garnered media attention from the *New York Times* and *Vanity Fair*.

Grantee **SADIA AFROZ**, who worked on a project titled, "Cybercrime Science: Understanding Criminal Networks and the Effect of Disruption," used CLTC funding to finish building a tool that analyzes cybercriminal networks to determine the nature of the transactions in underground forums. The tool has been tested to scan forums for products, prices, and buying/selling activity. A paper published as a result of this work has been accepted

to the 2017 World Wide Web Conference.

Professor **JOHN CHUANG** and a team of researchers at the UC Berkeley School of Information's BioSense Lab used a CLTC grant to explore the practical feasibility of using brainwaves for user identification and authentication. Their tests have confirmed that the use of an in-ear device to capture a user's "passthoughts" could potentially become a viable alternative to passwords. As a result of these studies, the team has three manuscripts under review or in preparation.

Professor **DOUG TYGAR** and Adjunct Professor **XIAO QIANG** developed Hiking GFW, an initiative dedicated to monitoring Chinese internet censorship. Their team built a map of 1,498 domains that are currently blocked by China's Great Firewall and allows users to sort sites based on the geolocation information extracted from their IP addresses. The Hiking GFW website also links to existing tools to help users circumvent online censorship.

2017 CLTC GRANTEES

THE FOLLOWING RESEARCH PROJECTS WERE GRANTED FUNDING THROUGH OUR 2016 REQUEST FOR PROPOSALS:

- Adversarially Robust Machine Learning (Sadia Afroz, Qi Zhong)
- Comparative Industrial Policy in the Cybersecurity Industry: Policy, Drivers, and International Implications (Vinod Aggarwal, Andrew Reddie, Tai Ming Cheung)
- Human-Centered Design Study on Cybersecurity of Soft Co-Robotic Systems (Alice M. Agogino, Euiyoung Kim, Kyunam Kim)
- Information Theoretic Methods in Cybersecurity (Venkatachalam Anantharam)
- Securing Protected Health Information in Mobile Health Devices (Anil Aswani, Xin Guo)
- Addressing the Privacy Gaps in Healthcare (Ruzena Bajcsy, Daniel Aranki)
- Exploring Internet Balkanization Through The Lens of Regional Discrimination (Jenna Burrell, Anne Jonas)
- Linking Behavioral and Physiological Responses in Virtual Reality to Privacy and Security Outcomes (Coye Cheshire)
- Zero Knowledge Proofs for Privacy-Preserving Cryptocurrencies (Alessandro Chiesa)
- NilDB: Computing on Encrypted Databases with No Information Leakage (Alessandro Chiesa, Raluca Ada Popa)
- Toward One-Step Three-Factor Authentication Using Custom-Fit Ear EEG (John Chuang)
- I Regret To Inform You That Your Private Information Has Been Compromised (Naniette H. Coleman)
- Analysis of Security Breaches of Local Law Enforcement Agency Data (Catherine Crump, Rena Coen, David Schlussel)
- Citizen Advocacy in a Connected World (Jason Danker, Andrea Gagliano, Paul Glenn, Molly Mahar, Sasha Volkov, Emily Witt)
- Identifying Audio-Video Manipulation by Detecting Temporal Anomalies (Alexei Efros, Andrew Owens)
- Cyber-Infrastructures of the Personal Data Economy (Marion Fourcade, Daniel Kluttz)
- Programming for Privacy in High School Classrooms (Gerald Friedland)
- Obfuscation from Weaker Variants of Multilinear Maps (Sanjam Garg, Daniel Masny)
- Mapping Sites of Politics: Values at Stake in Mitigating Toxic News (Daniel Griffin)
- Preparing for Blockchain: Policy Implications and Challenges for the Financial Industry (Ritt Keerati, Chloe Brown)
- Actuarial Justice in the 21st Century (Johann Koehler, Gil Rothschild Elyassi)
- Strengthening Cybersecurity in Human Rights Investigations (Alexa Koenig, Eric Stover)
- Tools and Methods for Inferring Demographic Bias in Social Media Datasets (Samuel Maurer)
- When to Avoid Digital Control: A Cybersecurity Case Study for Advanced Nuclear Reactors (Per F. Peterson, Michael Nacht)
- Data Security Breach Notification in Singapore: The Role of Data Privacy Officers in Enhancing Trust Relationship (Visakha Phusamruat)
- Sharing Personal Information with Humanlike Machines: The Role of Human Cues in Anthropomorphism and Trust in Machines (Juliana Schroeder, Matthew Schroeder)
- Allegro: A Framework for Practical Differential Privacy of SQL Queries (Dawn Song, Joseph Near)
- Secure and Usable Backup Authentication (David Wagner, Nathan Malkin, Serge Egelman)
- Secure Machine Learning (David Wagner)

AS WE ENTER 2017, WE ARE PAYING SPECIAL ATTENTION TO OPPORTUNITIES FOR DEVELOPING RESEARCH INITIATIVES IN THREE RESEARCH AREAS:

1 Security issues, writ broadly, associated with the growth and deployment of machine learning and artificial intelligence in societies and economies.

