Berkeley
UNIVERSITY OF CALIFORNIA

LOOKING OVER the HORIZON

FIVE YEARS OF GROWTH AND IMPACT

2015–2020

CENTER FOR LONG-TERM CYBERSECURITY

LOOKING OVER THE HORIZON

LETTER FROM THE DIRECTORS

Five years ago, we launched the UC Berkeley Center for Long-Term Cybersecurity (CLTC) with a mission to look over the horizon. With the help of thinkers from a wide range of disciplines, we developed scenarios depicting diverse narratives for what cybersecurity might look in the year 2020, which at the time was an almost unimaginable five years away.

The scenarios helped us identify key emerging issues—including predictive algorithms, the internet of things, and shifting attitudes about privacy—that have increasingly shaped our world. And while we didn't get everything right (see page 4), these long-term insights have informed CLTC's ambitious research, policy engagement, and education priorities.

Since our inception, our goal has been to create a new kind of research center, and to "move the needle" by broadening the aperture on cybersecurity and integrating technical research with the social sciences, law, and other domains. After all, as technologists often remind us, the human is the weakest link in digital security—and, in practice, the hardest to understand.

As you'll see in this report, CLTC has continued to push into new frontiers. We launched Citizen Clinic, a first-of-its-kind model that trains UC Berkeley students to provide cybersecurity assistance to civil society organizations that are at risk of politically motivated cyberattacks. We sponsored a pioneering cybersecurity arts contest, and started a research program to understand the global security implications of artificial intelligence. And we've supported hundreds of talented cybersecurity researchers working across UC Berkeley. We are particularly proud of the incredible "diaspora" of CLTC-affiliated student researchers who have moved on to do important professional work on the front lines of cybersecurity policy and practice (see page 8 for a few stories).

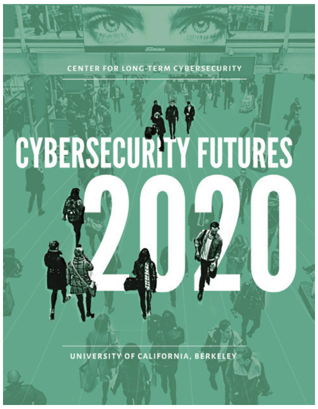
The Center for Long-Term Cybersecurity has made important progress over the past five years, but our work is just getting started. We hope you'll continue to join us as we keep reaching out toward the horizon for the next five years and beyond.

Ann Cleaveland, Executive Director

Steven Weber, Faculty Director

LOOKING OVER THE HORIZON

CYBERSECURITY FUTURES


CENTER FOR LONG-TERM CYBERSECURITY
CYBERSECURITY FUTURES
2020
UNIVERSITY OF CALIFORNIA, BERKELEY

Our futures practice is a recurring series, and every five years we apply a disciplined methodology to develop new scenarios and keep peering over the horizon.

In 2015, the Center for Long-Term Cybersecurity published its inaugural set of "cybersecurity futures" for the year 2020. Now that the future has arrived, we can reflect on those scenarios and assess what causes and implications we saw clearly and, importantly, what we failed to foresee and why.

WHAT WE DID FORESEE

We anticipated the rise of algorithmic authoritarianism—the use of digital systems for surveillance and control—in China and other nations. We argued that a set of techniques, tactics, and technologies would be packaged into an exportable tool kit that would appeal to many governments, and that has indeed happened.

We foresaw many aspects of the push-back against the large platform firms, even though what is now called a "techlash" was barely nascent in 2015. We saw that the era of permission-less innovation—the idea that, in the digital environment, private firms could do pretty much whatever they wanted until someone could show that what they were doing was dangerous—was coming to a close.

We foresaw the emergence of "emotion data" as a crucial new battleground for digital security. People now leave a trail of digital exhaust tracing not only what they do, but also what they feel, which is more valuable than a record of clicks and decisions.

What does this analysis of our past scenarios tell us about what we should do to be better prepared when we wake up on Jan 1, 2025? No matter how many billions of transistors can be put onto a chip and how many billions of data points can be processed in a machine-learning training set, in 2025 and beyond, human beings will still be the most complex variables in the cybersecurity equation.

WHAT WE DIDN'T FORESEE

We assumed a rate of change that was faster than what we observed. Many of the issues that cybersecurity professionals dealt with in 2015 (such as weak passwords, data breaches, ransomware, insider threats, etc.) remain challenges in 2020.

We did foresee the rising value of data for artificial intelligence, but we overestimated the market value of data, and we didn't understand how issues about bias and other flaws in data sets would become so prominent.

We understated how strongly traditional geopolitics would shape the digital security world.

We didn't foresee the deepest vulnerabilities in our democratic process, which turned out to be not voting machines, but public discourse on social media platforms and its relationship to "truth."

We underestimated the presence and prevalence of state-based attackers and defenders by paying too much attention to non-state-based criminal networks.

We underestimated the digital component of the "gray wars" between the United States and China, Russia, and Iran, and between other dyads that are less visible.

We overestimated the degree to which public infrastructure would incorporate the "internet of things" and other digital technologies to improve public services. Experimental deployments have moved slowly, the private sector has been more central in implementation, and public push-back on privacy has been more intense than expected.

