An Eye on the Future

2023 ANNUAL REPORT
UC BERKELEY CENTER FOR LONG-TERM CYBERSECURITY

DIRECTORS' LETTER

2023 will be remembered as the year that the Center for Long-Term Cybersecurity's mission to advance cybersecurity clinics snowballed into an international movement. In June, the Consortium of Cybersecurity Clinics, co-founded and co-chaired by CLTC, announced a transformative $20+ million partnership with Google to expand our network to 20 higher education-based cybersecurity clinics by 2025. This was followed by announcements of similar investments to spread the clinic model in Europe and Asia. Cybersecurity clinics were also included in the White House Office of the National Cyber Director's Workforce Strategy, and Congressional testimony highlighted the benefits of clinics. The model pioneered at UC Berkeley's Citizen Clinic since 2018 has truly achieved lift-off.

We're also ahead of the curve in anticipating the opportunities and challenges of artificial intelligence. While the rapid rise of AI tools like ChatGPT caught many off guard, CLTC has been anticipating such technologies for years, in keeping with our future-oriented mission. Five years ago, we launched the AI Security Initiative (AISI), a groundbreaking program dedicated to developing strong standards for the safe, responsible use of AI in a range of contexts. AISI research has proved to be a valuable resource to industry practitioners and has informed regulation like the NIST AI Risk Management Framework.

Closer to home, we are grateful to Professors Chris Hoofnagle and Andrew Reddie for their leadership and support, as they concluded their terms as faculty co-directors of CLTC. From leading the Future of Cybersecurity Working Group to coordinating a groundbreaking conference on digital security in Taiwan, Chris and Andrew helped ensure that CLTC's work stayed relevant and forward-focused.

As we enter our 10th year, we are pleased to welcome Professor Marti Hearst, Interim Dean of the School of Information, as our next Faculty Director. We remain focused on fulfilling our mission to amplify the upside of the digital revolution, help decision-makers act with foresight, and expand who has access to and participates in cybersecurity. We are grateful to you, our community of friends and supporters, and hope to see you soon at one of our upcoming events.

Ann Cleaveland
Executive Director, CLTC

Marti Hearst
Acting Faculty Director, CLTC;
Interim Dean, School of Information

Above: An AI-generated rendering of a time machine, created by the World Economic Forum for a presentation on Cybersecurity Futures 2030, an initiative led by CLTC to help decision-makers anticipate how digital technology may evolve over the next 3-6 years.

A FOCUS ON THE FUTURE

CYBERSECURITY FUTURES 2030

What will digital security look like in the year 2030 — and how can today's decision-makers prepare for the future? The strategic imperative to look over the horizon is at the heart of Cybersecurity Futures 2030, a scenario-based initiative led by CLTC in partnership with CNA's Institute for Public Research and the World Economic Forum Centre for Cybersecurity.

Throughout 2023, CLTC facilitated a series of in-person and virtual workshops with decision-makers from geographies around the world, including Dubai, UAE; Delhi, India; Kigali, Rwanda; diverse European countries; the UK; Singapore; and Washington, D.C.. Our goal: to better understand how technological, political, economic, and environmental changes are shaping the future of cybersecurity.

In December, we published the project's findings in *Cybersecurity Futures 2030: New Foundations*, a report replete with insights to help governments and organizations prepare for a rapidly evolving cybersecurity landscape.

In January, CLTC Executive Director Ann Cleaveland presented Cybersecurity Futures 2030 at the World Economic Forum's annual meeting in Davos, Switzerland. Cleaveland moderated a dialogue about the findings with Ken Xie, Founder, Chairman and CEO of Fortinet. Read a recap and watch the presentation In December, we published the project's findings in Cybersecurity Futures 2030: New Foundations, a report replete with insights to help governments and organizations prepare for a rapidly evolving cybersecurity landscape.

In January, CLTC Executive Director Ann Cleaveland presented Cybersecurity Futures 2030 at the World Economic Forum's annual meeting in Davos, Switzerland. Cleaveland moderated a dialogue about the findings with Ken Xie, Founder, Chairman and CEO of Fortinet. Read a recap and watch the presentation.

