2020 MID-YEAR UPDATE

UC BERKELEY CENTER FOR LONG-TERM CYBERSECURITY

CLTC
Center for Long-Term Cybersecurity
UC Berkeley

A WORLD TRANSFORMED

Dear Friends,

The first half of 2020 has brought unexpected challenges to the world, to the cybersecurity research community, and to CLTC. The pandemic has meant tremendous new hardships for families around the globe, and the struggle for racial equality in the U.S. reached an acute tipping point in May. We've heard many of our friends and colleagues say they feel like 10 years of digital transformation has happened in something like 10 weeks. Because we focus on how to amplify the upside of change, we're energized for what comes next, and resolute in our efforts to improve digital security in the public interest.

As you'll see in this report, we've been fortunate to be able to continue to publish research and drive dialogue around relevant topics like safe and ethical artificial intelligence deployment, the digital security of under-resourced non-profit organizations, impacts of the pandemic on the global security law and policy landscape, and emerging and diverging cybersecurity concerns and opportunities in regions of the Global South.

We are grateful to our dedicated corporate, foundation, and individual supporters, and to our new collaborators, including most recently Craig Newmark Philanthropies, whose support is playing a critical role as we advance our research and mission and scale our impact.

Thank you for your ongoing support, and please contact us with questions, feedback, or ideas via email at cltc@berkeley.edu.

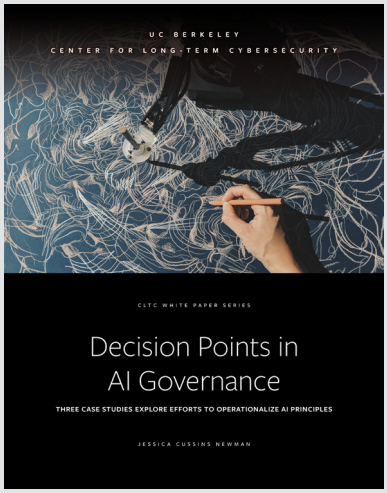
Steven Weber
Faculty Director

Ann Cleaveland
Executive Director

DECISION POINTS IN AI GOVERNANCE

A new report from CLTC's AI Security Initiative highlights how organizations are translating AI ethical principles into practice

In recent weeks, Amazon, Microsoft, and IBM have announced they will limit their sale of facial recognition software to law enforcement agencies, highlighting some of the ethical questions that are emerging alongside the advancement of artificial intelligence (AI). The Center for Long-Term Cybersecurity's AI Security Initiative (AISI) is working to address these questions, and help organizations develop and implement principles and practices to guide the use of these powerful new technologies.



In May, the AISI published a report, *Decision Points in AI Governance*, that provides an in-depth look at how organizations are translating AI principles —frameworks designed to improve safety, accountability, and other goals in support of the responsible advancement of AI — into practice.

Authored by Jessica Cussins Newman, program lead for the AISI, the report outlines 35 efforts already under way to implement AI principles, from tools and frameworks to standards and initiatives that can be applied at different stages of the AI development pipeline.

The paper focuses on three recent efforts as case studies: Microsoft's AETHER Committee, established to evaluate normative questions related to AI; OpenAI's "staged release" of a language processing model, which challenged traditional software publishing norms to promote research and dialogue about possible harms; and the Organisation for Economic Co-operation and Development (OECD) AI Policy Observatory, launched earlier this year as part of an international effort to establish shared guidelines around AI.

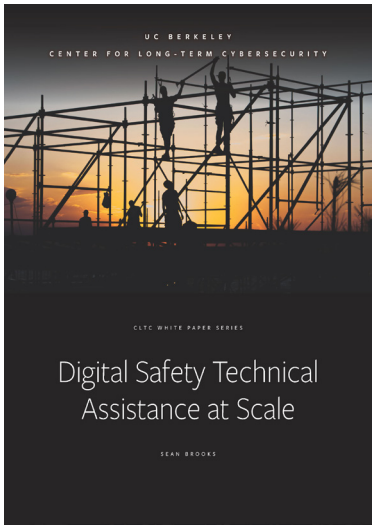
"The question of how to operationalize AI principles marks a critical juncture for AI stakeholders across sectors," Newman wrote. "Each case provides a meaningful example with lessons for other stakeholders hoping to develop and deploy trustworthy AI technologies."