CYBERSECURITY FUTURES 2025

For our latest effort to look over the horizon, CLTC—in partnership with CNA's Institute for Public Research (CNA) and the World Economic Forum's Global Centre for Cybersecurity (C4C)—created **Cybersecurity Futures 2025**, a global initiative that aims to shape a forward-looking research and policy agenda that is intellectually and practically robust—and broadly applicable across global geographies.

CLTC
Cybersecurity Futures in A Global Context And US policy options
WEF, CLTC, CNA
CLTC
Cybersecurity Futures in A Global Co
And US policy options

Sponsored by HP, Inc. and Qualcomm, with additional support from Cybercube and Symantec, the Cybersecurity Futures 2025 project began in 2017, when CLTC developed a set of four scenarios depicting possible futures that could result from the rise of artificial intelligence, ubiquitous sensors, quantum computing, divergent internet regulations, and other trends. In 2018, the project team convened a series of workshops in seven international cities to engage experts and decision-makers in dialogue about the challenges and opportunities the scenarios depict.

In the year since the scenarios were published, they've helped drive important conversations in a wide variety of forums:

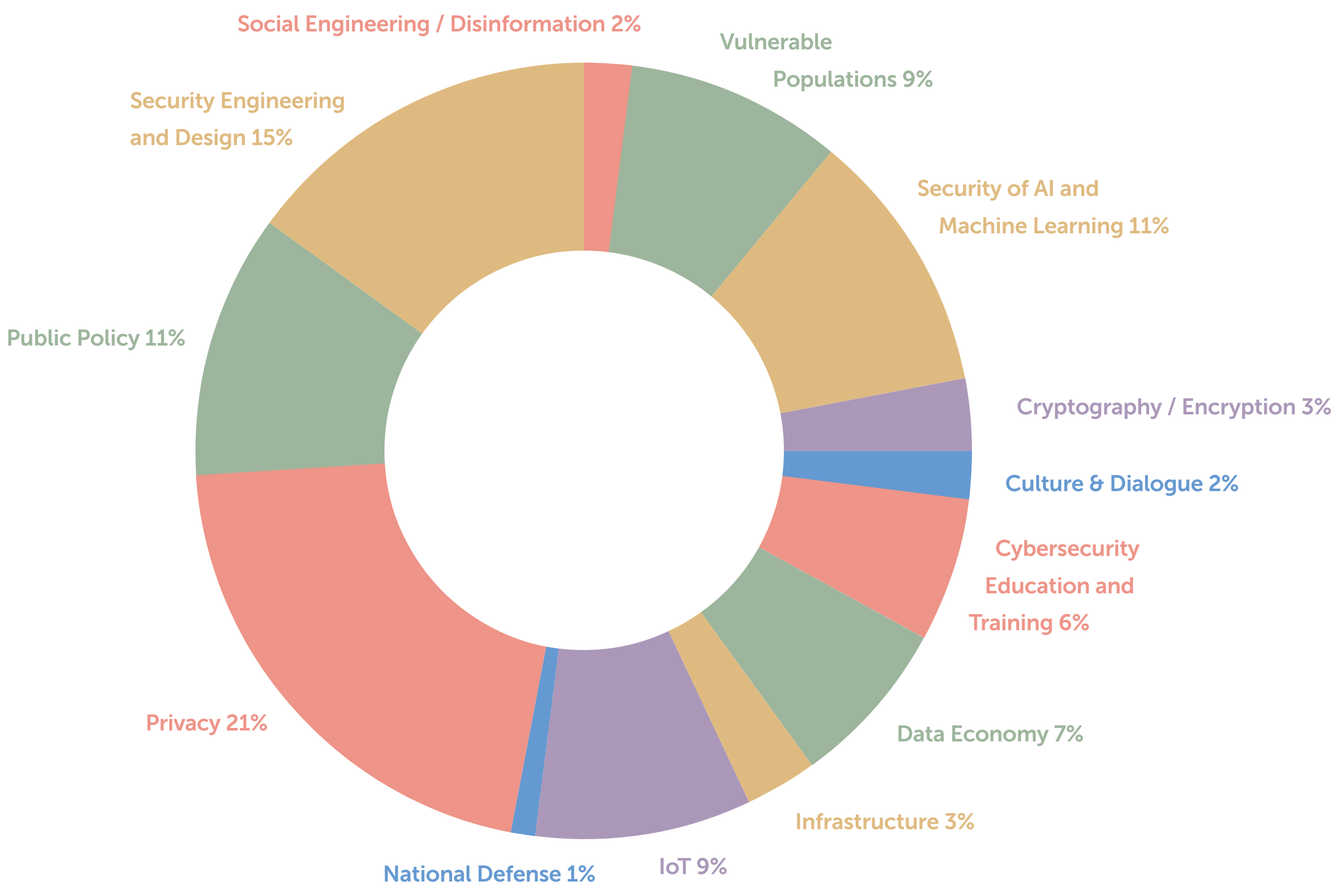
- We presented the scenarios at the RSA Conference, in San Francisco, one of the world's largest cybersecurity industry convenings.
- We led a workshop in London for risk and underwriting officers from major global insurance companies, using the scenarios to help think broadly about evolving risks.
- We convened a workshop for diplomats from over 25 countries organized by the Office of Denmark's Tech Ambassador.
- We presented the scenarios to an audience of hundreds at the Internet Economy Summit, in Hong Kong.
- The website application, videos, and resources we developed have been accessed by people around the world.

