UC BERKELEY

CENTER FOR LONG-TERM CYBERSECURITY

2018

ANNUAL REPORT

Contents

Letter from the Directors

The future of digital security issues arrives more quickly and with broader repercussions than most firms, societies, governments, and people are organized to plan for. The cybersecurity world spent 2018 again racing from one crisis to another, with a growing sense that problems are accelerating faster than the world's collective ability to identify and implement solutions.

At the core of all these developments, as ever, lies the human-technology nexus. This tenet has guided the UC Berkeley Center for Long-Term Cybersecurity (CLTC) since our inception. In 2018, we deepened and extended our work at this nexus with new partners, in new geographies, and on new issue-areas that we believe benefit from longer-term perspectives on how to preserve and extend the promise of digital technologies to improve the human experience.

After more than a year of careful planning and pilot initiatives, we officially launched the Citizen Clinic, a flagship CLTC initiative through which UC Berkeley students can gain practical training while working to improve the digital security of politically vulnerable organizations and communities.

At the request of the World Economic Forum (WEF), we engaged in a year-long collaboration to take a set of long-term scenarios for the year 2025 to a series of workshops—in Palo Alto, Munich, Singapore, Hong Kong, Moscow, Geneva, and Washington, DC—to compare how people and organizations in different parts of the world perceive trade-offs in emerging cybersecurity issues. We published the insights from this work at the annual meeting of the WEF Global Centre for Cybersecurity in November, and we will continue to build on this work in 2019.

We deepened our corporate engagement model to build research partnerships with industry on specific issues; these partnerships represent a real opportunity to shape policy on issues ranging from attack attribution and accountability to the role of the CISO in enterprise.

Meanwhile, we have continued to help expand the depth and reach of UC Berkeley's new Master of Information and Cybersecurity (MICS) degree program at the School of Information, which is delivered fully online and will graduate its first cohort in 2019.

Events of 2018 have further affirmed that the cybersecurity problem is growing in scale, scope, and significance. From the rise of artificial intelligence to diverging international norms around surveillance and privacy, technology is reshaping global society. Through our focus on research, teaching, and engagement with public- and private-sector institutions, the Center for Long-Term Cybersecurity helps people and organizations anticipate and address tomorrow's information security challenges, in order to amplify and extend the upside of the digital revolution.

After more than a year of careful planning and pilot initiatives, we officially launched the Citizen Clinic, a flagship CLTC initiative through which UC Berkeley students can gain practical training while working to improve the digital security of politically vulnerable organizations and communities.

Steve Weber,
Faculty Director
January 31, 2019

Ann Cleaveland,
Executive Director
January 31, 2019

Introduction

The Center for Long-Term Cybersecurity is a hub for research and scholarship at the world's premier public university; a convening platform for candid dialogue and problem-solving about cybersecurity challenges and solutions; a resource for educating the broader community, including media, practitioners, and the public; and an incubator for people and programs that will shape the future of cybersecurity debates for years to come.

This report reviews CLTC's accomplishments for 2018, with key opportunities and challenges that we faced as we look ahead to 2019. Additional information about most of the initiatives outlined in this report—including publications—can be found at https://cltc.berkeley.edu.

Research and Leading Scholarship

Throughout 2018, CLTC made progress in advancing an integrated research platform while establishing our thought-leadership on a broad range of issues related to cybersecurity. We expanded our internal research capacity and allocated funding to a diverse group of researchers working across the UC Berkeley campus and beyond, with an emphasis in four key areas: artificial intelligence, expanding the cybersecurity talent pool, exploring new regulatory and governance structures to support cybersecurity, and protecting vulnerable populations online.

IN-HOUSE RESEARCH CAPACITY

2018 marked the first year that CLTC was fully staffed with in-house research capacity, and we ended the year with five full-time-equivalent researchers on staff. In January, having already hired Sean Brooks as Research Fellow and Director of Citizen Clinic, we welcomed Research Fellow Jessica Cussins Newman, who was previously the AI policy lead at the Future of Life Institute. In the spring, Jessica conducted

2018 marked the first year that CLTC was fully staffed with in-house research capacity, and we ended the year with five full-time-equivalent researchers on staff.

Jessica Cussins Newman

Tarunima Prabhakar

Steve Trush

Nick Merrill

research focused on cyberattack attribution and identified major shifts—in scale, origin, transparency, and coordination—in how attacks on nation-states were attributed between 2007 and today. In addition, Cussins Newman has published research addressing policy questions around the security implications of artificial intelligence.

Our third Research Fellow, Tarunima Prabhakar, conducts research on classification and discrimination by machine learning in India. Prabhakar, who earned her masters degree at the Goldman School of Public Policy, is investigating private- and public-sector uses of AI, machine learning, and predictive analytics in India, with a specific focus on applications in health and finance.

In August, CLTC welcomed Steve Trush as a fourth Research Fellow and Nick Merrill as a Post-Doctoral Fellow. As a member of the United States military and other federal government agencies, Trush has spent over a decade supporting international security initiatives, with work ranging from data analysis and policy advising to technology development and training. He serves as Deputy Director of Citizen Clinic, and he has begun research focused on helping civil society organizations counter the risks and harms of disinformation and harassment. Merrill completed his Ph.D. at the UC Berkeley School of Information in 2018; his dissertation focused on the implications of 'mind-reading machines,' devices that can read or decode what people are thinking or feeling. Since arriving at CLTC, Merrill has focused his research on such questions as how people encounter security in their day-to-day lives.

VISITING SCHOLARS

CLTC has been honored to host a group of outstanding visiting scholars from outside institutions, all of whom are important contributors to interdisciplinary cybersecurity scholarship and collaborations. In 2018, we hosted: Ashwin Mathew, a Ph.D. from the School of Information who studies the governance of the internet through a

