UC BERKELEY CENTER FOR LONG-TERM CYBERSECURITY

2015 ANNUAL REPORT

TABLE OF CONTENTS

Contents

Introduction

In more ways than one, this has been a foundational year for the Center for Long-Term Cybersecurity. With the generous support of the Hewlett Foundation, we have identified and developed scenarios for cybersecurity futures; given out our first research grants; taken strides to develop partnerships both nationally and internationally; established a public presence, developing a website and e-mail list; and begun a process of strategic planning for the future of the Center. 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.

The overall goal of the Center remains to 'nudge' society toward both a broader view of what cybersecurity means and a longer term vision of how to approach it. In our initial grant proposal, we argued that "the 'cyber' and the 'security' components of cybersecurity are fluid concepts in rapid motion." We thus proposed "that any long-term research program in cybersecurity must be grounded in a robust, flexible and evolving understanding of the 'possibility space' of cybersecurity. This understanding will in turn frame and construct how researchers investigate the decision processes and tools that cybersecurity professionals will need to develop in the coming decades."

As narrowly construed and outdated cybersecurity legislation makes its way through Congress, as policymakers debate whether encryption provides a virtual haven to newly energized terrorists, and as new technologies—especially in the Internet of Things—rapidly change what it means to engage in cyberspace, the need to broaden the scope of understanding of cybersecurity, and to engage in long-term thinking about what the future will look like, remain as relevant as ever. Our goal remains to achieve a UC Berkeley "School of Thought" around long-term cybersecurity; in other words, to make the Berkeley perspective indispensable to public and scholarly thinking around the subject, and to make sure those two discussions interconnect in meaningful and helpful ways that improve the quality of both.

The Center has achieved the primary goal we laid out for our first year of operation: to develop scenario futures for cybersecurity. In our initial grant proposal, we sought to "finish the first year with a coherent, manageable set of up to five realistic visions for the future of cybersecurity." As the year ends, a draft set of those scenarios is complete, and is currently under review by a variety of actors in the United States and abroad. The scenarios have already begun to 'nudge' the Berkeley research agenda toward a longer-term vision of cybersecurity, as evidenced by the results from Berkeley's first awarding of grants. Drawing on themes highlighted in the scenarios, projects on subjects as diverse as bio-sensing, cybersecurity norm development, human professional management, and artificial intelligence risks were all funded out of CLTC's first call for grant proposals.

Our work has led us to the view that the range of possibilities are even broader and more consequential than we envisioned in our initial proposal. The technology landscape is changing more rapidly than we acknowledged – the Internet of Things is growing rapidly, individualized prediction capabilities are expanding at scale, and sensors are getting increasingly capable of understanding what we are experiencing, and even what we feel. The markets for data are more volatile, suggesting that either the growth is real and will proceed at pace, or that a bubble may be underfoot, with surprising consequences relevant for security. And the cybersecurity landscape itself is changing; increasingly vigorous hacks—at the Office for Personnel Management, Sony and the like—suggest that the new security frontier is going to be highly uncertain and rapidly evolving. All of these possibilities have important implications for how a cybersecurity research and policy agenda needs to develop.

What has not changed is our ambition. CLTC aspires to be 'the' voice on long-term cybersecurity – the home of a school of intellectual and academic thought on the subject. In our first year, we have taken a diverse approach to achieving that goal. As time goes on, we anticipate necessarily narrowing our scope and focusing on a more selective set of research, educational, and outreach activities. But we believe that exploration will remain an important part of developing that concrete research agenda.

Steve Weber, Faculty Director
Betsy Cooper, Executive Director
December 31, 2015

The Year In Review

In this report, we provide an overview of our programs and activities during 2015, detailing key opportunities and challenges we faced along the way. We also identify key short and long-term goals for the coming years.

ORGANIZATIONAL DEVELOPMENT

CLTC spent its initial year engaged in organizational infrastructure building, including by hiring a multi-disciplinary workforce, setting up an office, developing initial branding materials, and hiring numerous consultants to achieve center goals.