2 Expanding the cyber talent pool – by numbers, diversity, and impact.

3 New regulatory and governance structures that efficiently, creatively, and safely mobilize for cybersecurity objectives the activities of governments, companies, markets, civil society, individuals, and other relevant actors.

We are now beginning a scoping process to determine how we might be able to have the most impact—through research and beyond—in these areas.

CLTC also took advantage of various opportunities to engage in additional research activities. Executive Director Betsy Cooper secured funding to research cybersecurity at sporting events and has begun working on a research project commissioned by a major athletic organization. Additionally, the Center received a grant from the MacArthur Foundation, which will fund a scoping project for a human rights-focused initiative that the Center hopes to establish in the coming years.

At a CLTC Seminar, Steve Walker, CEO of Cobaltix, guided attendees through a scenario of a day in his life as a business technology consultant. (November 2016)

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, as well as areas that emerge on an opportunistic basis where we feel we can have a distinctive or outside impact. This includes:

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

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

Interim Goals for 2017

● Amplify the impact of some portion of the research we've funded to connect to other overarching goals, both to increase the profile of our Center and to help drive substantive outcomes;

● Test the efficacy, viability, and impact possibilities in priority areas, including by experimenting with targeted and/or outside-the-box approaches to solutions;

● Build the 'center of the center' in priority areas, and continue to encourage members of the campus to participate; and

● Explore the development of a 'scenarios one-year-on' research product and event.

Education

As an organization based at a university, CLTC is committed to providing educational opportunities and programming to students on the Berkeley campus, as well as addressing the cybersecurity talent pipeline problem more broadly. The Center has worked with the UC Berkeley School of Information and Department of Electrical Engineering and Computer Sciences (EECS) to write a formal proposal for a new Master's Degree of Information and Cybersecurity (MICS). Senior Advisor and Dean AnnaLee Saxenian, Professor and CLTC Grantee Doug Tygar, Professor and Faculty Director Steve Weber, and Senior Advisor and Associate Dean Jesse Goldhammer all played significant roles in writing and submitting the proposal. Pending approval by the university, the MICS degree hopes to welcome its first cohort of students in May 2018.[2] CLTC will continue to support the MICS program through its planning and development stages and will continue to be centrally involved in curriculum and course development as the program moves forward.

As an organization based at a university, CLTC is committed to providing educational opportunities and programming to students on the Berkeley campus, as well as addressing the cybersecurity talent pipeline problem more broadly.

Meanwhile, CLTC continues to enhance and lead cybersecurity education opportunities on campus. In the 2016 spring semester, CLTC worked with Faculty Grantee Deirdre Mulligan to welcome privacy expert Leslie Harris to campus to conduct research and lead a reading group for graduate students across campus. The largely student-driven group has brought individuals from across disciplines to discuss current research and events in the field. During the fall, the Center worked with Professor Chris Hoofnagle to establish the Cybersecurity Policy Reading Group as a for-credit course offered in Spring 2017.

The Center has also increased cybersecurity education through our Seminar Series, which in 2016 brought in 11 speakers from government, academia, and the private sector. In the spring, CLTC partnered with the Berkeley Center for Law, Business, and the Economy to host Vint Cerf, one of the founders of the internet and the reigning Chief Internet Evangelist at Google. In a far-reaching discussion, Cerf described the early evolution of the internet, and touched upon current and emerging issues related to cybersecurity, including encryption, privacy, the "Internet of Things," as well as the potential for a "digital dark age," in which human history fails to be adequately preserved in plastic devices and chips.

Some speakers opted for less traditional presentation formats. In the fall, Steve Walker, CEO of business technology and consulting firm Cobaltix, guided the audience through

a "Day in the Life" role-playing scenario. Walker discussed the kinds of security questions and challenges he faces while working with clients, and he challenged audience members to put themselves in his shoes to make difficult decisions.

CLTC also hosted grantee Bill Marczak's doctoral dissertation presentation, during which he presented the culmination of his work as a Berkeley Ph.D. candidate in the Electrical Engineering and Computer Science (EECS) Department. Marczak, whose work has been profiled in *Vanity Fair*, presented case studies on attack campaigns involving a variety of commercial "lawful intercept" and off-the-shelf tools. Marczak also presented software he developed that provides near real-time scanning of a subject's email messages to check for malware.