Ashwin Mathew

Naazneen H. Barma

L. Jean Camp

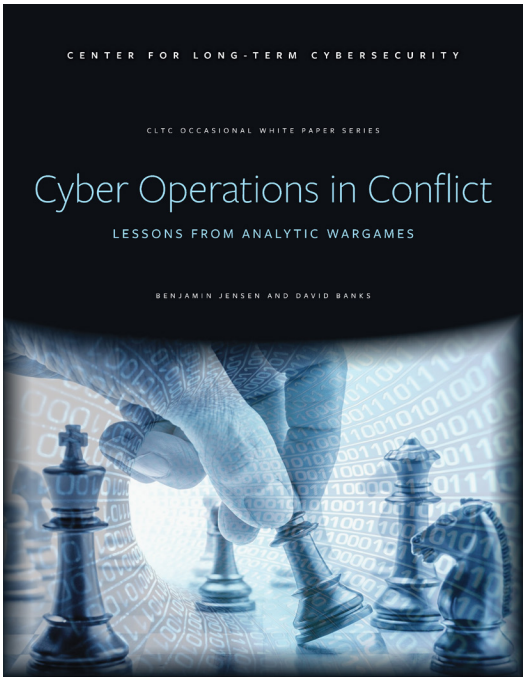
Brent Durbin

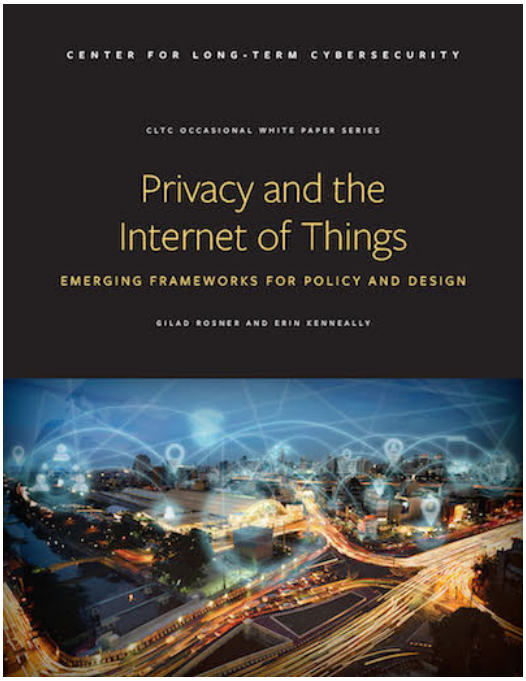
blend of sociological and technological analysis, and who is investigating trust relationships in the practices of information security professionals; Naazneen H. Barma, Associate Professor of National Security Affairs at the Naval Postgraduate School in Monterey, California, who is extending her work on the political economy of development and natural resource governance to the digital realm, with a special emphasis on the development consequences of machine learning; L. Jean Camp, Professor at Indiana University's School of Informatics and Computing, who is a founder of the interdiscipline of economics of security; and Brent Durbin, Associate Professor of Government at Smith College in Northampton, Massachusetts, who is extending his work on state-intelligence relationships to take account of the importance of data science in government-to-government interactions. These visiting scholars are expanding CLTC's reach and network while making important contributions that are aligned with the Center's research agenda.

CLTC WHITE PAPERS

2018 also saw the publication of three 'white papers,' reports authored by CLTC staff and grantees that are designed and disseminated with the support of the CLTC communications team.

In April, we published *Cyber Operations in Conflict: Lessons from Analytic Wargames*, a research project based on a novel methodology that suggests policymakers and military leaders may need to broaden their assumptions about how state and non-state actors—including nation-states, non-state organizations like ISIS, cyber-activist groups such as Wikileaks, and other groups—are likely to use hacking and other cyber operations in future crises and conflicts. The report's authors—Benjamin M. Jensen, associate professor at the Marine Corps University and scholar-in-residence at American University's School of International Service, and David Banks, professorial lecturer at American University—used analytic wargames, an innovative tool that investigates competition among diverse actors, to identify strategic preferences in two hypothetical contexts. Their study found that cyber operations are not likely to be

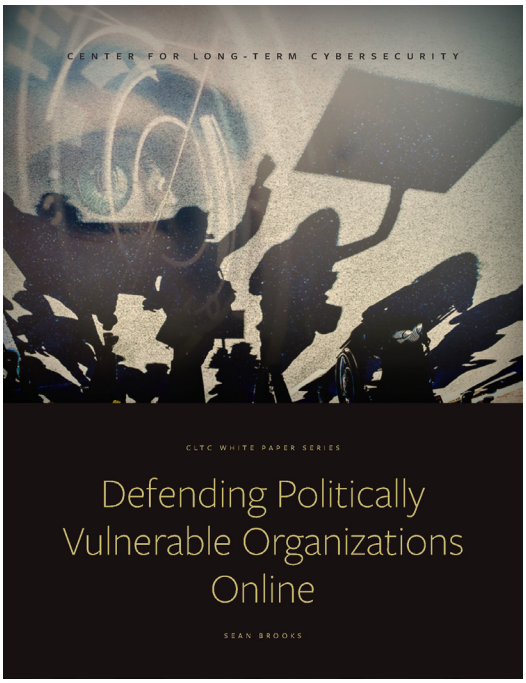


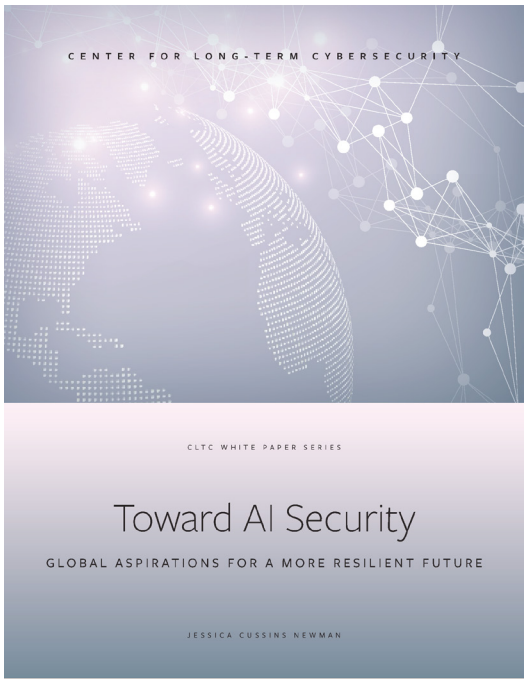


used for provocative conflict escalations, but rather provide a moderating influence by offering states a means of managing escalation 'in the shadows.' CLTC also helped draft and place an op-ed related to this report in the *Washington Post*'s Monkey Cage blog.

2018 also saw the publication of three 'white papers,' reports authored by CLTC staff and grantees that are designed and disseminated with the support of the CLTC communications team.

In June, we published *Privacy and the Internet of Things: Emerging Frameworks for Policy and Design*, produced in partnership with researchers from the Internet of Things Privacy Forum. The paper provides an overview of some of the key privacy issues resulting from the expansion of the IoT, as well as emerging frameworks that could help policymakers and corporate leaders reduce potential harms through regulation and product design. The authors—Gilad Rosner, Founder of the IoT Privacy Forum, and Erin Kenneally, who works with the U.S. Department of Homeland Security's Science & Technology Directorate—conducted workshops and interviews with scholars, regulators, industry practitioners, and other experts, and they completed a robust review of existing scholarship about privacy and the IoT. In addition to helping produce the report, CLTC supported the authors in placing an op-ed in *The Hill*.





CLTC has continued to support important new research focused on the cybersecurity needs of vulnerable populations. Research Fellow Sean Brooks has led our work in this area, and in July, CLTC published his report, *Defending Politically Vulnerable Organizations Online*, which provides an overview of the cybersecurity threats facing civil society organizations that may be targeted for political purposes, as well as what resources are (and are not) available to help these organizations improve their cybersecurity. Brooks 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. His research 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. His report earned coverage from the CBC, *Wall Street Journal*'s CyberPro Newsletter, and other media outlets, and it directly informed the work of Citizen Clinic, a new program (described in subsequent sections) focused on improving security and privacy for politically vulnerable organizations and communities.

CLTC Research Fellow Jessica Cussins Newman conducted a broad survey of different nations' artificial intelligence strategies. In early 2019, she published a report, *Toward AI Security: Global Aspirations for a More Resilient Future*, that introduces a new framework for global artificial intelligence security alongside an analysis of government strategies from around the world, including the U.S., China, France, and

RESEARCH

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 sit within CLTC's 'core' to pursue elements of that agenda.