Decision Points in AI Governance offers guidance for other AI stakeholders — including companies, communities, and national governments — facing decisions about how to safely and responsibly develop and deploy AI. The report has already drawn the attention of tech policy executives and was covered in media outlets like VentureBeat, Global Government Forum, and Biometric Update. In addition, Newman was invited to join the OECD Network of Experts on AI (ONE AI), an informal advisory group that provides expert input to the OECD's analytical work.

"Decisions made today about how to operationalize AI principles at scale will have major implications for decades to come," Newman wrote. "AI stakeholders have an opportunity to learn from existing efforts and to take concrete steps to ensure we build a better future."

Download the report at:
cltc.berkeley.edu/decision-points

CITIZEN CLINIC ISSUES REPORT ON SCALING DIGITAL SAFETY ASSISTANCE



CLTC's Citizen Clinic is a first-of-its-kind program that engages interdisciplinary teams of UC Berkeley students to provide digital safety services to politically targeted civil society organizations.

Citizen Clinic has remained active during the COVID-19 pandemic, as a team of 17 students worked throughout the spring (and six during the summer), supporting seven client organizations. "The Clinic, like everyone else, encountered a significant shock during the onset of the COVID shutdowns," said Sean Brooks, director of Citizen Clinic. "But luckily, because of the program's experience with online-only classes through our summer course for the Master of Information and Cybersecurity (MICS) program, and the determination and dedication of our incredible students, the projects of this spring's class were some of our best yet.

In June, Brooks released a new report that explores the opportunities and challenges of expanding digital safety technical assistance to civil society at a scale and pace that match the sector's needs.

Digital Safety Technical Assistance at Scale draws in part upon lessons learned from the first two years of operating Citizen Clinic. The report offers practical guidance on what will be needed to deliver cybersecurity assistance on a larger scale, and highlights examples of diverse technical assistance projects, as well as tactics from sectors outside the cybersecurity space.

The report assesses the strengths and limitations of diverse approaches to scaling up digital safety technical assistance, including volunteer networks, cybersecurity clinics, and community hubs. These technical assistance models all provide potential benefits, Brooks concludes, but all contribute differently to scaling digital security services for civil society organizations.

"Activating already existing expertise and helping organizations utilize existing channels for support are important elements, but we must also expand the number of professionals in the space," Brooks wrote. "A more nuanced perspective on the digital safety challenges facing civil society organizations is essential not only for providing a high quality of service, but also for designing appropriate technical products and policies."

In addition to providing valuable assistance to underresourced organizations, Citizen Clinic is helping develop a pipeline for talent. Citizen Clinic alumni have gone on to work at such organizations as Amnesty International, Google, Microsoft, and the ACLU.

CITIZENCLINIC.IO

Introducing the Citizen Clinic Online Cybersecurity Education Center

Citizen Clinic has officially launched the Citizen Clinic Cybersecurity Education Center, a GitHub site (citizenclinic.io) designed to share the Clinic's pioneering cybersecurity resources for civil society organizations, and to help other academic institutions that may be interested in establishing their own cybersecurity clinics. The site includes the Citizen Clinic curriculum, reading lists, and syllabi, as well as a link to a Baseline Organizational Security Guide.

"We see it as a library of sorts: a place to share what we've learned for others to learn, repurpose, and critique," said Citizen Clinic Deputy Director Steve Trush. "Citizen Clinic learns so much about the challenges of securing politically targeted civil society groups that we want to have a single place to share our activities, outputs, and lessons learned."

Thanks to an additional gift from the William and Flora Hewlett Foundation, Citizen Clinic is developing a coordinated communications campaign to build awareness about these newly developed resources, with an ultimate aim to scale the Clinic's unique model and help a growing number of civil-society organizations defend themselves online.