Following several months of operations with a temporary workforce, CLTC hired in August an Executive Director, Betsy Cooper, to manage its organizational development and strategic planning, as well as to make substantial intellectual contributions to the work and agenda. This hire culminated after numerous months of searching for appropriate candidates. The executive director position is absolutely critical to CLTC's success both intellectually and organizationally.

CLTC has otherwise made use of consultant help: for example, we have employed a part-time communications coordinator, Chuck Kapelke, who assisted with events, website development and branding, and copy-editing. Other consultant hires during the first year of CLTC's operations include a web designer, a publications designer, and a copy-editor, as well as two assistants who helped coordinate our conference last May.

In its first year, CLTC also brought to Berkeley our first Senior Fellow, Jonathan Reiber, an extremely experienced researcher with seven years' cybersecurity experience at the Department of Defense. Jonathan aims to produce a book manuscript on cybersecurity and resilience during his time at CLTC. Unlike other 'fellowship' models, which largely treat fellows independently and leave them to their own research agendas, we have made the conscious decision not only to bring researchers advancing important parts of our agenda in house, but to make them integral parts of our day-to-day operations and activities. As such, we consider our fellows' activities during the reporting period to be an integral part of CLTC.

Throughout 2015, CLTC has also made significant strides in developing our organizational structure. CLTC maintains an internal Berkeley Advisory Committee with five members: UC Berkeley School of Information Dean AnnaLee Saxenian, Senior Advisor and Assistant Dean Jesse Goldhammer; Professor John Chuang; Professor Deirdre Mulligan; and Professor Doug Tygar. The Advisory Committee has provided strategic guidance on Center decisions, and served as key members of the CLTC's grant review committee as well.

CLTC is currently housed in a suite in South Hall, the home of Berkeley's School of Information. CLTC is looking to expand into larger office space in the coming year, to enable additional staff and researcher hires. CLTC has also developed a logo and joint UC Berkeley branding materials, and will look to develop additional materials next year to come.

ORGANIZATIONAL DEVELOPMENT: THE FUTURE OF CLTC

Goals for 2020: By 2020, we aspire to have a robust center that will at a minimum include 1) a deputy director, 2) an administrator, and 3) in-house multi-disciplinary researchers focused on key questions of the long-term cybersecurity research agenda.

Interim Goals for 2016:

- Find facilities capable of housing a 'center of the center', so that we can provide an academic community for CLTC fellows and those hired by our grants;
- Hire an administrative assistant to assist the executive director with operational tasks;
- Hire at least one additional in-house researcher focused on a key component of the research agenda; and
- Reorganize the structure of the Advisory Committee while considering options for external advisory support.

RESEARCH AND THOUGHT LEADERSHIP

CLTC engaged in two major research and thought-leadership initiatives in 2015: the development of scenarios for cybersecurity, and the allocation of approximately $1 million in grants to Berkeley researchers and their partners. In years to come, CLTC hopes to nudge the research agenda at Berkeley further in the direction of long-term cybersecurity, and to create a stronger 'center' of internal research being performed at the Center itself (i.e. in addition to the research activities that we fund elsewhere).

Scenarios for Cybersecurity Futures

In 2015, CLTC developed and distributed for review five scenarios for cybersecurity futures. These scenarios were developed out of a process that began in May 2015. The Center for Long-Term Cybersecurity brought together a broad interdisciplinary group from universities, the private sector, non-profits, and governments, and drew on their varied points of view and expertise to develop five prototype scenarios for the year 2020.

Scenario Workshop: Participants discuss futures for cybersecurity at the Marconi Center in May 2015.

Working with graduate students, the Center then refined and elaborated the scenarios to illuminate their potential impacts. We tried to strike a balance between developing the richness and complexity of each narrative, and making them accessible and digestible to the public. Our aim in writing these five scenarios is to create a usable representation of an imaginative map of the possibility space — stretched in some respects to the boundaries of plausibility — that researchers, decision-makers, and policy-makers can use to help navigate in the future.