Interim Goals We Targeted 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

India. The report highlights significant divergences between government approaches to the security implications of AI, and identifies numerous synergies that can be leveraged to support global coordination. The paper uses the lens of global AI security to investigate the robustness and resiliency of AI systems, as well as the social, political, and economic systems with which AI interacts.

CAMPUS GRANTMAKING

In 2018, CLTC committed more than $1 million in funding to 39 different research initiatives, including 13 renewal grants from 2017. As with previous grant periods, CLTC supports two types of grants: 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. (For a list of projects funded in 2018, please see page 11.)

The purpose of our research funding is to address the most interesting and complex challenges of today's socio-technical security environment and to grapple with the broader challenges of the next decade's environment. The Center focused our efforts in four priority areas: machine learning and artificial intelligence, building the cyber-talent pipeline, improving cybersecurity governance, and protecting vulnerable populations online. The funded projects included important issues such as improving the cybersecurity of local governments; protecting vulnerable individuals and organizations from state surveillance; defending against social engineering attacks; understanding the security implications of 5G networks; developing secure contracts through blockchain; and more. All principal investigators (PIs) have a UC Berkeley research affiliation, but many of the initiatives involve partners from outside institutions, including Bar-Ilan University, Carnegie Mellon, the City and County of San Francisco, New York University, Norwegian University of Science and Technology, The Policy Lab, the United States Department of Agriculture, University of British Columbia, University of Michigan, and the University of Washington.

CLTC has received praise for our efforts to create a community of cybersecurity researchers at UC Berkeley and beyond, and in 2018 we engaged our grantees in diverse ways, including by connecting members of the CLTC research community with private-sector partners and public-sector policymakers.

RESEARCH IMPACT

Following are highlights from the many accomplishments of our in-house and extended community of researchers in 2018:

- CLTC Grantee Amit Elazari has steadily led the industry toward a standardization of legal terms to minimize the legal risks for good-faith hackers participating in bug bounty programs. In 2018, Elazari launched Disclose.io, a collaborative

effort to create an open-source standard for bug bounty and vulnerability-disclosure programs. In March, she successfully lobbied DropBox to expand its policy to include a pledge to not allege copyright infringement against good-faith participants in its bug bounty program, and Mozilla cited Elazari's work as the inspiration behind changes to its bounty program policies. Elazari's work was also published in "Economics of Vulnerability Disclosure," a paper released by the European Union Agency for Network and Information Security (ENISA).

- February saw the publication of "A Fragmented Whole: Cooperation and Learning in the Practice of Information Security," by UC Berkeley School of Information Professor Coye Cheshire and Visiting Scholar Ashwin J. Mathew. Mathew worked at multiple UC campuses to engage information technology teams and other departments in a collaborative effort to investigate information security cooperation and learning among higher education institutions, particularly the UC system. His research showed how risk and uncertainty can be navigated by developing trust relationships among information security professionals, both within a campus and across the system.
- A team of CLTC grantees released a paper revealing how deep learning is vulnerable to information leakage. In "The Secret Sharer: Measuring Unintended Neural Network Memorization & Extracting Secrets," the researchers— Nicholas Carlini, Chang Liu, and Dawn Song, along with Jaernej Kos and Úlfar Erlingsson—introduced 'exposure,' a simple-to-compute metric that can be applied to any deep learning model for measuring the memorization of secrets. Using this metric, they detailed how to extract those secrets efficiently using black-box API access.
- In April, a team of CLTC-affiliated researchers led by Serge Egelman published "Won't Somebody Think of the Children? Examining COPPA Compliance at Scale," in the journal *Proceedings on Privacy Enhancing Technologies*. The researchers analyzed the privacy settings of 6,000 child-directed Android apps; they found that well over half of the apps potentially violated the U.S. Children's Online Privacy Protection Act (COPPA). This research was detailed in the *New York Times* and has led state governments to take legal action against the app developers.
- CLTC Faculty Director Steve Weber and UC Berkeley School of Information Ph.D Student and 2018 CLTC grantee Shazeda Ahmed published a paper in *First Monday* titled "China's Long Game in Techno-Nationalism," which explored how the passage of China's national cybersecurity law in June 2017 was interpreted as an unprecedented impediment to the operation of foreign firms in the country. Weber and Ahmed argued that economic concerns have consistently overshadowed claims of national security considerations throughout laws directed at foreign enterprises.
- In May, CLTC grantees Aniket Kesari, Chris Hoofnagle, and Damon McCoy released "Deterring Cybercrime: Focus on the Intermediaries," published in the *Berkeley Technology Law Journal*, which chronicled how enforcers are using the law to police cybercrime. The authors described how intellectual property owners, technology companies, and law enforcement agencies employ a "deterrence by denial" strategy, which entails disrupting access to cybercriminals' intermediaries, including domain registrars, web hosts, payment providers, banks, and even shipping companies.
- Grantees Alice M. Agogino, Danielle Poreh, Euiyoung Kim, and Matilde Bisballe Jensen published "Novice Designers' Lack of Awareness To Cybersecurity and Data Vulnerability in New Concept Development of Mobile Sensing Devices" on the Design Society website. Their research focused on the privacy awareness of vulnerable users of mobile sensing devices and co-robots in domestic settings. Drawing upon user approaches to phishing and malware in the online domain, the researchers aimed to create relevant guidelines on cybersecurity behavior for private users, and to inform designers on how to more effectively build cybersecurity into their product design.
- Nicholas Carlini and David Wagner won the Best Paper Award at the 1st Deep Learning and Security Workshop, which was held in May as part of the 39th IEEE Symposium on Security and Privacy. In their paper, "Audio Adversarial Examples: Targeted Attacks on Speech-to-Text," the researchers demonstrated that they could make small changes to audio files and embed commands directly into recordings of music or spoken text in order to trick smart devices such as Apple's Siri, Amazon's Alexa, and Google's Assistant. This research was profiled in the *New York Times*.
- A team of CLTC grantees published "rIoT: Quantifying Consumer Costs of Insecure Internet of Things Devices," which sought to identify the costs to consumers of DDoS attacks on IoT devices. The researchers explored potential implications of these issues and discussed regulations that could be used to promote more a secure IoT ecosystem in the future.

In 2018, CLTC committed more than $1 million in funding to 39 different research initiatives, including 13 renewal grants from 2017.