CUTTING-EDGE RESEARCH

Since our inception, the Center for Long-Term Cybersecurity has awarded roughly $5.2 million to 109 innovative research projects.

- **Total number of research projects CLTC has funded since 2016: 109**
- **Total number of researchers supported: 167**
- **Percentage of projects led by women: 40 percent**

RESEARCH AREAS FUNDED

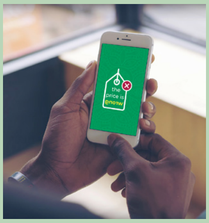


CLTC GRANTS HAVE BEEN AWARDED TO RESEARCHERS WORKING ACROSS THE UC BERKELEY CAMPUS, AT THESE AND OTHER ACADEMIC UNITS

Blum Center for Developing Economies
CITRIS and the Banatao Institute
Civil and Environmental Engineering
College of Environmental Design
College of Letters and Science
Department of Electrical Engineering and Computer Science
Department of Mechanical Engineering
Department of Nuclear Engineering
Department of Political Science
Department of Sociology
Department of Statistics
Goldman School of Public Policy
Haas School of Business
Human Rights Center
International Computer Science Institute
School of Information
School of Law
School of Social Welfare
Simons Institute for the Theory of Computing

CYBERSECURITY ARTS PRIZE

In 2019, CLTC's Daylight Security Research Lab (DSRL) identified a research gap in representations of cybersecurity. As part of a series of efforts to address this gap, the DSRL led a first-of-its-kind Cybersecurity Arts Contest, which awards prizes to artists whose work has potential to expand the ways that the public engages with and imagines cybersecurity. Six artistic projects were selected based on their potential to illuminate the human impacts of security and provoke critical dialogue about important issues like privacy, surveillance, cyberattacks, and malware. The prize-winning projects have been announced online and will be spotlighted at CLTC convenings in 2020.



Winners of the Cybersecurity Arts Contest included "Virtual Caring," for which artist Lauren McCarthy will use a network of cameras and remotely controlled appliances to serve as a "human AI" assistant for elderly residents; and "The Price is Wrong," a series of videos by Uganda-based collaborators Shayna Robinson and Neema Iyer calling attention to the public's lack of awareness around cybersecurity.

CAL CYBERSECURITY RESEARCH FELLOWSHIP

Thanks to a generous gift from a Cal alumnus, the Center for Long-Term Cybersecurity has established a new annual award, the Cal Cybersecurity Research Fellowship, which provides $15,000 to students or postdoctoral scholars to pursue cybersecurity research, with preference given to researchers working in areas related to blockchain for information security/cybersecurity purposes and security in 5G networks.

Fellowships offer a launchpad for groundbreaking research for promising students. The 2019 recipient, Matt Olfat, a PhD candidate in Industrial Engineering and Operations Research, is investigating the development of flexible watermarking techniques for detecting attacks on cyber-physical systems such as 5G networks. The 2020, recipient, Nathan Malkin, a PhD student in the Department of Electrical Engineering and Computer Science, has a research focus on improving privacy controls for "always-on" listening devices.

Matt Olfat, 2019 Cal Cybersecurity Research Fellow

CLTC ALUMNI IN THE FIELD

After five years of CLTC operations, we're proud that former CLTC grantees, fellows, and student researchers have pursued careers in cybersecurity and are now in positions of influence at a wide range of organizations. The CLTC diaspora is helping to lead cybersecurity policy and practice at a national and global scale.

ELAINE SEDENBERG

Privacy and Data Policy Manager, Facebook

Elaine Sedenberg (PhD '19) was involved with the Center for Long-Term Cybersecurity in its earliest stages. She helped draft the first set of scenarios, and she received a grant to research private- and public-sector information sharing. She also served as co-director of the Center for Technology, Society, and Policy (CTSP), which awards research grants in partnership with CLTC.

After completing her PhD in the School of Information, Sedenberg was recruited to become the Privacy and Data Policy Manager for Facebook's Privacy Policy Team. "CLTC helps train a new generation of researchers and technologists—my career so far is living proof," Sedenberg says. "CLTC has helped diversify the scope of problems, methodologies, and actors included within the traditional cybersecurity and privacy tent. The research problems CLTC tackles are rooted in actual challenges faced by governments, industry, and society. CLTC has developed a wide range of tools and approaches for bridging the academic and real-world divide, and I have come to appreciate this even more as I transitioned from the academy to a role in industry."

AHMAD SULTAN

Associate Director for Research and Technology Policy, Anti-Defamation League Center for Technology and Society

As a Master's student in the Goldman School of Public Policy, Ahmad Sultan received a CLTC grant to conduct a first-of-its-kind survey that demonstrated how underserved residents in San Francisco—including low-income residents, seniors, and foreign language speakers—face higher-than-average risks of being victims of cyber attacks. With CLTC's support, Sultan published a white paper and op-ed about his research findings, and the resulting media exposure earned him an invitation to give testimony to a Congressional Homeland Security Subcommittee on Cybersecurity, Infrastructure Protection, and Innovation.