CLTC 2023 BY THE NUMBERS

$20M
Amount pledged by Google to grow US-based cybersecurity clinics

1304
Number of attendees at CLTC events in 2023

78
Number of media outlets covering CLTC in 2023

52
New participants in the Consortium of Cybersecurity Clinics monthly calls

25
Number of speakers at the 2023 Cyber Civil Defense Summit

12
AI Policy Hub Fellows supported since 2022

5
Number of continents where Cybersecurity Futures 2030 workshops were held

A FOCUS ON THE FUTURE

CYBER DEFENDING TAIWAN: LESSONS FROM UKRAINE

In September, CLTC hosted "Cyber Defending Taiwan: Lessons from Ukraine," a daylong conference centered on applying lessons learned from Russia's invasion of Ukraine to strengthen Taiwanese cybersecurity and infrastructure. Drawing over 120 attendees, the conference featured panelists from academia, government, research, and the intelligence community.

"The ongoing tension between China and Taiwan represents one of the most critical flashpoints in international relations today," explained Chris Hoofnagle, Faculty Director of CLTC, in opening remarks. "There are profound implications for regional stability, and for international security.... Let's navigate these uncertain waters today to foster a deeper understanding of the dynamics and the strategic options."

Read a recap of Cyber Defending Taiwan and download a report on the conference.

CYBER AND INTERNATIONAL SECURITY

CLTC welcomed two postdoctoral scholars whose research spans the intersection of digital security and international governance.

Elaine Korzak researches a wide range of legal and policy aspects of cybersecurity, including norms and international law in cyberspace, cyber capacity-building, and international export control regimes seeking to curb the proliferation of commercial spyware and cyber weapons.

Gil Baram works at the intersection of cyber and international security, including such topics as cyber warfare and covert actions, the role of intelligence agencies in cyberattacks, cyber threats to space systems, and other topics.

(L to R): Elaine Korzak and Gil Baram

DEVELOPING TOMORROW'S LEADERS

CLTC supports early-stage researchers who are working on the cutting edge of digital security. Our past affiliates have gone on to assume professorships at leading universities, and to serve as leaders in industry, non-profit, and government positions.

AI POLICY HUB FELLOWS

Led jointly by CLTC and the CITRIS Policy Lab, the AI Policy Hub trains UC Berkeley graduate student researchers (shown above) to develop governance and policy frameworks to guide artificial intelligence, today and into the future.

In 2023, we welcomed the second cohort of AI Policy Hub Fellows, a group of six outstanding graduate students working on a range of topics, including developing new methods to prevent deception in AI-based language models, harnessing computer vision to help first responders, strengthening safety mechanisms in generative AI models, and developing publicly verifiable proofs to ensure that AI systems are fair, valid, and reliable.

CAL CYBERSECURITY FELLOWS

Through the Cal Cybersecurity Research Fellowship, CLTC supports the work of scholars exploring new frontiers of cybersecurity. In 2023, the fellowship focused on the intersection of cybersecurity and artificial intelligence and machine learning technologies. Three UC Berkeley graduate students received funding for their work in 2023: Gowri Swami studies the limits of free speech for AI-generated content on the internet, Sarah Barrington is developing a deepfake 'Captcha' to help identify synthetic media, and Marsalis Gibson is investigating new methods for preventing machine learning-based attacks on autonomous vehicles.

Gowri Swami

SUMMER RESEARCH COHORT

Nyah Mattison

CLTC welcomed a multi-disciplinary cohort of four summer researchers, who explored topics such as how boards of directors use cybersecurity metrics, the interdisciplinary cybersecurity education landscape, and bridging the knowledge gap between cybersecurity, safety, and software engineers.

CLTC summer researcher Nyah Mattison, who works with CLTC's AI Security Initiative and the Algorithmic Fairness and Opacity Group (AFOG), organized a panel on responsible AI licensing. Watch a recap.

EXPANDING WHO PARTICIPATES IN CYBERSECURITY

A key part of CLTC's mission is to expand access to the field of cybersecurity, and make it more accessible to people from all walks of life. As part of this mission, we showcase the voices of communities that are disproportionately affected by digital harms.