Citizen Clinic Gets Philanthropic Boost from craigslist Founder to Help At-risk Groups with Cybersecurity

Citizen Clinic has received $275,000 in grant support from Craig Newmark Philanthropies to expand and refine its work training students to provide digital safety assistance to politically targeted organizations, and creating new pathways for women in cybersecurity careers. This generous grant from the founder of craigslist will help Citizen Clinic develop a variety of resources — including workshops and training curricula — to make its model and methods more accessible to other organizations, including universities that want to build their own clinics, as well as journalists, NGOs, and technical assistance providers that want to duplicate the Clinic's successful practices.

DAYLIGHT SECURITY RESEARCH LAB

Led by CLTC Researcher Nick Merrill, the Daylight Security Research Lab works to shift the way people understand and identify the harms of technology—and expand the populations able to do so.

In recent months, the Daylight Lab has continued to develop its Internet Interoperability Index (III), a first-of-its-kind analysis of how different countries' internets differ based on diverse measures, including how their laws regulate the flow, storage, or production of data in 66 different countries; which websites are most commonly visited across 144 countries; and to what degree government and private-sector network interference impacts browsing around the globe.

"With this tool, policymakers could create more targeted interventions to, for example, 'join' a like-minded cluster or reduce transaction costs with an opposing cluster," Merrill explains. "Those in industry could use these clusters as a key strategic planning tool, allowing them to move products across internets that, despite superficial differences, are actually interoperable."

Meanwhile, the Daylight Lab team has begun a new study to measure the effectiveness of "Adversary Personas," an improvisational role-playing game developed to help teams better imagine potential security threats. Adversary Personas focuses on the "who" of security by forcing players to ask: who might our adversaries be, what do they want, and what would they be willing to go through to get it? This summer's study will engage groups of software developers and UX designers, who will play through a newly developed online version of the game.

The Daylight Lab is also working to bring awareness to the potential failures and biases of machine-learning algorithms. The Twitter account, @MLFailures, aggregates examples of mistakes made by AI systems. And this spring, Merrill led the development of a Jupyter notebook designed to help people understand how AI systems might be biased or provide erroneous or incomplete answers. This new teaching tool uses the example of a health risk-assessment (as might be used by an insurance provider) to expose how AI systems can exhibit racial bias in recommending treatment.

Merrill is planning to introduce this important new teaching tool into UC Berkeley computer science, statistics, and applied math courses, and to later bring the lab to other universities in the U.S. and around the world. "This is a first-of-its-kind class focused on teaching students how to detect machine-learning bias in real-life settings, which is urgently needed right now."

EVENT SERIES: CLTC CYBERSECURITY ARTS CONTEST

The Daylight Lab has launched a new series of virtual events featuring the winners of the inaugural CLTC Cybersecurity Arts Contest. The first event showcased "The Price Is Wrong," a three-part mockumentary that aims to start dialogue on cybersecurity in the African context through a lens of comedy and realism.

Moderated by Elizabeth Resor, a PhD student in the School of Information, the panel featured Neema Iyer, Executive Director of Pollicy, a civic technology organization that works at the intersection of data, design and technology to revolutionize civic engagement and participation, and Shayna Robinson, a Uganda-based artist and former member of the Pollicy team.

Iyer and Robison explained that "The Price is Wrong" aims to help audiences understand what cybersecurity really looks like in Uganda, where a cybercrime can be as simple as having your phone stolen at the local market. "Cybersecurity threats happen every day around us," Iyer said. "It's people who look like us... It's in the market. It's in the taxi."

The producers stressed the need for more cybersecurity research and education that is accessible and culturally relevant, and for more technologies that are appropriate for the African context. "Most of the technology that is used by African users is developed in the Global West and the Global North, with very little input from African users," Iyer said. "A lot of projects are being outsourced to foreign companies, and that is eating into the little space that we have for indigenous innovation and development."

Read more of the interview on the CLTC Bulletin, https://www.medium.com/cltc-bulletin. And stay tuned to the CLTC newsletter for updates about upcoming Arts Contest panels. The next event will be held on July 15.