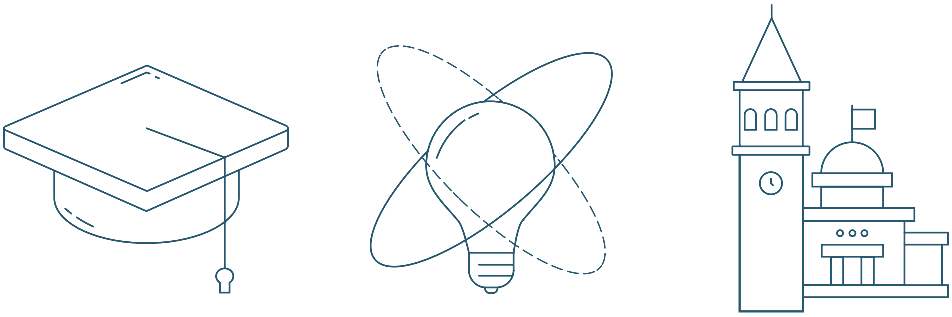
Today, Sultan serves as the Associate Director for Research and Technology Policy at the Anti-Defamation League's Center for Technology and Society. He also serves as an Adjunct Professor at the UC Berkeley School of Information, where he teaches a course entitled Designing Against Hate: An Exploration of Speech and Affordances on Social Media. “I would not be doing what I’m doing right now without the support I received from CLTC,” Sultan says. “My work continues to focus on the online experiences of historically marginalized communities, the ways in which they are increasingly subject to online harassment, and the ways in which civil society, technologists, and policymakers can do more to make the internet a safer place for all.”

AMIT ELAZARI

Director, Global Cybersecurity Policy, Intel

While earning her Doctor of Science of the Law (JSD) at UC Berkeley’s School of Law, Amit Elazari pursued a variety of CLTC-funded research initiatives. Among her projects, she created a standardized set of form-contracts for crowdsourced security programs (bug bounties, frameworks under which entities offer financial rewards for external security researchers ethically disclosing vulnerabilities to the entity), fostering legal safe-harbor and computer crime protections for ethical hackers. Her research has been widely adopted in industry, including by DropBox, Mozilla, and Tesla, among others.

Today, Elazari serves as Director, Global Cybersecurity Policy at Intel, and she is a lecturer in the School of Information’s Master of Information and Cybersecurity (MICS) program. “CLTC was instrumental to my getting to where I am today,” she says. “It was a chance to conduct research on privacy and security policy and to shape a framework to be made widely available to industry. The interdisciplinary nature of the research involving students from the School of Information, as well as lawyers and engineers, gives you valuable experience if you aim to work in industry with researchers and technologists.”



EDUCATION DEVELOPING TOMORROW'S LEADERS

CITIZEN CLINIC

CLTC's Citizen Clinic is the first program of its kind in the world. Following the model of "clinics" used in medicine and law, our team members provide hands-on training to interdisciplinary teams of students, who learn to assess threats to targeted organizations, recommend risk-appropriate mitigations, and work collaboratively with clients to implement new policies and technical controls that enhance their cybersecurity. Through their work, students gain valuable practical experience while helping improve the digital security of an array of mission-driven partners.

This work is critically important for expanding cybersecurity assistance to civil society organizations that are politically targeted online. In Fall 2019, for example, Citizen Clinic's students:

- helped secure the data of reproductive rights healthcare providers;
- improved digital security for indigenous activists;
- explored innovative solutions to threats to members of the trans community; and
- helped improve the security of voter information efforts.

"As a director of a small organization working on complex issues, digital security has become increasingly concerning for us," says Casey Box, executive director of Land Is Life, a global organization supporting indigenous peoples' right to self determination. "We recognize that we have very limited expertise in digital security, and that's why partnering with Citizen Clinic was incredibly valuable for us. We felt like we had an in-house team that was working with us day-to-day to not only strengthen the organization of Land is Life, but to look at strategies that we might be able to roll out and disseminate across the organizations we work with."

A CLTC seminar entitled "Indigenous-led Security and Digital Safety" addressed some of the security challenges facing non-governmental organizations. Pictured (L to R): Jemimah Kerenge, Director of Enkishon Indigenous Initiative; Daniel Kobei of the Ogiek Peoples' Development Programme (OPDP); and Sean Brooks, Director of Citizen Clinic.

Citizen Clinic has grown steadily (see sidebar), and is developing into a pipeline for public-interest technologists; Citizen Clinic alumni are now working at major technology companies such as Google, IBM Security, and Microsoft, as well as large law firms, public institutions, and advocacy organizations. Citizen Clinic's staff members have also begun to develop curricula to train other civil society organizations to manage online threats.