The 2015 version of the scenarios has been made available, on a restricted basis, to key stakeholders and academics for engagement, commentary, and refinement. CLTC in December hosted a workshop with British stakeholders at Oxford University's Department of Politics and International Relations. Co-sponsored by CyberSecurity Oxford, and funded by the UK's Government Communications Headquarters (GCHQ), the seminar produced useful feedback on and engagement with the draft scenarios, which will be incorporated into the final versions, to be released to the public in early 2016.

CLTC is planning at least four additional engagement sessions on the draft scenarios: one in Berkeley, one in Singapore, and two to be held electronically to collect feedback from national and international stakeholders from outside the Bay Area. Further engagement will follow once the document is released to the public.

Research Funding

CLTC released our first call for proposals in August 2015. The call was carefully crafted to expand and refine understandings of and means of intervening in the cybersecurity problem space, broadly defined, as well as to stimulate the entry of new perspectives from cross-disciplinary collaborations and insights, in the interest of building capacity for on-going academic research input into the cybersecurity field. The RFP specifically requested that applicants reflect on emerging problems identified as part of the scenario development process.

CLTC GRANTEES 2015

Projects offered funding in 2015 include:

- Secure Machine Learning for Adversarial Environments (*Anthony Joseph & Doug Tygar*)
- Trust, Community, and the Production of Cybersecurity Professionals (*Ashwin Mathew & Coye Cheshire*)
- Constructing Intermediary Policies to Effectively Deter Financially-Motivated Cyber Criminals (*Damon McCoy, Chris Hoofnagle & Vern Paxson*)
- Robust Access in Hostile Networks (*David Fifield, Doug Tygar & Xiao Quang*)
- Defense Against Social Engineering Attacks (*David Wagner & Vern Paxson*)
- Blazar: Secure and Practical Program Hardening (*Dawn Song & Chao Zhang*)
- Cybersecurity: Meaning and Practice (*Deirdre Mulligan, Kenneth Bamberger & partners*)
- Social Media Data and Cybersecurity (*Galen Panger*)
- Privacy, Disclosure, and Social Exchange (*Jennifer King*)
- Unpacking Cybersecurity Information Sharing for an Emerging Future (*Jim Dempsey & Elaine Sedenberg*)
- Security and Privacy of Biosensing at Scale (*John Chuang, Tapan Parikh & partners*)
- (Im)balances of Power in the Age of Personal Data (*Paul Laskowski & Ben Johnson*)
- Security Behavior Observatory (*Serge Egelman & partners*)
- Using Individual Differences to Tailor Security Mitigations (Serge Egelman & Eyal Peer)

CLTC received a total of 50 proposals for review from faculty, staff, and graduate students affiliated with UC Berkeley. All proposals were peer-reviewed by at least two anonymous experts from the UC Berkeley community. Evaluation criteria included scholarly excellence; stretch and novelty of the proposal; relevance to real-world problems and particularly to long-term cybersecurity; interdisciplinarity; prospects for partnerships; and qualifications of researchers.

In total, CLTC made offers totaling $882,000 in grants to 19 projects across five departments. Because CLTC received such a great diversity of interesting and innovative proposals, we decided not to award any multi-year grants in this initial grant cycle.

In addition to $782,000 in seed and discrete project grants, CLTC also distributed $100,000 in 'research scoping' grants. These funds were distributed to discrete projects that showed great interest and promise, but were insufficiently developed to warrant full funding based on the initial proposal. Scoping grantees will be given a small amount of funds to begin work, and will receive the opportunity to submit a more developed research proposal in April 2016. CLTC has reserved and could elect to give up to $450,000 in additional funds to fully fund these scoping grantees at that time.

CLTC GRANTEES 2015 (CONT.)

Projects offered funding in 2015 include:

- Cybercrime Science: Understanding Cybercriminal Networks and the Effect of Disruption (*Sadia Afroz*)
- Cybersecurity as a Corporate Governance Issue (*Steven Davidoff Solomon & Adam Sterline*)
- Corrigibility in Artificial Intelligence Systems (*Stuart Russell & Patrick LaVictoire*)
- Illuminating and Defending Against Targeted Government Surveillance of Activists (*Vern Paxson, Bill Marczak & Nick Weaver*)
- The Internet's Challenge to the State (*Vinod K. Aggarwal, Andrew Reddie & Claire Tam*)

RESEARCH AND THOUGHT LEADERSHIP: THE FUTURE OF CLTC

Goals for 2020: Develop a multi-disciplinary research agenda that is directed by a vision of long-term cybersecurity, as elucidated in the scenarios and in future iterations thereof; nudge Berkeley researchers in the direction of pursuing that agenda; and hire internal researchers to sit within CLTC's 'core' to pursue elements of that agenda.