CLTC 2018 RESEARCH GRANTEES

BELOW IS A LIST OF THE PROJECTS FUNDED BY THE CENTER FOR LONG-TERM CYBERSECURITY THROUGH OUR 2018 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 for Urban Infrastructure | Alison E. Post, Associate Professor, Political Science and Global Metropolitan Studies, 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, Education Director of the Blum Center for Developing Economies; Euiyoung Kim, Postdoctoral Design Fellow, Jacobs Institute for Design Innovation, 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, Professor, 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; Dr. Anat Peleg, Lecturer, Faculty of Law and Director of the Center for the Study of Law, Media at 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

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

rIoT: Quantifying IoT Costs and Harms | Kimberly Fong, MIMS student, UC Berkeley School of Information; Kurt Hepler, MIMS student, UC Berkeley School of Information; Rohit Raghavan, MIMS student, UC Berkeley School of Information; Peter Rowland, MIMS student, UC Berkeley School of Information

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, Carnegie Mellon University; Nicolas Christin, Assistant Research Professor in Electrical and Computer Engineering, Carnegie Mellon University; Rahul Telang, Professor of Information Systems and Management, Heinz College, Carnegie Mellon University

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

- Grantee Ahmad Sultan published research based on interviews with nearly 300 individuals from vulnerable populations (e.g., elderly, low-income, and English-learners) in the City and County of San Francisco. Sultan found several sobering insights about the potential risks and harm that such individuals experience when conducting online activities, and called for new solutions to improve the cybersecurity awareness of vulnerable populations. Sultan has engaged with the San Francisco Tech Council and other civic leaders to explore potential solutions.
- CLTC grantee Melissa K. Griffith published multiple papers examining cybersecurity policy in Europe and beyond. In October, Griffith published "A comprehensive security approach: bolstering Finnish cybersecurity capacity" in the *Journal of Cyber Policy*, which highlighted how Finland has established unusually robust cybersecurity capacity and competency. She also co-wrote "International Security and the Strategic Dynamics of Cyber Conflict," which was released as part of the Cyber Conflict Studies Association's Cyber Conflict State of the Field conference, and "Strengthening the EU's Cyber Defence Capabilities," published for the Centre for European Policy Studies, which makes the case for greater cyber defense coordination within the EU.
- In September, CLTC grantees Max Curran, Nick Merrill, Swapan Gandhi, and Professor John Chuang received the Best Student Paper award at the International Conference on Physiological Computing Systems (PhyCS 2018) in Seville, Spain. The researchers developed a custom-fit earpiece that can capture 'passthoughts' through brainwave signals from the ear canal, demonstrating one-step, three-factor authentication for the first time.
- CLTC Research Fellow Tarunima Prabhakar won first place in "AI and the News: An Open Challenge," a competition sponsored by the Ethics and Governance of AI Initiative. Her project "Tattle" seeks to address the challenge of misinformation disseminated through WhatsApp in India.
- In December, CLTC grantee and professor Anil Aswani, from the Industrial Engineering & Operations Research Department (IEOR) in the UC Berkeley College of Engineering, published research in JAMA Network showing it is possible to use artificial intelligence to identify individuals by collecting physical activity from wearable devices and correlating it to demographic data. His research suggests that current laws and regulations are insufficient to ensure the privacy of an individual's health status, and that there is a broader threat to the privacy of health data. *USA Today* published an op-ed on this issue that CLTC supported Aswani to write and place.
- CLTC grantees Elaine Sedenberg, John Chuang, and Richmond Wong published their research on the privacy and surveillance implications of remote biosensing in an academic book released as part of the Routledge Studies in Surveillance series. *Surveillance, Privacy, and Public Space* included the CLTC-funded paper "A window into the soul: Biosensing in public," which examined the unique nature and inferential potential of biosensed data by creating a taxonomy of signals that may be collected remotely or from traces left behind, and considered how these data may be used to create novel privacy concerns, particularly in public.
- In a report published by the *Journal of Cyber Policy* in December, CLTC grantees Vinod Aggarwal and Andrew Reddie evaluated the roles of firms, governments, and other key stakeholders in the rise of industrial policy in important states in the cybersecurity industry. Their paper, "Comparative Industrial Policy and Cybersecurity: A Framework for Analysis," centered on the U.S., China, Taiwan, Japan, the EU, and key European states. The researchers also published "Comparative Industrial Policy and Cybersecurity: the US Case," focused on how the U.S. government's industrial policy addresses cybersecurity market failures.

CLTC supports two types of grants: 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.

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 progress in this area in 2018.

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

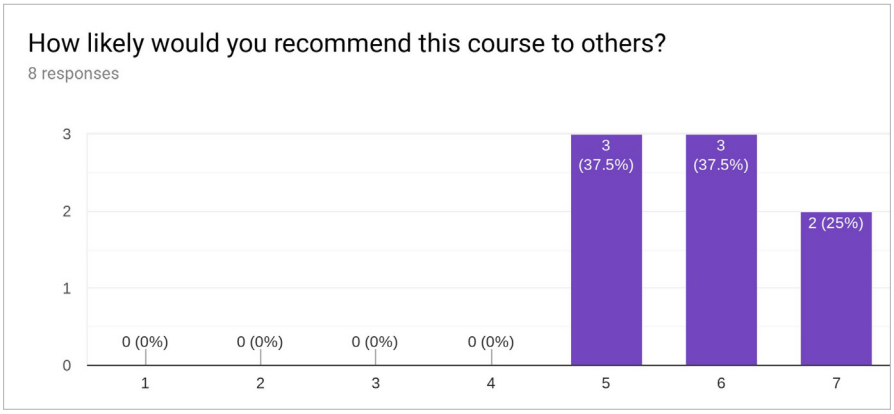
In 2017, CLTC helped plan "cybersecurity@berkeley," a Master of Information and Cybersecurity (MICS) online degree program taught by UC Berkeley faculty members and offered through the School of Information. The past year brought the launch of this exciting new program, as the first cohort of students began classes in June 2018. CLTC has continued to support the MICS program in diverse ways. We were involved in the process of hiring the Academic Program Manager, and welcomed Lisa Ho to that position in March. CLTC is actively helping to connect MICS students and industry leaders through webinars, on-campus 'immersion' events, and customized mentorship programs. We are also experimenting with approaches to engage MICS students in the public-interest work of the Citizen Clinic.

Lisa Ho

CITIZEN CLINIC

As a highlight for 2018, CLTC was proud to launch Citizen Clinic, a first-of-its-kind public interest cybersecurity program that provides pro bono services to politically vulnerable individuals or organizations that are at risk of cyberattack. Citizen Clinic is based on a clinical model (similar to a law clinic or medical clinic), in which students work with real-world clients and have a unique opportunity for experiential learning; we know of no other academic institution that is delivering such a program.

With support from the MacArthur Foundation, Citizen Clinic is offered through the School of Information as a class called "Public Interest Cybersecurity: The Citizen Clinic Practicum." Taught by CLTC Research Fellows Sean Brooks and Steve Trush,



Client organizations and participating students have provided positive feedback about Citizen Clinic.

EDUCATION

Goals for 2020

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

Interim Goals We Targeted for 2018

- Successfully launch the first cohort of the MICS degree program
- Develop new training programs to support diversity in cybersecurity education

with supervision from CLTC Faculty Director Steven Weber, the course provides students with real-world experience in developing and implementing sound cybersecurity practices needed to protect politically vulnerable organizations and persons around the world. Working with civil society organizations as clients, students learn how to assess vulnerabilities and develop, recommend, and perform mitigating controls for security risks; they learn about both the theory and practice of baseline digital security, the intricacies of protection for largely under-resourced organizations, and effective risk management in complex political, sociological, legal, and ethical contexts. The emphasis is on pragmatic, workable solutions that client organizations can feasibly implement in effective ways.