RESEARCH PROFILE: **MATT OLFAT**

The development of fifth-generation cellular technology (5G) is set to dramatically expand the number of devices connected through the "internet of things" (IoT). Yet this rapid proliferation of devices — from smart appliances to autonomous cars — will usher in countless new nodes of attack for malicious actors, and the security software in many IoT devices may be unable to adapt to variable external conditions.

This central challenge at the heart of research led by Matt Olfat, a recent PhD graduate from the School of Information — and the 2019 recipient of the Cal Cybersecurity Fellowship. Olfat worked with researchers from UC Berkeley's Department of Industrial Engineering and Operations Research and the University of Michigan to develop a new approach called "covariance-robust dynamic watermarking," which helps keep a system's defenses strong, even under dynamic conditions. The researchers described the approach in a paper that was submitted to the Controls and Decisions Conference (CDC).

"People have come up with methods for testing whether an attack is happening, but they depend on knowing everything about the system and everything remaining static," Olfat explains. "There's a lot of potential for noise in sensor measurements resulting from things like temperature or weather. A self-driving car that gets tested in Palo Alto, where it's not raining and is always 72 degrees, doesn't reflect reality. If the weather gets more humid or it starts raining, the noise input to these sensors is going to be different, which will change the efficacy of these security methods."

Traditional "watermarking" entails "injecting a little bit of randomness into your controls that you know about, but the attacker does not," Olfat says. "Our contribution was to make sure this could be applied even when you don't know what the surrounding noise is and when it changes. Even if the weather or road conditions change, the cybersecurity test — to determine if there's a cyberattack going on — would remain valid, whereas previous work might send off false alarms or might be fooled entirely."

Covariance-robust dynamic watermarking emerged from the integration of methods that were previously developed to reduce bias in machine-learning systems, where systems are designed to be adaptive to a variety of inputs. "We connected the dots between the fairness and cybersecurity literature and were able to come up with cybersecurity methods that were more robust to shifts in state dynamics," Olfat explains. "These notions of fairness and robustness in statistical learning situations are very closely connected, and there is a lot of opportunity to bring these areas of cybersecurity research together."

CLTC and Booz Allen Hamilton Release Report on Board Governance

In January, CLTC released a report — authored in partnership with Booz Allen Hamilton — that used insights gleaned from board members with 130+ years of board service across nine industry sectors to offer guidance for boards of directors in managing cybersecurity risk within large global companies.

The report, *Resilient Governance for Boards of Directors: Considerations for Effective Oversight of Cyber Risk*, provides an innovative framework to help boards take a dynamic approach to cybersecurity governance and oversight. The report has helped inform the practices of diverse organizations, and earned coverage from an array of media outlets, including CIO Dive, Help Net Security, and the Security and Compliance Weekly podcast, which featured CLTC Executive Director Ann Cleaveland.

INTRODUCING "SECURITY WIRE"

CLTC has launched a new quarterly conference call designed for members of our Corporate Membership Program and other supporters. Each "Security Wire" call focuses on an emerging cybersecurity topic relevant to our industry partners.

The first call in the series featured UC Berkeley Professors Hany Farid and Steven Weber discussing content moderation and Section 230 of the Communications Decency Act. The second featured Weber in conversation with Arik Ben-Zvi, CEO and President of Breakwater Strategy (BWS), on "COVID-19 Future: Digital Security Implications."

"We take it as a welcome challenge to produce insights that serve short-term needs and have longer-term staying power," Weber said. "'Security Wire' is our new format for sharing those insights in a collaborative way with our corporate partners."

To learn more about the Corporate Membership Program, visit https://cltc.berkeley.edu/corporate-membership-program/ or email cltc@berkeley.edu.

AI SECURITY INITIATIVE (AISI)

The AI Security Initiative works across technical, institutional, and policy domains to support trustworthy development of AI systems today and into the future.

The AISI is working on many fronts to shape the dialogue around artificial intelligence. Following the release of her *Decision Points* paper (see page 1), Jessica Cussins Newman published an op-ed in "The Hill" focused on how the pandemic has exposed risks related to the use of AI. "The COVID-19 pandemic has spurred a massive and sudden change in human behavior, sending automation into a 'tailspin,' and exposing fragilities in integrated systems our society relies upon," she wrote. "This comes at a time when we need artificial intelligence (AI) more than ever."