Interim Goals for 2016:

- Finish workshopping scenarios and release final version in early 2016;
- Host sessions across the world seeking engagement with the scenarios, for the purpose of inspiring the research and policy/real-world agenda and encouraging press and public coverage;
- Develop robust programming for new grantees, including seminar series at which results are reported; and
- Complete a second request for proposals, nudging research further in the direction of long-term cybersecurity.

EDUCATION

CLTC's educational programming is still under development, though we have made significant strides in our first year toward stronger investment in cybersecurity curriculum at Berkeley.

CLTC hosted a regular seminar series in 2015, focusing on emerging trends in cybersecurity. These seminars were regularly attended by 25 to 40 people, and involved active discussion as well as presentations of new material.

We invited speakers to highlight different prongs of cybersecurity that require additional long-term focus. For instance, Carey Nachenberg of Symantec presented an integrated security framework that centralizes the collection of information from a vast network to compile information about cybersecurity threats on a massive scale. Jonathan Reiber of CLTC similarly emphasized the importance of resilience in preparing for cyber attacks. Several speakers also emphasized privacy and data security; Joanne McNabb of the California Attorney General's office proposed a new default favoring privacy in online interactions, while Chief Technologist of the Federal Trade Commission Ashkan Soltani, in a talk cosponsored with Berkeley's Team for Research in Ubiquitous Secure Technology, emphasized the role of the law in protecting consumers from misleading technologies.

CLTC also began the planning process for additional educational programming, including an emerging leaders program and a course at Berkeley. CLTC is currently investigating opportunities to expand our direct impact on cybersecurity education, including UC Berkeley-based certificates or degrees, and possible course offerings.

LIST OF SELECTED 2015 SEMINARS

- Professor Steve Weber, introducing CLTC to the Berkeley campus at a CLTC Open House;
- David D. Clark, Senior Research Scientist, MIT's Computer Science and Artificial Intelligence Laboratory;
- Parisa Tabriz, Google's "Security Princess" and Director of Chrome Security;
- Chris Demchak, Professor | RADM Grace M. Hopper Chair of Cybersecurity at the U.S. Naval War College.
- Carey Nachenberg, Technical Fellow, Symantec;
- Jonathan Reiber, Senior Fellow, CLTC;
- Joanne McNabb, Director of Privacy Education and Outreach, CA Attorney General's Office; and
- Ashkan Soltani, Chief Technologist, Federal Trade Commission

EDUCATION: THE FUTURE OF CLTC

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

Interim Goals for 2016:

- Continue seminar series (confirmed speakers already include the Tanium CEO and CSO, David and Orion Hindawi; Peter Eckersley; and Vint Cerf); and
- Finalize plans for educational programming at UC Berkeley, and begin curriculum development.

Selected CLTC Seminars 2015

Joanne McNabb

Carey Nachenberg

Parisa Tabriz

Chris Demchak

Jonathan Reiber

COLLABORATION AND STRATEGIC COMMUNICATION

In addition to the above core activities, CLTC also engaged in a variety of other collaborative and strategic communications initiatives over the course of 2015. We review these activities in three categories: domestic collaboration, international collaboration, and strategic communications.

In general, CLTC sees strategic collaboration as essential to our overall goal of developing a Berkeley 'school of thought' around cybersecurity. So far, CLTC has engaged in such strategic engagement with a broad approach; in brief, we will have a coffee with anyone. Over time, CLTC hopes to approach collaboration using a more targeted effort, identifying key nodes of activity within long-term cybersecurity and selectively pursuing partners. However, in our first year, this broader approach has allowed us to get a better sense of the scope of existing cyber partnerships and activities.