CITIZEN CLINIC TIMELINE

H1 2017	Citizen Clinic receives scoping grant from the MacArthur Foundation
DECEMBER 2017	MacArthur provides additional support for work focused on low-risk organizations
APRIL 2018	Citizen Clinic initiates pilot
JULY 2018	Research Fellow Sean Brooks publishes “Defending Politically Vulnerable Organizations Online”
SEPTEMBER 2018	Citizen Clinic begins first semester of instruction
SPRING 2019	Citizen Clinic offers its first advanced class
APRIL 2019	Citizen Clinic is formally certified as a class in the UC Berkeley School of Information and holds its first recruiting event
JUNE 2019	Microsoft supports research on scaling-up the Citizen Clinic model
SUMMER 2019	Citizen Clinic class is offered online, as part of the Master of Information and Cybersecurity program
FALL 2019	Led by Deputy Director Steve Trush, Citizen Clinic creates an open-source website on GitHub to provide access to learning resources
SEPTEMBER 2019	Mentorship program established with private-sector volunteers; Atlassian becomes first corporate participant
WINTER/SPRING 2020	Citizen Clinic enrolls 18 students, the largest cohort yet, bringing the total number of students to pass through the clinic to over 60 from more than 10 different academic programs
JANUARY 2020	Citizen Clinic has now served over 10 organizations across three continents
FEBRUARY 2020	Citizen Clinic secures $275K grant from Craig Newmark Philanthropies to grow its scale and impact

MASTER OF INFORMATION AND CYBERSECURITY DEGREE

In 2017, CLTC helped initiate “cybersecurity@berkeley,” a new online Master of Information and Cybersecurity (MICS) degree program offered by the UC Berkeley School of Information. We have continued to support and enrich the MICS program since the program’s inception. In 2019, for example, CLTC offered a summer Citizen Clinic course to MICS students, and we offered research funding for selected MICS capstone projects. We continue to support the MICS mentorship program through our network of industry and government leaders, and connect MICS students to Berkeley cybersecurity research and opportunities through an “immersion” program on-campus.

CLTC grantee Fattaneh Bayatbabolghani presented to students enrolled in the MICS program as part of their on-campus immersion.

RSA SECURITY SCHOLARS

Together with the UC Berkeley School of Information, CLTC annually selects students to participate in the RSA® Conference Security Scholar program, which connects 80 top cybersecurity students with leading experts, peers, and attendees at RSA® Conference, the world’s largest information security conference. RSAC Security Scholars are invited to present to RSAC attendees, potential employers, and fellow students at the RSAC Scholar Poster Board Session, and they participate in private functions and meet industry experts, academic colleagues, and potential employers.

PRIVACY ENGINEERING COURSE

CLTC grantee Daniel Aranki developed first-of-their-kind training resources related to privacy engineering, including tools and frameworks to help achieve provable privacy in information systems. His first course, “Introduction to Privacy Engineering” (I2PE), was delivered as part of the MICS program; it has been offered twice (online) and is also offered on campus at the School of Information.

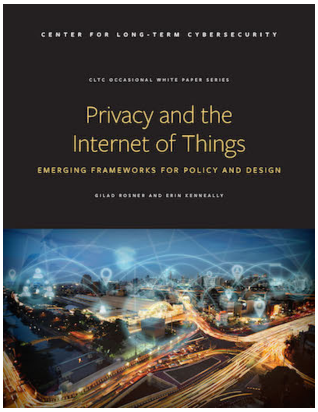
POLICY ENGAGEMENT AND IMPACT

From hosting the White House Commission on Enhancing National Cybersecurity to convening workshops with the Office of Denmark's Tech Ambassador, the Center for Long-Term Cybersecurity has worked on many fronts to inform policymakers and encourage collaboration across sectors.

CLTC WHITE PAPER SERIES

The CLTC White Paper Series makes our research accessible to a non-specialist audience, including policymakers. During the past five years, CLTC white papers have been used in a variety of contexts, from Congressional hearings and legislative briefings to industry workshops and city and local initiatives.

- *A Public, Private War: How the U.S. Government and U.S. Technology Sector Can Build Trust and Better Prepare for Conflict in the Digital Age*
- *Asian Cybersecurity Futures: Opportunity and Risk in the Rising Digital World*
- *Cyber Industrial Policy in an Era of Strategic Competition*
- *Cyber Operations in Conflict: Lessons from Analytic Wargames*
- *Cyber Workforce Incubator*
- *Cybersecurity Futures 2025: Insights and Findings*
- *Cybersecurity in Low-Risk Organizations*
- *The Cybersecurity of Olympic Sports: New Opportunities, New Risks*
- *Cybersecurity Policy Ideas for a New Presidency*
- *Defending Politically Vulnerable Organizations Online*
- *Improving Cybersecurity Awareness in Underserved Populations*
- *Privacy and the Internet of Things: Emerging Frameworks for Policy and Design*
- *Resilient Governance for Boards of Directors: Considerations for Effective Oversight of Cyber Risk*
- *Toward AI Security: Global Aspirations for a More Resilient Future*