Over the course of 2018, students and staff provided services to partner organizations, including (but not limited to) contextualized risk assessments, network and third-party service audits, secure survey design, endpoint configuration and encryption, secure communications deployment, improved authentication practices, and cloud migration planning. Our partners represent a broad diversity of communities at risk of cyberattacks, including women's reproductive healthcare providers and advocates, transgender community members in crisis, indigenous communities in the Amazon basin, and digital rights advocates in Latin America. Students also represent a diverse cross-section of the UC Berkeley student body, including undergraduates, graduates, and doctoral students from a variety of programs, including computer science, law, public policy, and the School of Information.

The Clinic has received positive feedback (see graph on page 14) and has continued to gain traction; as of January 2019, the program has expanded from eight to nearly twenty students supporting four partner organizations. In response to feedback, this will also include at least four students participating in an advanced class that provides for deeper technical work with selected clients. CLTC is pursuing additional funding in order to expand the Clinic's capacity to serve more partner organizations with a wider range of services.

TEACHING AND SEMINARS

The Spring and Fall 2018 semesters saw the continuation of "Info 290: Future of Cybersecurity Policy Reading Group," a two-credit reading group in which students discussed contemporary cybersecurity policy problems. Taught by 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.

CLTC has also continued to support cybersecurity education at UC Berkeley through our Seminar Series. CLTC seminars typically attract between 25–50 attendees, and

Left: Andrew Ferguson and Catherine Crump
Right: Juliana Schroeder

Habeas Data panel discussion

are also open to the public. CLTC is committed to making these events as accessible as possible through livestreaming and social media engagement. Following are brief summaries of our 2018 Seminar Series events:

- In March, Catherine Crump, Assistant Clinical Professor of Law at Berkeley Law, and Andrew Guthrie Ferguson, Professor of Law at UDC David A. Clarke School of Law, presented "A Conversation on Big Data, Surveillance, and Policing," focusing largely on how data and surveillance are shaping local governments and law enforcement agencies.
- Also in March, CLTC presented a seminar with Juliana Schroeder, who discussed "Mistaking Minds and Machines: How Cues in Language Affect Evaluations of 'Humanness'." Schroeder, Assistant Professor in the Haas Management of Organizations Group, presented her research on how people interpret communication differently based on whether it comes from machines or other human beings.
- In April, Doug Tygar, Professor of Computer Science and Professor of Information Management at UC Berkeley, presented a seminar on "Adversarial Machine

Herb Lin

Kristen Eichensehr

CLTC has continued to support cybersecurity education at UC Berkeley through our Seminar Series.

Learning," which outlined some of the major security challenges facing developers of machine-learning algorithms.

- In August, CLTC's Fall Seminar Series kicked off with "Habeas Data," a panel discussion focused on what citizens can do to ensure that the powerful surveillance technologies available to city and state governments are used responsibly, with sufficient transparency and oversight. The panel featured Cyrus Farivar, a senior technology policy reporter at Ars Technica and author of the book *Habeas Data*. The panel was moderated by Steve Trush, Research Fellow for CLTC; panelists included Deirdre K. Mulligan, Associate Professor in the School of Information; Catherine Crump, Assistant Clinical Professor of Law; and Camille Ochoa, Coordinator, Grassroots Advocacy, Electronic Frontier Foundation.
- In October, Herb Lin, a senior research scholar for cyber policy and security at the Center for International Security and Cooperation and Hank J. Holland Fellow in Cyber Policy and Security at the Hoover Institution, both at Stanford University, delivered an interactive talk called "Complexity and Security: Managing the Tradeoffs," which addressed some of the trade-offs between security and efficiency of design.
- In November, Kristen Eichensehr, Assistant Professor at UCLA School of Law, presented "Digital Switzerlands," which explored the evolving role of increasingly powerful U.S. technology companies. Eichensehr explained that two primary characteristics—parity and neutrality—have shaped the emergence of companies as "digital Switzerlands."

Engagement

A major part of CLTC's mission is to serve as a translator that connects research and education with practitioners and the public, and as a convening platform for dialogue and problem-solving across government, academia, and the private sector. Below we describe highlights from our engagement and collaboration efforts in 2018, including highlights from our strategic communications efforts, which represent a key piece of our engagement strategy.

Cybersecurity Futures 2025 Project: At the request of the World Economic Forum's Global Centre for Cybersecurity (C4C), CLTC has led an effort to address the growing chasm between today's operational security agenda and the range of cybersecurity challenges likely to emerge in the coming years. The project focused on shaping a forward-looking research and policy agenda that is more intellectually and practically robust—and more broadly applicable across countries and regions.

In 2018, together with CNA's Institute for Public Research (CNA), we brought four alternate future scenarios to seven international workshops around the world—including Palo Alto, Munich, Singapore, Hong Kong, Moscow, Geneva, and Washington, DC.

In 2018, together with CNA's Institute for Public Research (CNA), we brought four alternate future scenarios to seven international workshops around the world—including Palo Alto, Munich, Singapore, Hong Kong, Moscow, Geneva, and Washington, DC—to compare how people and organizations in different parts of the world assess the trade-offs around a range of emerging cybersecurity issues. These workshops brought together over 200 experts and decision-makers from government, industry, civil society, academia, and other domains.

This project resulted in multiple outputs designed to inform decision-makers in different sectors, and to help reduce detrimental frictions and expose opportunities for cooperation. Our report, "Cybersecurity Futures 2025: Insights and Findings," was released at the annual meeting of the C4C in Geneva in November. In line with our goals to translate research findings to the public in compelling, creative ways, we also created a website, cyberfutures2025.org, that allows users to virtually experience the Cybersecurity Futures 2025 workshop environment and interact with some of the key findings. The site features a video of Walter Parkes, writer and producer of iconic cybersecurity films such as *WarGames*, *Sneakers*, and *Minority Report*, in an introductory video, and four short videos that illustrate different futures for the world in 2025. The site also features a decision-making heuristic that walks users

ENGAGEMENT

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 We Targeted for 2018

Continue to identify strategic partnerships in our priority areas (artificial intelligence and machine learning; cyber talent pipeline; governance regimes; protecting vulnerable people online) and begin to develop those partnerships.

through a series of questions to create a customized framework for determining priorities and assessing near-term investment choices to prepare for the future.

The insights that emerged through this project are helping decision-makers in multiple arenas to engage with tomorrow's cybersecurity challenges and lift out of "today's attack" to anticipate what's around the corner. In 2019, we have been invited to extend the scenarios and the work resulting from this project to new audiences, locations, and settings. For example, CLTC and CNA will host a Cybersecurity Futures 2025 session at RSA Conference 2019 in March 2019, and this spring, at the invitation of project sponsor CyberCube, we plan to facilitate a dialogue for Chief Risk Officers in the global insurance industry.

Cyber Workforce Incubator: In 2018, we continued discussions to find a home and sponsor for the Cyber Workforce Incubator (CWI), which we presented in testimony to Congress in 2017. We see the CWI, which proposes a public-private partnership model to address the twin problems of cultural divide between Silicon Valley and Washington, D.C. and the erosion of skills in the government cybersecurity workforce, as among the most impactful legacies CLTC could set up.