Domestic Collaboration

CLTC engaged a number of key government, private sector, and nonprofit sector stakeholders over the course of its first year in operation. Below, we list some of our most significant engagements:

- CLTC leaders Steve Weber and Jesse Goldhammer took a scoping trip to Washington, DC, in March 2015, and met with officials from the Center for a New American Security (CNAS), CSIS, and numerous government agencies. One outgrowth of that trip was a collaboration between CLTC and CNAS on the development of the NextWare Cyber Collaboration Toolkit, a web-native, prototype set of interactive tools designed to encourage clearer communication and coordination among specialists who are approaching cybersecurity from a variety of technical and non-technical perspectives.

- In spring 2015, CLTC presented seminars on cybersecurity at Lawrence Livermore National Labs ("Cybersecurity Metaphors: How They Shape National Cyber Policy. Technical Research, and the Future of US National Security") and at the UC Berkeley Social Science Matrix ("Cybersecurity Metaphors and Futures").
- In collaboration with Ben Jensen, a Scholar in Residence at American University and an Assistant Professor at the Marine Corps University, CLTC is designing a set of cybersecurity 'games' that go significantly beyond conventional table-top exercises and will be used in experimental settings for the U.S. military.
- With help from CLTC supporter Sameer Bhalotra, former senior director for cyber security at the White House, CLTC has engaged in a number of C-level meetings with principals from top Silicon Valley firms. Many of these individuals will be visiting Berkeley for meetings with faculty and staff in the weeks to come.
- In October 2015, CLTC hosted CyberCom and NSA Director Admiral Rogers in a private, closed door event, and discussed possibilities for future collaboration. CLTC has been invited to bring Berkeley personnel to Fort Meade for further discussions and education about government activity in this space.
- CLTC is working with the Berkeley Center for Law, Business, and the Economy (BCLBE) to develop programming for high-level corporate officials on cybersecurity. The first step in this process was a dinner, held on December 16, 2015 with key corporate partners and legal counsel, to discuss how Berkeley can most helpfully engage in this space. BCLBE received a seed grant from CLTC to undertake a scoping research paper on this subject as well.

NSA/CyberCOM Visit: Faculty Director Steven Weber with Admiral Rogers

In addition to the above, CLTC has been actively engaged in planning for key events in 2016. Among those scheduled for early 2016:

- CLTC is a platinum sponsor of the 15th Annual Workshop on the Economics of Information Security (WEIS 2016), to be held at UC Berkeley between June 13-14, 2016. WEIS 2016 is a cross-disciplinary conference bringing together economists, computer scientists, legal scholars, business school researchers, security and privacy specialists, as well as industry experts to discuss information security, with findings to be released in a special issue of the *Journal of Cybersecurity*, a new, interdisciplinary, open-access journal published by Oxford University Press.

- CLTC is hosting a Government and Tech Conference on January 28, 2016 with the National Intelligence Council. The purpose of this conference is to provide specific input for the *Global Trends 2035* report, which will be delivered to the incoming federal administration in late 2016.

- Following on from CLTC's participation in the RAND Corporation's cybersecurity game in September 2015, CLTC and RAND will be co-hosting a second session of RAND's cybersecurity game in mid-February.

DOMESTIC COLLABORATION: THE FUTURE OF CLTC

Goals for 2020: Identify a handful of key government and private-sector strategic partners and develop concrete agenda for joint projects.

Interim Goals for 2016:

- Continue to develop high-priority government, private sector, and non-profit relationships;
- Identify and establish at least one engagement that seeks to diversify the population working in the cybersecurity field (e.g., women and minorities); and
- Evaluate the possibility of establishing a C-level advisory committee to seek key feedback on relevant trends developing in the private sector.

International Cooperation

CLTC was actively engaged in international activities over the course of 2015. In addition to the scenario workshop held at Oxford in December 2015, examples of key activities include:

- CLTC and partners in France held a workshop on digital sovereignty and intermediation platforms in France on December 8-10, 2015. Fifteen partners, including representatives from Microsoft, *The New Yorker* magazine, the insurance industry, and domestic and international academic institutions met to discuss possible challenges presented by intermediation platforms to current conceptions of sovereignty, and to consider concrete research projects derived from those challenges.