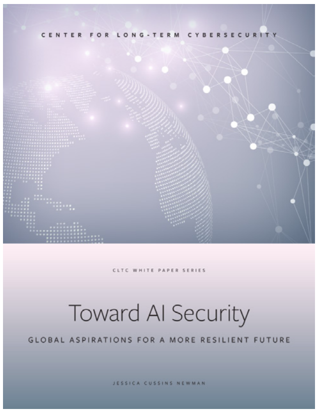

CENTER FOR LONG-TERM CYBERSECURITY

CLTC OCCASIONAL WHITE PAPER SERIES

Privacy and the Internet of Things

EMERGING FRAMEWORKS FOR POLICY AND DESIGN

GILAD ROSNER AND ERIN KENNEALLY


CENTER FOR LONG-TERM CYBERSECURITY

CLTC WHITE PAPER SERIES

Toward AI Security

GLOBAL ASPIRATIONS FOR A MORE RESILIENT FUTURE

JESSICA CUSSINS NEWMAN

CLTC
Center for Long-Term Cybersecurity
UC Berkeley

RESILIENT GOVERNANCE FOR BOARDS OF DIRECTORS

CONSIDERATIONS FOR EFFECTIVE OVERSIGHT OF CYBER RISK

In partnership with
Booz | Allen | Hamilton

CONVENINGS AND COLLABORATIONS: SELECT HIGHLIGHTS

Cyberattack Attribution Workshop

Through a partnership with Microsoft, we explored the recent history and possible futures of cyberattack attribution, with an emphasis on the shifting roles of the private and public sectors. The outcomes helped establish a platform of the global Cyber Peace Institute, an independent NGO created to address the growing impact of major cyberattacks.

We convened a gathering of academic researchers and public- and private-sector representatives to tackle the challenge of cyberattack attribution.

Resilient Governance for Boards of Directors

Through collaborative research with Booz Allen Hamilton, we looked at the state-of-the-art in board oversight of cybersecurity, and developed a practical, adaptive framework to help boards manage cybersecurity governance. The report identifies four "dynamic tensions" likely to shape board governance and oversight of cybersecurity, including an organization's overall risk model or mindset; distribution of cybersecurity expertise on the board; balance between cooperation and competition with other enterprises; and the model for information flows between management and the board.

Corporate Membership Program

CLTC has welcomed nearly a dozen industry partners into its Corporate Membership Program since 2015. These valued collaborators have been integral to our success. In a 2019 survey, they gave high marks to the value of belonging to our international network of cyber, policy, and academic experts, and of having access to the insights and talent that better prepare them for tomorrow's security landscape. Benefits to partners range from curated CLTC content and special convenings to customized workshops and the opportunity to shape collaborative research. In 2020, a new quarterly *Security Wire* conference call was introduced that provides members access to CLTC expertise and a long-term view about pressing cybersecurity issues of the day. CLTC invites inquiries and introductions to expand our dynamic network of partners (see page 16 for a list).

Cybersecurity Futures 2025

Through a research partnership with the World Economic Forum, sponsored by HP, Inc, Qualcomm, Symantec, and CyberCube, we conducted a series of global workshops and bespoke salon dinners / industry roundtables that engaged our partners and their customers in developing actionable insights to navigate cybersecurity futures.

TECHSOUP WEBINAR ON "CYBERSECURITY IN LOW-RISK ORGANIZATIONS"

CLTC collaborated with TechSoup, a provider of technology to nonprofits, charities, and libraries, to conduct a webinar titled "Cybersecurity in Low-Risk Organizations: Understanding Your Risk and Making Practical Improvements." A total of 140 people participated in the session, which provided an overview of the basic tenets of cybersecurity, what qualifies an organization as 'low-risk', and a risk-informed decision-making process to identify where organizations need to invest in digital security.

POLICY ENGAGEMENT AND IMPACT

PROFILE

ARTIFICIAL INTELLIGENCE SECURITY INITIATIVE SHAPES LOCAL, NATIONAL, AND GLOBAL GOVERNANCE

AI SECURITY INITIATIVE

Jessica Cussins-Newman, CLTC Research Fellow and Program Lead of the AI Security Initiative.

Artificial intelligence can bring enormous benefits to the world if we develop the right training, standards, and policies to guide its development and use. In 2019, CLTC launched the Artificial Intelligence Security Initiative (AISI), a program led by researcher Jessica Cussins-Newman focused on the global security implications of AI. Cussins-Newman has been active in shaping AI standards on the local, national, and global levels: she has presented at international forums like the Global Governance of AI Roundtable and World Government Summit, in Dubai, and she penned op-eds for *The Hill* that were widely shared (including by Ivanka Trump) and earned an invitation to meet with cyberpolicy officials in the White House. The AISI also contributed comments that were integrated into the National Institute of Standards and Technology (NIST) federal plan for technical AI standards, and Cussins-Newman co-presented a briefing at the California State Capitol that helped shape Assembly Bill No. 459 (AB 459), which calls for the establishment of guidelines for the use of AI in state government.