For example, we convened an online panel that brought together representatives from Berkeley Underground Scholars, an organization of UC Berkeley students who were formerly incarcerated, to discuss how people affected by the criminal legal system are subjected to privacy and surveillance, online financial scams, and other harms — along with potential solutions. (Watch the panel.)

CYBERSECURITY ARTS CONTEST

In June, we announced the winners of our third-annual Cybersecurity Arts Contest, which aims to expand representations of cybersecurity through artistic expression and public dialogue. Three projects were selected: Kyle McDonald's "Facework," a game that imagines a world where face analysis is key to the latest gig economy app; Mac Pierce's "Portrait of a Digital Weapon," a series of electronically activated portraits depicting infamous, real-life examples of computer viruses being used as a tool of geopolitical and financial attack by nation-states; and Seeyam's "Kristine Is Not Well," an animated social media simulation that visualizes how internet users protest against algorithmic surveillance and censorship with interactive and spatial metaphors in virtual reality (VR).

GROWING THE MOVEMENT FOR CYBERSECURITY CLINICS

2023 was a breakthrough year for cybersecurity clinics, higher education-based programs that train students to provide digital security

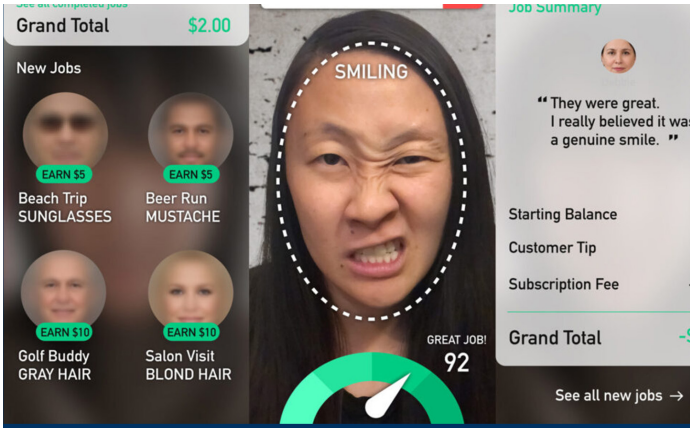


Image from Kyle McDonald's "Facework," a winner of the 2023 CLTC Cybersecurity Arts Contest.

assistance to non-profits, city governments, and other critical public infrastructure organizations. Cybersecurity clinics are a "win-win" as they are helping train the next generation of cybersecurity professionals while shoring up cybersecurity in local communities.

In June, Google pledged $20+ million to grow and establish 20 US-based cybersecurity clinics by 2025, well on the way to the Consortium of Cybersecurity Clinics' goal to establish a clinic in every state by 2030. UC Berkeley received funding to expand its Citizen Clinic, a course in the UC Berkeley School of Information that helped pioneer the cybersecurity clinic model.

Google CEO Sundar Pichai, Acting National Cybersecurity Director Kemba Walden, and UC Berkeley's Ann Cleaveland (front right), pictured together with cybersecurity clinic students from across the U.S. — including Citizen Clinic alumna Zaina Siyed (far left) — at the June announcement of Google's $20M+ commitment in cybersecurity clinics.