CLTC's seminars are open to the public and regularly attract between 25-50 attendees. Because we are committed to making these events as accessible as possible, we have invested in live-streaming capabilities and have started posting videos of each seminar on our website.

CLTC is particularly committed to increasing diversity within the field of cybersecurity by supporting curriculum development and programming for women, minorities, and other underrepresented groups. Together with CITRIS and the Banatao Institute, we co-hosted a Women in Technology Conference in October, drawing more than 100 attendees and 15 speakers, including keynote Nicole Wong, former U.S. Deputy Chief Technology Officer. CLTC also was able to secure funding to develop a one-day technical training course for women and minorities, and we have plans to pilot the program in 2017.

2016 SEMINAR SERIES

PETER ECKERSLEY, Chief Computer Scientist, Electronic Frontier Foundation

VINTON G. CERF, Chief Internet Evangelist, Google

DAVID & ORION HINDAWI, Executive Chairman of the Board & CEO, Tanium

JAMES C. TRAINOR, JR., Assistant Director, Cyber Division, FBI Headquarters

TOM ANDRIOLA, Vice President and CIO, University of California System

CHRIS FINAN, CEO and Co-founder, Manifold Technology

STEVE WALKER, CEO, Cobaltix

ANGELA MCKAY, Director of the Government Security Policy and Strategy, Microsoft

MARSHALL KUYPERS, Cyber Risk Scientist, Qadium

JOHN CRAIN, Chief Security, Stability and Resiliency Officer, ICANN

BILL MARCZAK, Ph.D. Candidate, UC Berkeley

EDUCATION GOALS

Goals for 2020
Create a world-renowned educational program for UC Berkeley cybersecurity students.

Interim Goals for 2017
● Prepare to launch Berkeley's Master's of Information and Cybersecurity degree;
● Expand support for diversity in cybersecurity.

Collaboration and Strategic Communication

CLTC sees immense value in investing time to connect the public with our research and education initiatives, both domestically and internationally. We believe that we are uniquely positioned to be a neutral convener across government, academia, and the private sector, and that facilitating these conversations can lead to productive partnerships for everyone. The Center approaches 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

CLTC's domestic collaboration efforts in 2016 focused on engaging government through events like the White House Commission on Enhancing Cybersecurity and the FBI General Counsel Summit, as well as one-on-one meetings with policymakers and legislators. Additionally, the Center spoke at five companies and attended 14 conferences to build our network for future engagement. CLTC also facilitated smaller group conversations by partnering with Andreessen Horowitz and the Hewlett Foundation to host a salon dinner in the Bay Area. These engagements have led to a large network of individuals that we can draw upon for our upcoming programming and research initiatives.

We believe that we are uniquely positioned to be a neutral convener across government, academia, and the private sector, and that facilitating these conversations can lead to productive partnerships for everyone.

OUR MOST SIGNIFICANT DOMESTIC ENGAGEMENTS ARE HIGHLIGHTED BELOW:

In January, CLTC hosted a Government and Tech conference that Steve Weber organized for the National Intelligence Council (NIC). The purpose was to provide specific input for the *Global Trends 2035 Report,* which the NIC releases every four years to inform high-level government policymakers about important drivers of change in the U.S. and around the world. CLTC's Jesse Goldhammer, Jonathan Reiber, and Betsy Cooper all served as experts at this convening.

In April, we released our *Cybersecurity Futures 2020 Report,* an analysis of five possible scenarios for the future, at a launch event in Washington, D.C. (Please see the "Research and Thought Leadership" section for more information.)

CLTC hosted a discussion panel on policy ideas for the new administration at the Bipartisan Policy Center in Washington, D.C. Speakers from left to right: USA Today *Reporter Erin Kelly, former Deputy Attorney General Jamie Gorelick, CLTC Faculty Director Steve Weber, Congressman Will Hurd (R-TX), and CLTC Executive Director Betsy Cooper.* (*November 2016*)

In June, CLTC hosted a meeting of the White House Commission on Enhancing National Cybersecurity, which was established by President Obama to inform the next presidential administration on priority issues in cybersecurity. Thanks in large part to our publicity efforts, the meeting drew more than 150 attendees, who listened as 11 expert panelists testified about key challenges and opportunities for strengthening cybersecurity in the digital economy. The UC Berkeley meeting was one of only seven that the Commission convened, and was the only event held on the West Coast. The Commission has since presented its report of recommendations to President Obama and the public.[3]

In September, CLTC partnered with the FBI to host a General Counsel Summit on the Berkeley campus. A group of General Counsels from over 25 companies met at Berkeley for a day of discussion with the FBI to discuss productive avenues for partnership and engagement.