Corporate Membership Program: CLTC's Corporate Membership Program is designed to provide a two-way bridge between UC Berkeley and corporate practitioners. In 2018, we deepened our model for corporate engagement to be not merely transactional and membership-based, but to include thought partnership on research projects through which our industry colleagues can serve as dissemination partners. We welcomed three new companies—HP Inc., Microsoft, and T-Mobile—as members of the CLTC Corporate Membership Program, and received renewals from Qualcomm and Kaiser Permanente. In addition to basic membership, nearly all of these companies partnered with CLTC on aspects of our research agenda, from the Cybersecurity Futures 2025 project to the Digital Accountability workshop. Corporate members also participated in CLTC events throughout the year, including our 2018 Research Exchange, which sparked additional research partnerships for 2019.

Research Exchange: On September 28, CLTC hosted our second annual Research Exchange at Berkeley's David Brower Center. Approximately 60 scholars and community partners attended the conference, where CLTC grantees from 2017 and 2018 presented concise summaries of their research projects. The day-long event showcased the far-reaching topics addressed by UC Berkeley researchers who have received CLTC funding. Both researchers and grantees expressed their appreciation for CLTC's role in convening the Research Exchange. Several attendees noted that

there are few other forums that offer opportunities to learn about the landscape of quantitative and qualitative research at UC Berkeley. "This is where a lot of innovation happens," a corporate member remarked.

Cyberattack Attribution Workshop: In July, CLTC partnered with Microsoft to organize and convene a one-day workshop focused on "Digital Accountability: Designing Futures for Cyberattack Attribution." Held on the UC Berkeley campus, this workshop brought together participants from industry, academia, civil society, and government to explore the recent history and possible futures of cyberattack attribution, with an emphasis on the shifting roles of the private and public sectors. The workshop was organized into three sessions: "Where have we been?" "Where are we going?" and "Designing for the future." By the end of the workshop, participants had identified a number of approaches for improving tangible problems in the attribution landscape. Leading up to the workshop, CLTC Research Fellow Jessica Cussins Newman produced research on the recent history of cyberattack attribution and identified major shifts—in scale, origin, transparency, and coordination—in how attacks on nation-states were attributed between 2007 and today, anchoring the background and frameworks for discussion. Our colleagues in industry and government have informed us that this workshop has helped shape strategy, including the key idea of moving from an attribution mindset toward an accountability mindset.

Top: Ann Cleaveland welcomes attendees at the CLTC Research Exchange. Bottom: CLTC Grantee Sanjam Garg

AI Advocacy: In August, CLTC Researcher Jessica Cussins Newman testified before the California State Senate Judiciary Committee in support of ACR 215, which went on to pass the State Senate with unanimous support. The bill expressed endorsement for the Asilomar AI Principles, a set of 23 principles intended to promote the safe and beneficial development of artificial intelligence. Signatories to the Principles include Demis Hassabis, Yoshua Bengio, Elon Musk, Ray Kurzweil, the late Stephen Hawking, Stuart Russell, and more than 3,800 other AI researchers and experts. Adding support from the California State Legislature was an historic example of government recognition of the importance of responsible AI development.

Top: Participants in the Attribution Workshop. Below: Jessica Cussins Newman, CLTC Research Fellow; Rachel Wesen, Events and Communications Specialist; and Matt Nagamine, Manager of Strategic Partnerships

Guide for Low-Risk Organizations: In collaboration with TechSoup, Sean Brooks, CLTC Research Fellow and Director of the Citizen Clinic, developed an online resource to provide resource-constrained organizations with a basic, risk-informed cybersecurity awareness. Brooks presented this resource in a TechSoup webinar attended by 140 participants. Designed to serve "low-risk" organizations, whose work is not likely to generate targeted online attacks from motivated actors, this

The insights that emerged through this project are helping decision-makers in multiple arenas to engage with tomorrow's cybersecurity challenges and lift out of "today's attack" to anticipate what's around the corner.

resource will help NGOs and other organizations identify where they need to invest in digital security.

Paris Call for Trust and Security in Cyberspace: In November, CLTC signed on to the Paris Call for Trust and Security in Cyberspace, which was launched by French President Emmanuel Macron at the Internet Governance Forum. Signatories of this declaration urge governments and companies to agree to a new initiative to regulate the internet and fight threats such as cyber attacks, election meddling, theft of trade secrets, online censorship, and hate speech.

Elaine Sedenberg participated in the Danish Tech Ambassador Program's "Tech Ambassador for One Day" program.

Danish Tech Ambassador Program: CLTC selected past grantee Elaine Sedenberg to participate in a program called "Tech Ambassador for One Day," sponsored by The Center for Strategic & International Studies (CSIS) and the Office of Denmark's Tech Ambassador. Denmark is the first country in the world to appoint a tech ambassador with a global mandate to meet the technological reality of tomorrow by interrelating the world of technology with diplomacy. In 2019, CLTC will host Caspar Klynge, Tech Ambassador, for an invitation-only roundtable with Berkeley faculty and students. Also in partnership with the Office of the Tech Ambassador, we are planning a two-day workshop in the spring that will bring technology diplomats from multiple countries to the Bay Area for dialogue and engagement with industry.

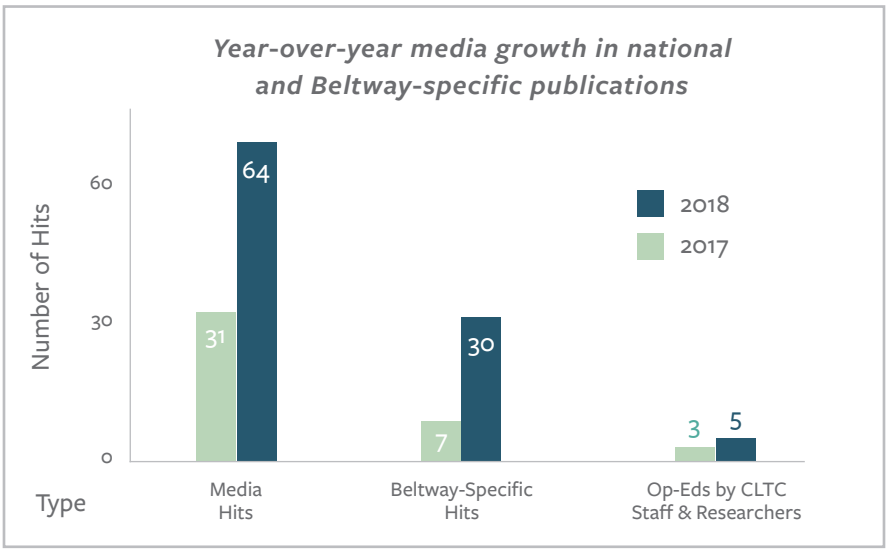
ICANN Security and Stability Advisory Committee: Steve Weber served as part of a small independent examiner group chartered by the ICANN Security and Stability Advisory Committee (SSAC) to evaluate the present performance and future plans of this important ICANN body, whose job is to advise the ICANN community and board of directors on issues concerning the security and integrity of the Internet's naming and address allocation systems. After a six-month process, the group published at the end of 2108 an extensive study with a large number of recommendations that are now being addressed by the ICANN board.

Strategic Communications

With the support of our communications team, we have continued to raise awareness in the public about our work and cybersecurity issues broadly. Strategic communications will be a continued CLTC priority in 2019. 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 on upcoming events, report releases, and other news. We now have nearly 2,300 Twitter followers. We also established an account on LinkedIn and have begun to use that channel for outreach to professional communities.