PROFILE

EGELMAN AND TEAM WIN POLICY CHANGES AND "BUG BOUNTY" FROM GOOGLE

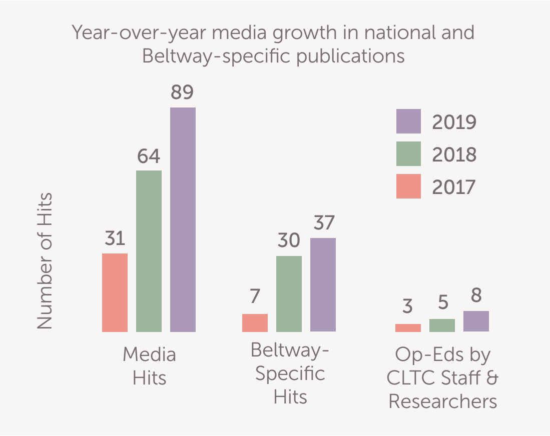
Serge Egelman, Research Director of the Usable Security & Privacy Group at the International Computer Science Institute (ICSI).

CLTC Grantee Serge Egelman and his colleagues at the International Computer Science Institute (ICSI) have seen major real-world impacts of their research, which focuses on monitoring smartphone applications and observing their behavior. Egelman and his colleagues previously exposed that a majority of applications in the Designed for Families (DFF) section on Google's app store were violating the Children's Online Privacy Protection Act (COPPA). Based on those results, Google announced changes to its policies, and multiple state governments filed lawsuits against app developers who were violating COPPA. More recently, Egelman and his fellow researchers observed tens of thousands of apps transmitting sensitive user data without holding the requisite Android permissions. This work received the Distinguished Paper Award at this year's USENIX Security Symposium, and Google paid the researchers a "bug bounty" for disclosing the underlying vulnerabilities, which have been fixed in a new version of Android.

MEDIA HIGHLIGHTS

From op-eds to news stories, CLTC has earned media coverage in a wide range of outlets in the U.S. and around the world. Below are examples from the past three years.

- "Artificial intelligence could identify you and your health history from your step tracker," *USA Today* op-ed co-authored by CLTC grantee Anil Aswani
- "Web of Assumptions," Slate op-ed on inference by CLTC Grantee Rena Coen
- "Digital Insecurity is the New Normal," *New York Times* op-ed co-authored by Steven Weber and Betsy Cooper



@MLFAILURES

In 2019, the Daylight Security Research Lab launched a new Twitter account, @MLFailures, to capture instances where machine learning and artificial intelligence failed to live up to their potential, from self-driving cars tricked into breaking the speed limit to image classifiers mistaking an owl for a pineapple. Follow the handle @MLFailures, and use the hashtag #MLFailures to share.

CLTC BULLETIN

CLTC's new "Bulletin" blog on Medium has facilitated rapid dissemination of researcher insights and expanded our readership. Follow us at https://medium.com/cltc-bulletin.

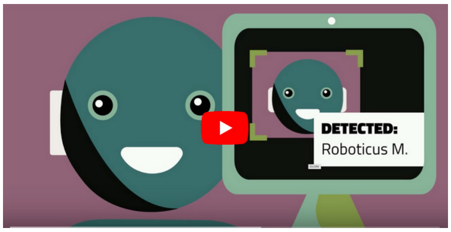
THE CLTC NEWSLETTER

Our bi-weekly email newsletter has grown steadily, and now provides nearly 1600 subscribers with a round-up of news, events, and opportunities, including recent posts from our online cybersecurity jobs board. We've also built up a base of followers on Facebook and Twitter, where we have more than 4000 followers. (Find us at @CLTCBerkeley.)

ADVERSARIAL MACHINE EXPLAINER VIDEO

We also initiated production of a series of "explainer videos" with the theme, "What? So What? Now What?" The first video, on adversarial machine learning, was shared with high-level decision-makers in the Department of Defense.

"The video on machine learning was amazing; it took something that is complex and distilled it down into a digestible, easy-to-comprehend format. I immediately shared it with my network, as it was a way to easily explain machine learning and how it can be used and misused, which is crucial for decision-makers to understand."
—**KAITIE PENRY**, University Program Director, UC Berkeley, National Security Innovation Network



GROWTH & FUNDRAISING

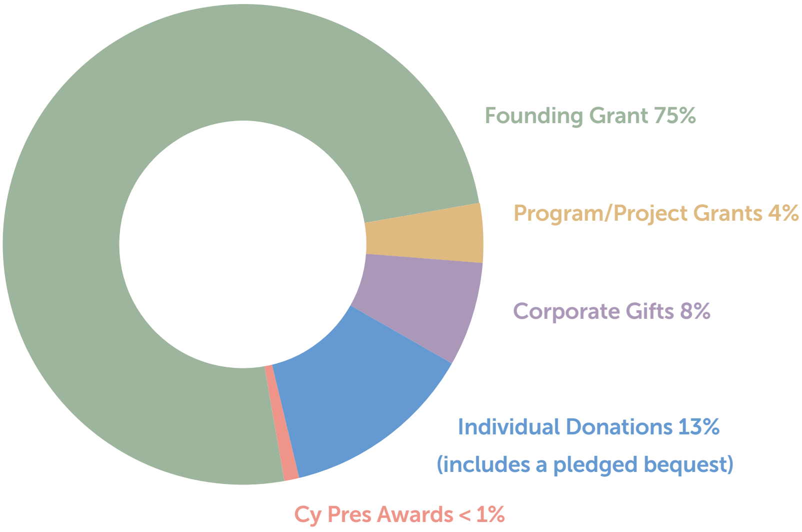
The Center for Long-Term Cybersecurity is indebted to the William and Flora Hewlett Foundation, whose foresight in recognizing the importance of cybersecurity to our global landscape resulted in a generous founding grant. Our growth since that time has been nurtured by our association with UC Berkeley's School of Information, a wide range of faculty across the campus, the talents of our Executive Advisory Committee, and generous support from corporate partners, foundations, and individuals. With continued support from our diverse community, CLTC looks forward to a bright long-term future.