In November, shortly after the election, CLTC hosted an event in Washington, D.C. together with the Bipartisan Policy Center. Faculty Director Steve Weber and Executive Director Betsy Cooper presented a policy brief detailing cybersecurity policy ideas for the new administration, which included recommendations for how to bolster the cybersecurity talent pipeline and effectively support the demand for research and innovative technical solutions to policy challenges. The event included a panel discussion, moderated by *USA Today* reporter Erin Kelly and featuring former Deputy Attorney General Jamie Gorelick and Congressman Will Hurd (R-TX). During the same trip to Washington D.C., CLTC set up one-on-one meetings with legislators and organizations interested in engaging in cybersecurity policy.

CLTC's domestic collaboration efforts in 2016 focused on engaging government through events like the White House Commission on Enhancing Cybersecurity and the FBI General Counsel Summit, as well as one-on-one meetings with policymakers and legislators.

In December, Senior Fellow Jonathan Reiber initiated a public-private contingency project with important industry and government partners. The group convened to discuss opportunities for cooperation and collaboration. The Center plans to continue facilitating these dialogues in 2017 and beyond.

Throughout the year, CLTC sent representatives to speak at numerous panels and conferences, including the New America Conference, Stanford WorldView, RSA, and Techonomy 2016.

INTERNATIONAL COLLABORATION

In 2016, CLTC's leadership traveled to Ireland, India, Russia, Singapore, and France as part of ongoing efforts to work on cybersecurity issues internationally.

OUR MOST SIGNIFICANT INTERNATIONAL ENGAGEMENTS ARE HIGHLIGHTED BELOW:

● CLTC partnered with European-based researcher Gilad Rosner on the Internet of Things Privacy Risk Mapping Project. CLTC has provided input and advice on the Project's first workshop, to be held in early 2017.
● Senior Fellow Jonathan Reiber has spearheaded efforts to engage cybersecurity professionals and government leaders in India, and he participated in meetings

CLTC Senior Advisor Jesse Goldhammer presented the Cybersecurity Futures 2020 Report in New Delhi. (September 2016)

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 2017

● Identify strategic partnerships in priority areas and begin to develop those partnerships.

CLTC hosted the only West Coast meeting of the White House Commission on Enhancing National Cybersecurity. The Commission's report was published in December 2016. (June 2016)

and public events in March and October. As part of his work, Reiber is contributing to the U.S.-India Track 1.5 cyber dialogue, an effort to chart the future of digital economy and cybersecurity cooperation between the two nations.

● In May, Executive Director Betsy Cooper traveled with the East-West Institute (and with the Hewlett Foundation's Eli Sugarman) for cybersecurity consultations with Russian officials and companies.

● In May, Cooper also met with visitors from UK academia on a United States tour. Out of that meeting, CLTC partnered with several UK academics to apply for project funding from the Engineering and Physical Sciences Research Council (EPSRC) on Evaluating Cyber Security Evidence for Policy Advice. That proposal was successful and work will begin in mid-2017.

● In July, the Center, as a participant of the Digital Sovereignty Working Group, published the "The Chamonix Manifesto: Transatlantic dialog on the impact of the rise of global intermediation platforms." The document was the result of ongoing dialog with European colleagues, and focused on policy and other challenges related to intermediation platforms. The Manifesto calls for a "common vocabulary" and increased collaboration among "relevant institutions to address growing disputes."

● In September, Senior Advisor Jesse Goldhammer and Senior Fellow Jonathan Reiber partnered with INK to host a forum on the future of cybersecurity in India.

● In October, Betsy Cooper gave a keynote speech at the Ronan Daly Jermyn Game Change Conference in Ireland.

● CLTC assisted two graduate students in traveling to China and France to give cybersecurity-related presentations on their work.

● In December, Steve Weber and Jesse Goldhammer organized a workshop for finance and insurance executives at AXA Insurance in Paris to explore future collaboration opportunities in IoT security.

In 2017, CLTC intends to consider selective additional international relationships that will help facilitate progress in priority areas.

In 2016, CLTC's leadership traveled to Ireland, India, Russia, Singapore, and France as part of ongoing efforts to work on cybersecurity issues internationally.