Media Relations: With the support of the Glen Echo Group, a Washington, D.C.-based firm, we have steadily elevated CLTC's presence in the media over the past two years, particularly among Beltway-based publications, many of which have come to regard CLTC as a trusted and substantive thought leader for cybersecurity and policy (see graph below). CLTC has been featured in some of the nation's most recognizable publications, including *The New York Times*, *Washington Post*, *USA Today*, *Wall Street Journal*, *CNN*, *Politico*, *Axios*, *Quartz*, *Slate*, and *The Hill*.



CLTC increased our media coverage in national and Beltway-specific publications in 2018.

Weekly Newsletters: We have continued to release regular newsletters to engage our community of supporters. Our newsletters, which are now distributed via email on a bi-weekly basis, include CLTC news, event announcements, job listings, internships, academic opportunities, and more. Our newsletter has roughly 1,200 subscribers.

Quarterly and Annual Reports: In addition to releasing a public version of this annual report, which provides an overview of the Center's progress and achievements and our goals for the future, we began producing quarterly

STRATEGIC COMMUNICATIONS

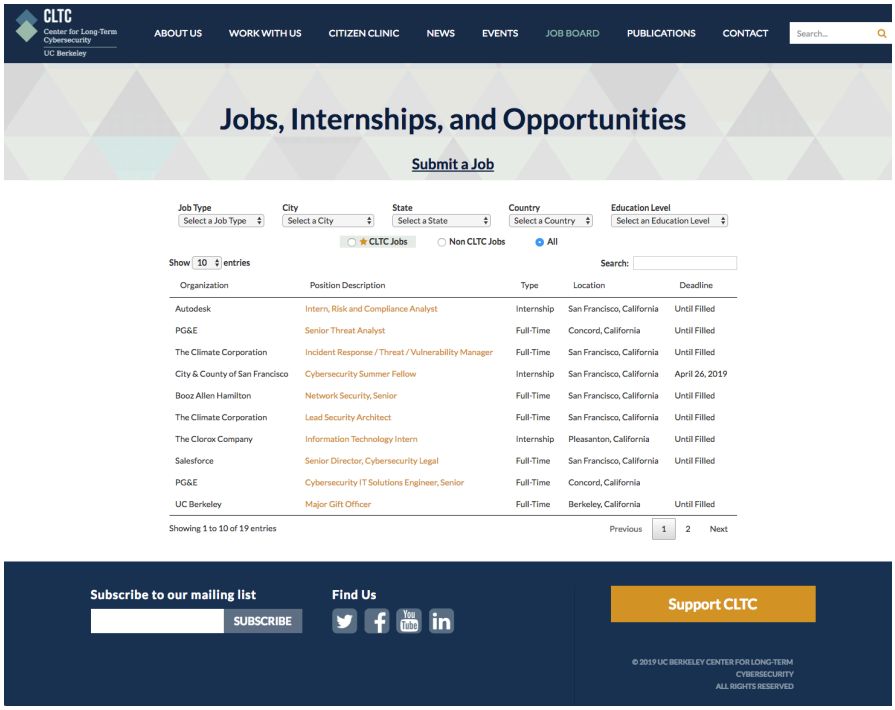
Goals for 2020

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

Interim Goals We Targeted 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.



CLTC added a job board to our website.

newsletters specifically designed for our external community of supporters. These reports are intended to share highlights and keep key stakeholders engaged in our progress.

Enhancements to the CLTC Website: Throughout the year, we worked to enhance our website with new features, including social media links, improved design functionality, and added pages (to showcase our Corporate Membership Program, External Advisory Committee, and other programs). As a key enhancement in 2018, we added a job board that allows users to search for jobs and internships—and allows external organizations to post cybersecurity jobs listings on our site.

Grantee Media Training: In April, as part of our effort to assist with effective public outreach, CLTC hosted a broadcast media training workshop conducted by Brent Durbin, Associate Professor of Government at Smith College. Brent is also Co-Director of the Bridging the Gap Project, a program designed to help scholars promote their research beyond academia and build relationships with the broader policy-making community; he regularly hosts media training sessions for academics at universities around the U.S. Fifteen CLTC grantees participated in the session, which included group training in developing and executing a media outreach strategy, as well as individual mock interviews followed by a group review. We plan to offer our grantees another session of media training in the first half of 2019.

MEDIA HIGHLIGHTS

CLTC and our grantees received coverage in dozens of media outlets in 2018, including the *New York Times*, *Financial Times*, *Washington Post*, *USA Today*, *Axios*, *Quartz*, *Cyber Scoop*, VICE's *Motherboard*, and other outlets. In addition, CLTC's leaders were regularly quoted for interviews in publications produced by organizations such as *TechTarget* and *The Internet Law & Policy Foundry*. Below are some highlights from our media exposure from 2018:

- In the weeks leading up to the 2018 Winter Olympics, several outlets—including ***The New York Times***, ***Financial Times***, ***Toronto Star***, and ***Quartz***—cited CLTC's report on the cybersecurity of the Olympic Games, and former CLTC Executive Director Betsy Cooper published an op-ed in ***USA Today*** on the potential for the competitions to be compromised. As CLTC Faculty Director Steve Weber told ***The Baltimore Sun***, "Every single piece of digital technology that is being used, whether it's for tickets or scoring or timing . . . all that stuff makes really interesting targets, not only to create damage, but as hacktivism, to show that you can."

- In March, an article in the ***Financial Times*** highlighted the efforts of CLTC and lauded the Hewlett Foundation for its commitment to funding the future of cybersecurity. The article referenced a CLTC panel discussion on the cybersecurity of the Olympic Games that took place in October 2017.

- In April, CLTC Grantees Ben Jensen and David Banks penned an article for ***The Washington Post's* Monkey Cage** based on their white paper, *Cyber Operations in Conflict: Lessons from Analytic Wargames.* CLTC communications staff played a key role in helping draft and place this op-ed.

- In April, CLTC Faculty Director Steve Weber wrote an essay in the ***National Journal*** highlighting the growing balkanization of the tech world and its potential to impact development in the tech and cybersecurity spheres in the United States and abroad. The article explained how this trend is largely driven by national security and economic protectionism, and spurred by fears of diminished privacy.

- In May, CLTC Grantee Amit Elazari Bar On wrote an article for **VICE's *Motherboard*** entitled "We Need Bug Bounties for Bad Algorithms," which called for new standards to enable white-hat hackers to participate in bug bounty programs without risk of legal ramifications. Elazari's work was also profiled by Cyber Scoop and other outlets.

- In May, a ***New York Times*** article, "Alexa and Siri Can Hear This Hidden Command. You Can't," profiled research by CLTC Grantees Nicholas Carlini and David Wagner showing they could embed commands directly into recordings of music or spoken text in order to compromise AI-enabled smart devices.

- In June, ***The Hill*** published an op-ed by Gilad Rosner, founder of the Internet of Things Privacy Forum and author of the CLTC white paper, *Privacy and the Internet of Things: Emerging Frameworks for Policy and Design*. In the piece, "The Internet of Things is Built to Leak," Rosner explained that "as more products come equipped with cameras and microphones—not to mention thermal sensors, accelerometers, facial and biometric analysis, and GPS—we are quietly building a sensor fabric that may soon be inescapable, even inside private spaces like the home."