UC BERKELEY
CITIZEN CLINIC

1. Citizen Clinic receives scoping grant from the MacArthur Foundation, with additional support for work focused on low-risk organizations. — JAN.-DEC. 2017
2. APRIL-JULY 2018 — Citizen Clinic launches pilot. Research Fellow Sean Brooks publishes "Defending Politically Vulnerable Organizations Online."
3. Citizen Clinic begins its first full year of instruction. — SEPTEMBER 2018
4. SPRING 2019 — Citizen Clinic offers its first advanced class, and is formally certified as a course in the UC Berkeley School of Information.
5. Citizen Clinic class offered online as part of Master of Information and Cybersecurity program; Microsoft supports research on scaling-up the model. — SUMMER 2019
6. FALL 2019 — Citizen Clinic creates open-source website on GitHub to provide access to resources; mentorship program established with private-sector volunteers.
7. Citizen Clinic enrolls 18 students, bringing the total to over 60 students from more than 10 different academic programs — WINTER/SPRING 2020
8. FEBRUARY 2020 — Citizen Clinic secures its first $275K grant from Craig Newmark Philanthropies to grow its scale and impact.
9. CLTC publishes "Digital Safety and Technical Assistance at Scale," by Citizen Clinic Director Sean Brooks. — JUNE 2020
10. MAY 2021 — UC Berkeley, MIT, Indiana University, and the University of Alabama launch the Consortium of Cybersecurity Clinics, a network for sharing best practices and resources.
11. The Consortium launches cybersecurityclinics.org to share teaching materials, client resources, and news about clinics. Membership grows to 10 clinics and ally organizations. — MAY 2022
12. SUMMER 2022 — The Consortium receives seed funding from the Public Interest Technology University Network (PIT-UN) and Fidelity Charitable Trustees' Initiative. Craig Newmark Philanthropies pledges $1.7M to grow the Consortium network and Cyber Civil Defense Summit.
13. The Consortium hosts the first "Clinic of Clinics" tabletop exercise and student networking event, which becomes a tradition every semester. — NOV. 2022
14. JUNE 2023 — Google pledges $20+ million to support 20 new and existing cybersecurity Clinics in the U.S., in collaboration with the Consortium of Cybersecurity Clinics.
15. ONCD publishes the National Cybersecurity Workforce Strategy; the Consortium publishes the "Clinic Development Toolkit," by Program Director Sarah Powazek. — JUNE 2023
16. OCT. 2023 — UC Berkeley, along with nine other clinics, receives $500,000 from Google to expand Citizen Clinic, which has trained more than 165 students and served 17 non-profit clients. Cumulative Consortium alumni reaches nearly 900 students.
17. Citizen Clinic adds a second class section on-campus. The Consortium of Cybersecurity Clinics grows to 18 active and developing clinics and ally organizations around the world. — WINTER 2023-2024

CITIZEN CLINIC MARKS 5TH ANNIVERSARY

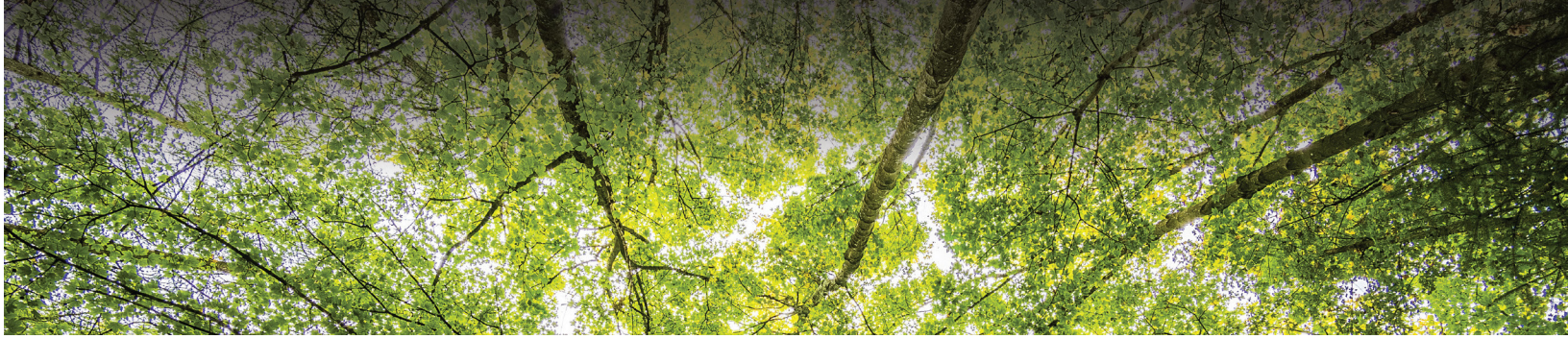
Launched in 2018, UC Berkeley's Citizen Clinic helped pioneer the model for cybersecurity clinics, through which students provide pro bono digital security assistance to non-profits, city governments, and other organizations with limited resources to defend themselves online. To the right, a timeline shows the evolution of the Citizen Clinic and the Consortium of Cybersecurity Clinics.