STRATEGIC COMMUNICATIONS

Beyond in-person engagements, CLTC seeks to grow our impact through strategic communications, including media outreach. In 2016, the Center shaped our communications strategy for the next four years, laying out a vision for how the Center can best engage with the greater public about our work

and research. The Center plans to revisit and revise this document as we carry out the action items we have planned for the next three years. The communications strategy provides a roadmap to achieve the kind of intentional and sustainable growth we hope to achieve through our long-term goals.

In 2016, the Center shaped our communications strategy for the next four years, laying out a vision for how the Center can best engage with the greater public about our work and research.

CLTC also launched Twitter and Facebook accounts, which have made our work and programs more accessible and searchable by the general public. We also refined the contents of our weekly newsletter, which has a continually growing subscription base.

The Center is working to establish a partnership with a media organization to host an online content platform focused on the future of cybersecurity. If successful, subscribers to this platform will receive news and reports on cutting-edge cybersecurity research being conducted at UC Berkeley and beyond. CLTC saw a spike in media coverage toward the end of 2016.

Angela McKay, Senior Director of Cybersecurity Policy and Strategy at Microsoft, spoke at a CLTC Seminar about challenges related to cybersecurity in the global context. (November 2016)

STRATEGIC COMMUNICATIONS GOALS

Goals for 2020

Execute our Communications Strategic Plan, as developed in 2016.

Interim Goals for 2017

● Engage and influence decision makers (both in and out of government) to influence cyber governance models, including regulations, standards, and/or legislation.

● Grow a community of corporations, foundations, NGOs, and other partners who support and draw upon our work.

● 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.

MEDIA COVERAGE HIGHLIGHTS

● **The Atlantic** wrote an article on one of the scenarios covered in Cybersecurity Futures 2020.

● **The Wall Street Journal** covered the Center's RSA panel on scenarios.

● CLTC was profiled in the **San Francisco Chronicle**.

● **CSM Passcode** published an op-ed that Executive Director Betsy Cooper wrote about gender diversity in cybersecurity.

● Steve Weber and Betsy Cooper co-wrote an op-ed in **Bloomberg Government** on election hacking and the economy.

● CLTC's cybersecurity policy brief received front-page business section coverage in **USA Today**.

● Betsy Cooper was named one of the 10 Women in Security Power Players by **SC Magazine**.

● Steve Weber and Betsy Cooper appeared on several podcasts to discuss scenarios and policy recommendations. You can listen to interviews on the **Steptoe Cyberlaw Podcast**, as well as the **Council on Foreign Relations Podcast** and **Raw Data**.

● The **San Jose Mercury News** published Steve and Betsy's op-ed arguing for stronger public-private partnerships in cybersecurity.

● Betsy Cooper was featured in a story about cybersecurity on NPR's **All Things Considered**.

Fundraising

We are thinking strategically about what it would take for CLTC to be self-sustaining by 2020, in part by envisioning creative and robust funding models. Seeking to capitalize on some early fundraising successes from our first two years in operation, the Center launched a 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.

Additionally, the Center began planning our fundraising strategy for the next three years. CLTC will continue to revise and deliberate this strategy, putting us in a strong position to achieve financial sustainability by 2020.

CLTC launched its Cybersecurity Futures 2020 report at the National Press Club in Washington, D.C. (April 2016)

FUNDRAISING GOALS

Goals for 2020
Develop a self-sustaining organization with a robust funding model.

Interim Goals for 2017
● Finalize and launch fundraising plan;
● Match or exceed fundraising success from 2016.

The Way Forward

In our second year, we have focused on growing and developing our institution to be able to achieve greater impact. Some of this effort has been focused on internal development, by growing our staff, structures, and space. We have also continued to prioritize our work across the campus, as we know that the intellectual firepower and research results we continue to harness from our Berkeley colleagues are at the center of our success.

As we adjust to the new reality of American politics, we anticipate the need to be flexible, yet responsive. We look forward to working with our partners to build the future of cybersecurity together.

Going forward, we intend to focus our efforts more intensively on how the 'core' of our center can make a greater impact on and beyond our campus. In some cases, that may involve prioritizing our existing research and education activities. In others, it may involve developing deeper collaborations. We also anticipate that, going forward, we may need to undertake more direct action on behalf of the Center to have an impact in the public space. Our MacArthur grant—which has a goal of developing an institution dedicated to supporting vulnerable populations online—is an example of our careful, intentional shift in that direction.

As we adjust to the new reality of American politics, we anticipate the need to be flexible, yet responsive. We look forward to working with our partners to build the future of cybersecurity together.

Contact Information

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

Steve Weber
Faculty Director
steve_weber@berkeley.edu

Betsy Cooper
Executive Director
bcc9@berkeley.edu

CLTC

Center for Long-Term Cybersecurity

UC Berkeley