- CLTC has agreed to fund a researcher at Singapore Management University to develop a plan for a future partnership on cybersecurity. We will conduct a workshop around our scenarios in Singapore in February 2016 to get this process started.

- CLTC fellow Jonathan Reiber gave a presentation on cybersecurity defense and resilience to 2,000 people at Microsoft's biggest conference in India, and conducted numerous interviews and engagements with Indian personnel while there. Reiber will be returning to India in February.

INTERNATIONAL COOPERATION: THE FUTURE OF CLTC

Goals for 2020: Establish key 'nodes' of international cooperation, with ongoing research projects and a strong agenda for partnership.

Interim Goals for 2016:

- Develop research agenda on platforms and digital sovereignty, in preparation for an expanded meeting and publications in 2016;
- Finalize Singapore node of research agenda;
- Identify and begin to develop a partner in the developing world.

Strategic Communications

During the past year, CLTC has made significant strides in establishing a public presence through strategic communications. We developed and launched our first website, which was custom-designed and covers (through video and text) select news items related to cybersecurity, as well as CLTC activities. CLTC also developed the infrastructure to implement Facebook and Twitter feeds so we can maintain a more dynamic internet presence.

CLTC has built an e-mail list of more than 300 people, largely in the Berkeley area, and we send regular, professionally designed announcements about events, news, and opportunities. In the New Year, CLTC will launch a weekly events list for events not just at Berkeley, but in the Bay Area. This will hopefully extend CLTC's reach to new partners beyond the Berkeley campus. Our senior fellow, Jonathan Reiber, is also developing several op-eds for publication.

STRATEGIC COMMUNICATIONS: THE FUTURE OF CLTC

Goals for 2020: Have a robust public profile and help establish UC Berkeley and the CLTC as a key resource for expertise on issues of cybersecurity.

Interim Goals for 2016:

- Develop a robust communications plan for public dissemination of CLTC work products, including contact with print and electronic media;
- Establish a weekly 'cyber events in the Bay area' list, in order to expand the range of CLTC announcements;
- Launch and maintain active Facebook and Twitter feeds to disseminate progress and results of Berkeley-funded research.

FUNDRAISING

CLTC's approach to fundraising has been necessarily reserved in our first few months of full operation, and so our fundraising strategy is still under development. We have taken initial steps to develop fundraising relationships, including by meeting with university fundraisers; engaging with high net worth corporate individuals; and discussing joint research activities with prospective corporate sponsors.

FUNDRAISING: THE FUTURE OF CLTC

Goals for 2020: Develop a self-sustaining organization with a robust funding model. Outlets under consideration may include a board of directors, corporate sponsorship, membership fees, etc.

Interim Goals for 2016:

- Publish public version of this annual report to facilitate future fundraising;
- Develop a robust fundraising plan and strategy; and
- Generate small-level private donations and/or co-sponsored research.

Reactions and the Way Forward

In our first year, we have been deliberate and intentional in laying the groundwork for longer term impact and a sustainable presence on the UC Berkeley campus and beyond. We have focused on learning, forming an intellectual community, preparing scenarios, getting our organization up and running, and giving out the first tranche of research grants.

We have made significant progress toward a key short-term goal: to successfully become the center of gravity for UC Berkeley's community of cybersecurity scholars. Berkeley had no previous central hub for cybersecurity work that could bring together the diverse scholars working across the campus. This created a unique gap for CLTC to fill. Our Center is now beginning to bring together in a meaningful way faculty across diverse disciplines for events and research projects, and to bring more consistent and high-quality cybersecurity programming to Berkeley. CLTC will work in our second year to expand that community further to scholars who do not work on traditional cybersecurity topics.

Contact Information

STEVE WEBER FACULTY DIRECTOR	BETSY COOPER EXECUTIVE DIRECTOR
steve.weber@icloud.com	bcc9@berkeley.edu

CLTC
Center for Long-Term Cybersecurity
UC Berkeley

Center for Long-Term Cybersecurity
102 South Hall
510-664-7506
cltc.berkeley.edu
@cltcberkeley