PARTNERSHIP WITH CYVERSITY

Throughout 2023, CLTC continued to grow our partnership with Cyversity, an organization dedicated to securing inclusivity in the cybersecurity field.

During the RSA Conference in April, we teamed up to lead an event inside Salesforce Tower called "Cultivating Diverse Cybersecurity Leadership," sponsored by Accenture.

And in December, we celebrated our partnership with Cyversity at an event on the UC Berkeley campus, with the theme, "Stronger Together: Securing Inclusivity in Cyber." Keynote speakers included Marco Lindsey, Associate Director of Diversity, Equity and Inclusion at the UC Berkeley Haas School of Business, and Justin Steele, Director of Google.org, Google's philanthropy arm, in the Americas region.



HELPING LEADERS ACT ON FORESIGHT

CLTC works to help bring research from academia into broadly usable contexts, and to help leaders in government, industry, and the nonprofit sector act on foresight.

AI SECURITY INITIATIVE

CLTC's AI Security Initiative is working to shape standards for the safe, responsible development and use of AI. In early 2023, AISI program director Jessica Newman published *A Taxonomy of Trustworthiness for Artificial Intelligence*, a complement to NIST's AI Risk Management Framework (AI RMF) that provides guidelines to AI organizations and teams developing AI technologies, systems, and applications. The Taxonomy was one of a small number of external resources selected for inclusion in NIST's Trustworthy & Responsible AI Resource Center, which is intended to support usability by connecting the AI RMF more closely to product cycles and workflows. Several companies and government agencies have incorporated the Taxonomy in their AI governance practices.

A team of AISI researchers led by Anthony Barrett published the *AI Risk-Management Standards Profile for General-Purpose AI Systems (GPAIS) and Foundation Models*, a robust resource that provides risk-management practices and controls for identifying, analyzing, and mitigating risks of large language models and other "general purpose" AI systems. The paper was accepted into the Association for the Advancement of Artificial Intelligence (AAAI) Fall Symposia in the Assured and Trustworthy Human-Centered AI track. The work was also selected for inclusion in the OECD Catalogue of Tools & Metrics for Trustworthy AI, and has been endorsed by numerous key stakeholders in industry, government, and civil society.

AISI researchers regularly present their work in public forums and with policymakers, including with the National Institute of Standards and Technology (NIST), US Agency for International Development (USAID), the White House Office of Science and Technology Policy (OSTP), the World Economic Forum, and many others.

Jessica Newman
Director, Artificial Intelligence Security Initiative

Anthony Barrett
Visiting Scholar, CLTC

QUANTIFYING CYBERSECURITY FOR CORPORATE GOVERNANCE

CLTC Visiting Scholar Laura Schaffner is developing a groundbreaking, research-based reporting template that can be used by boards of directors, security executives, investors, and companies to monitor, disclose, and evaluate risks and opportunities related to cybersecurity. This template is designed with a financial statement format that can be used across industries.

Laura Schaffner

CYBER CIVIL DEFENSE SUMMIT

In June, CLTC hosted the inaugural Cyber Civil Defense Summit, a daylong conference focused on exploring novel solutions to help non-profits, local governments, hospitals, small businesses, and other community-based organizations defend themselves online. The sold-out event drew more than 100 participants, including high-level cyber professionals, academics, government officials, and journalists, who convened to share and spread creative programs aimed at bolstering the cyber resilience of public interest organizations.

The event featured a series of panel discussions and "fireside chats," as well as keynote presentations by Jen Easterly, Director of the Cybersecurity and Infrastructure Security Agency (CISA); Wendy Nather, Head of Advisory CISOs at Cisco; and Craig Newmark, founder of craigslist and Craig Newmark Philanthropies.

Read a recap of the Summit.

From left to right: Sarah Powazek, Program Director, CLTC Public Interest Cybersecurity Program; Ann Cleaveland, CLTC Executive Director; Craig Newmark, Founder, craigslist and Craig Newmark Philanthropies; and Jen Easterly, Director of CISA.