- In July, Steve Weber published an article in **Duck of Minerva** focused on how the supposed artificial intelligence 'arms race' between the U.S. and China may turn out to be less relevant than the relationships between the two machine-learning superpowers and everyone else.

- In August, ***Quartz*** published an article by the School of Information focused on the cybersecurity workforce gap. The piece quoted Steve Weber: "The notion that there's this thing called 'cybersecurity' that's distinct from this other thing called 'security'—that's an idea that is disappearing," Weber said. "This change is going to have some significant implications for all of us over the next 10 years."

- In September, ***The New York Times*** reported on a CLTC grantee study that examined nearly 6,000 children's apps and found that over half of them may have violated the Children's Online Privacy Protection Act (COPPA). The article, "How Game Apps That Captivate Kids Have Been Collecting Their Data," showcased the research of Serge Egelman and his colleagues at the International Computer Science Institute (ICSI).

- In September, **Melissa Griffith** published a blog on the Council on Foreign Relations' "Net Politics" detailing three categories of factors that make scholarly cyber conflict research a more challenging task than its nuclear era counterparts: (1) the characteristics of the threat space, (2) data availability constraints, and (3) the state of political science as a discipline. Her article described steps that universities and grant-making organizations can take to address these barriers.

- In October, Steve Weber was interviewed for the ***Washington Post*'s Cybersecurity 202 newsletter**, which surveyed 85 digital security experts on whether the US should pass a privacy law similar to Europe's General Data Protection Regulation (GDPR).

- In November, ***The Hill*** published an article on the resurgence of Russian meddling during the U.S. midterm elections. CLTC Faculty Director Steve Weber warned against trying to predict hackers' motivations without knowing the specifics of what's driving the phishing campaigns.

- In December, CLTC Faculty Director Steve Weber was featured on **Marketplace Morning Report** to discuss a House panel on issues concerning privacy, data practices, and bias of Google search engines. Weber was also interviewed by **ABC7 News** to weigh in on the data breach at Marriott.

- CLTC researchers were featured in multiple podcasts in 2018. Citizen Clinic, for example, was featured on **CyberWire's Hacking Humans Podcast** as well as the ***Berkeley Technology Law Journal*** podcast; CLTC Research Fellow Jessica Cussins Newman spoke on the **Future of Life Institute** podcast; and CLTC grantee Melissa Griffith spoke about cybersecurity and national security on **Sift Science's Trust & Safety** podcast.

Organizational Health and Fundraising

Ann Cleaveland

LEADERSHIP AND INSTITUTIONAL TRANSITIONS

2018 saw a transition in our leadership team, as we bid farewell to Betsy Cooper, CLTC's founding Executive Director. Betsy built a strong foundation for the Center in the initial development of its programs, people, facilities, and external presence, and we are deeply indebted to her for her efforts. Following a search, in September we welcomed Ann Cleaveland as the new ED. Ann joined CLTC from the ClimateWorks Foundation, where she led multiple efforts to support a large philanthropic collaborative in a more strategic, effective, and science-based response to global climate change. Upon joining CLTC, Ann immediately assumed responsibility for growing key partnerships, managing day-to-day operations, and stewarding a strategy to fulfill the Center's mission.

COMMUNICATION, EVENTS, AND ADMINISTRATIVE CAPACITY

In addition to growing our research team, CLTC has continued to carefully build an expert staff for administration, communication, and events planning. This small core staff is essential for carrying out operational functions, from procurement and financial administration to creating videos and planning events. Their work underlies our model of translating research into practice and amplifies and extends all of CLTC's programmatic work.

Beyond our team on campus, we have 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

CLTC's External Advisory Committee (EAC), a group of corporate executives charged with helping the Center advance our research and educational agendas

We have continued to work to achieve our goal of becoming self-sustaining by 2020. CLTC leadership has ramped up our fundraising efforts, with special attention to major gifts.

by providing perspectives from industry and other domains, remained active in 2018. The committee 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, formerly of Defense Innovation Unit Experimental (DIUx); Maggie Wilderotter, from Wilderotter Vineyard; and Jesse Goldhammer, who previously served as Associate Dean at the UC Berkeley School of Information and is currently Managing Director at Deloitte. We consulted the EAC as part of our "strategic refresh" process, as well as at other key moments throughout the year. We are grateful that these members have committed time and resources to help the Center think strategically about our growth plans and programs.

FUNDRAISING

We have continued to work to achieve our goal of becoming self-sustaining by 2020. CLTC leadership has ramped up our fundraising efforts, with special attention to major gifts. While prioritizing the cultivation of a new financial base, we are also working to establish closer working relationships with University Development and Alumni Relations, in the context of the UC Berkeley's ongoing fundraising priorities.

As discussed above, we continued to grow our Corporate Membership Program in 2018. We are optimistic about the potential to extend these partnerships in 2019, and have had conversations with several supporters of the Cybersecurity Futures 2025 project about deepening this work to generate industry-specific insights for their stakeholders in 2019. We also have a research partnership in development focused on the relationships between corporate boards and chief information security officers (CISOs).

In 2018, Citizen Clinic has invested in relationship-building, which has led to grant funding from IIE for work on *Digital Security Policy for Low-Risk Politically Vulnerable Organizations* and gifts from Mozilla and Facebook. Citizen Clinic has several larger proposals in development to meet its goals for growth in 2019–2020.

We originally planned to hire a Major Gifts Officer in 2018, jointly with the School of Information (I School). This recruitment faced delays, but we are pleased that a new Senior Philanthropy Officer will join CLTC in a joint appointment with the School of Information in Q2 2019.

ORGANIZATIONAL HEALTH

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, and a robust fundraising model.

Interim Goals We Targeted 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.

The Way Forward

We are entering 2019 eager to build on our successes, deepen our impact, and cultivate the financial base needed to sustain CLTC's mission. After four years in operation, CLTC is at an exciting inflection point: we are no longer a start-up, and can now point to several mature programs. We celebrate this progress, and also see it as an opportunity to engage in a strategic refresh. Our emerging strategic objectives for 2019 include expanding our role as a platform to convene industry, policymakers, and civil society in joint problem-solving; scaling up the Citizen Clinic to train the next generation of public interest cybersecurity professionals; and selectively investing in high-impact media relationships. We also plan to launch several new initiatives in the coming year based on insights from the 2025 Cybersecurity Futures project and the gaps we see in the field.

There is no silver bullet for cybersecurity. Security is multifaceted, upstream of technical constraints, downstream of popular conceptions in the media, and entangled with messy social and political realities. In other words, our mission demands a "full-stack" approach. We repeatedly see our most effective work emerging from the application of broad competencies and unique perspectives to the cybersecurity problem set. We look forward to amplifying and expanding this important work in 2019 with your support.

After four years in operation, CLTC is at an exciting inflection point: we are no longer a start-up, and can now point to several mature programs. We celebrate this progress, and also see it as an opportunity to engage in a strategic refresh.

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

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.

CLTC

Center for Long-Term Cybersecurity

UC Berkeley

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