All individual and corporate donors agree to contribute their funds as gifts in support of independent academic research and education. CLTC retains full discretion on the design, implementation, and expenditures for all activities enabled by these gifts.

GIFTS AND GRANTS

Booz Allen Hamilton | CyberCube | Craig Newmark Philanthropies | Facebook | HP, Inc. | Huawei | Institute for International Education | John D. and Catherine T. MacArthur Foundation | Kaiser Permanente | LA 2024 Exploratory Committee | Microsoft, Inc. | Mozilla | National Science Foundation | Qualcomm | Symantec | T-Mobile | The William and Flora Hewlett Foundation | UC Berkeley alumni and individual donors

TOTAL FUNDRAISING: $20,000,000

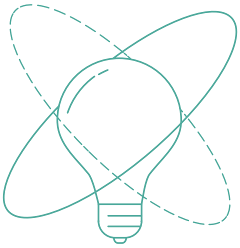


LOOKING AHEAD TO THE NEXT FIVE YEARS

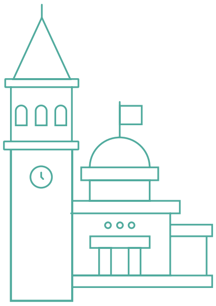
CLTC was launched in 2015 with a clear objective: to amplify the upside of the digital revolution, by anticipating and addressing security issues that emerge where human beings and digital technologies intersect. The time horizon for this work needs to be thought of in years and in decades, and as we celebrate our five-year mark, we are proud of the strong foundations we have established.

The overall goal of the Center remains to generate a broader view of what cybersecurity means and a longer-term, practical vision of how to approach it. In that spirit, we have a variety of exciting new initiatives planned for the future. We hope you'll help us build on our track record of success in 2020 as we:

- Advance diverse and multi-disciplinary cybersecurity research through the CLTC Grants program;
- Help politically targeted organizations stay safe online through Citizen Clinic, which is helping to level the playing field for civil society in the digital environment;
- Analyze the global impacts of artificial intelligence through our AI Security Initiative;
- Illuminate the cultural dimensions of cybersecurity through our Daylight Security Research Lab; and
- Continue to develop a diverse, ever-growing group of tomorrow's leaders in the cybersecurity field, through research opportunities, fellowships, connections to industry, and other support.



Meanwhile, we're already thinking about what we need to do today to be better prepared when we wake up on Jan 1, 2025. We'll be keeping our eyes on the small and subtle trends, as well as big-picture developments in the technology industry, geopolitics, and society writ large.



Cybersecurity is more important than ever, and while the challenges seem to be mounting faster every day, we're confident that our approach—thinking broadly about technology and security and focusing on a long-term time horizon—will help us identify robust solutions for tomorrow's institutions.

We are excited to embark upon our next phase, and hope you will join us on our journey.

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

We gratefully acknowledge the contributions of our staff and External Advisory Committee to advancing the mission of CLTC.

CLTC STAFF

Kristin Berdan
Citizen Clinic Fellow

Sean Brooks
Research Fellow

Ann Cleaveland
Executive Director

Shanti Corrigan
Senior Director of Philanthropy

Jessica Cussins Newman
Research Fellow

Melissa Griffith
Non-Resident Research Fellow

Chuck Kapelke
Communications

Herb Lin
Non-Resident Research Fellow

Nick Merrill
Post-Doctoral Fellow

Matt Nagamine
Manager of Strategic Partnerships

Steve Trush
Research Fellow

Steven Weber
Faculty Director

Rachel Wesen
Events and Communications Specialist

EXTERNAL ADVISORY COMMITTEE

Sameer Bhalotra
Co-Founder and CEO, ActZero.ai

Amit Elazari
Director, Global Cybersecurity Policy, Intel Corporation

Jesse Goldhammer
Managing Director, Deloitte

Gilman Louie
Partner, Alsop Louie Partners

Ellen Richey
Vice Chairman and Chief Risk Officer (retired), Visa Inc.

Jim Routh
CISO, MassMutual

Ted Schlein
General Partner, Kleiner Perkins Caufield & Byers

Raj Shah
Chairman and Co-Founder, Arceo.ai

Maggie Wilderotter
Former Chairman and CEO,
Frontier Communications

CLTC

Center for Long-Term Cybersecurity

UC Berkeley

Berkeley SCHOOL OF INFORMATION

CENTER FOR LONG-TERM CYBERSECURITY

CLTC.BERKELEY.EDU

@CLTCBERKELEY