CLTC WHITE PAPERS AND PUBLICATIONS

CLTC researchers regularly author journal articles and white papers that serve a variety of audiences, presenting the latest scholarship to the academic research community and to the public in a clear, accessible format. In 2023, we released publications on a wide array of topics:

Future Directions in Corporate Disclosure on Digital Responsibility, by CLTC Postdoctoral Scholar Jordan Famularo, illustrates how institutional investors, technology firms, and civil society are shaping norms about how companies should disclose information related to digital responsibility.

A Comparative Study of Interdisciplinary Cybersecurity Education, by Lisa Ho, Sahar Rabiei, and Drake White, examines how different universities approach the challenge of teaching cybersecurity through an interdisciplinary lens, with a goal to guide other educational institutions as they develop and create their cybersecurity programs.

Privacy Legislation on the Ground: Effects of and Responses to the GDPR and CCPA, by Saba Chinian, examines how firms have responded to two major privacy laws: the European Union's General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA).

Representing Privacy Legislation as Business Risks: How Technology Companies Discuss the GDPR and CCPA in Investment Risk Disclosures, by Richmond Wong and Andrew Chong, examines how technology companies assess the business risks of privacy regulation.

"Inside the Internet," a paper published in Duke Law Review by Nick Merrill and Tejas Narechania, highlights the potential harms of the consolidation of content delivery networks, or CDNs, which serve as part of the core infrastructure of the internet. The authors argue that the shrinking number of CDNs raises concerns for network reliability, online speech, and consumer choice, among other issues.

LOOKING AHEAD

Late 2024 marks CLTC's 10th birthday, and we have an exciting array of programs lined up for the coming months.

- On June 13, CLTC will present the second-annual Cyber Civil Defense Summit, a one-of-a-kind gathering of cyber defenders, academics, and policymakers with a shared mission of protecting the most vulnerable public institutions against cybersecurity threats.. This year's event will be held in Washington, DC at the International Spy Museum. Register here!
- CLTC's Public Interest Cybersecurity program is collaborating with the City of San Francisco to help Bay Area community-based organizations (CBOs) to improve their cybersecurity defenses. We will publish results this year, with a goal to identify threat mitigations that can serve as a model for cities across the country.
- Hanlin Li, a former CLTC post-doc, will be wrapping up a research project on the implications of data scraping in the development of AI technologies. (Read Hanlin's op-ed about data scraping.)
- CLTC's AI Security Initiative is working together with the CITRIS Policy Lab on a collaboration on responsible AI and generative AI with the Washington state government. Working in support of Washington Technology Solutions (WaTech), the UC Berkeley team is conducting interviews with Washington state government employees to understand current and planned uses of generative AI technologies, benefits and challenges, and desired guidance and oversight. They will produce a report and their work will help inform WaTech guidelines for public sector procurement, uses, and assessments of generative AI technology. This work builds on previous collaboration with the California Department of Technology.
- Through the Consortium of Cybersecurity Clinics, we will continue to strengthen the capacity of new and existing cybersecurity clinics. The Google Cybersecurity Clinics Fund will announce funding for 10 new clinics in the US this spring, and we will host a pre-conference workshop at the NICE Conference in June, "Building a higher education cybersecurity clinic for the long-term."technology. This work builds on previous collaboration with the California Department of Technology.

THANK YOU!

We offer heartfelt thanks to our valued philanthropic partners and contributors, who propel CLTC's future. Special thanks to Google for their first-time and phenomenal investment in CLTC and cybersecurity clinics; to Craig Newmark Philanthropies for multi-year support; to our four Cybersecurity Futures 2030 partners, Fortinet, Meta, Okta and Repsol; and to the following funders, whose investments have helped guide our success in 2023: Fidelity Charitable Trustees' Initiative, the Future of Life Institute, the Omidyar Network, our valued CLTC External Advisory Committee, and many individual alumni and friends of UC Berkeley. Last but not least, we thank The William and Flora Hewlett Foundation for not only strengthening our reserves in 2023, but also for your visionary and generous founding gift that established CLTC in November 2014. We would not be here without you and the talented staff behind your trailblazing Cyber Initiative.