In February, the AISI co-hosted an event featuring Professor Bin Yu, Chancellor's Professor in the Departments of Statistics and Electrical Engineering & Computer Science at UC Berkeley, who spoke about "Veridical Data Science," focusing on a predictability, computability, and stability (PCS) framework that aims to provide responsible, reproducible, and transparent results across the data-science life cycle.

The AISI has also hired a team of graduate student researchers (GSRs), who are conducting research about diverse topics related to artificial intelligence, including competitive race dynamics in industrial AI applications, AI safety and the aviation industry, AI-enabled surveillance technologies for national security and border control, the detection and analysis of backdoor attacks in deep neural networks, and more.

Collectively, these efforts are helping shape the dialogue about how institutions can address the potential risks and benefits of AI-based technologies—in California, the United States, and around the world.

CLTC Convenes Dialogue with U.S. Cyberspace Solarium Commission

CLTC recently convened a virtual roundtable with representatives from the U.S. Cyberspace Solarium Commission, as well as other government agencies and private firms, to probe the question, "How can the U.S. Government and the private sector work together under the 'defend-forward' strategy to protect the nation's critical interests?"

Participants were asked to be candid about challenges that need to be addressed and resolved in order to bridge the gap between the Commission's vision and what is possible for government agencies and companies to achieve on the ground.

The discussion was anchored in scenarios designed to help participants consider in more concrete terms the kinds of situations for which their organizations might need to prepare in the future, including a hypothetical situation in which the goverment is warned about a nation-state adversary preparing for a major cyber attack against the U.S. financial and telecommunication sectors; and a scenario in which a nation-state adversary escalates malign influence campaign activities against the U.S., consisting of increased disinformation via social media accounts and hijacking Twitter and Facebook accounts of U.S. public officials and private citizens.

Participants shared viewpoints in response to these scenarios, noting where collaboration between government and industry breaks down. The discussion identified several areas where future work could expose the barriers to collaboration and develop practical steps to overcome them.

Among the opportunities highlighted were the need for a better defined U.S. government strategy; improved processes for information sharing; and improved recognition for positive actions firms are taking.

"As our dialogue reinforced, there is a significant amount of work to be done in all of these domains, but there is also appetite to deepen this kind of discussion, addressing bite-sized pieces that could be taken into the practical, tactical realm," wrote Ann Cleaveland, Executive Director of CLTC, in a summary of the project. "The relationships that are developed before a crisis — and a shared commitment to joint planning — will make the difference between successful defend-forward actions, and those that adversaries can avoid or defeat."

Read more on the CLTC Bulletin:
https://medium.com/cltc-bulletin

CLTC SUPPORTS STUDENT AND FACULTY CYBERSECURITY RESEARCH ACROSS CAMPUS

In January, CLTC announced the recipients of our 2020 research grants. In total, 22 different groups of researchers — including both students and faculty — shared nearly $1 million in funding to support a broad range of initiatives related to cybersecurity and digital security, including secure machine learning, data protection policy, understanding the privacy implications of always-on IoT devices, detecting malicious photo manipulation, and more. Learn more about our 2020 grantees at https://cltc.berkeley.edu/grants.

Projects Awarded Funding for 2020

- A Cryptographic Study of Data Protection Laws
- An Open Research Privacy Toolkit
- Crafting Public Policy for Reinforcement Learning Applications
- Cybersecurity for Non-Primary and Primary Users of Always-On Internet of Things Devices: An Ethnographic, Participatory, and Multidisciplinary Design Approach
- Cybersecurity Guidance for COVID-19 Pandemic Tracking (MICS Capstone Project)
- The Cybersecurity of "Smart Infrastructure"
- Designing a Privacy Curriculum for the Elderly
- Detecting Images Generated by Neural Networks
- Examining The Third-Party Tracking Ecosystem
- Eximius Hardware Key (MICS Capstone Project)
- Hard Pass: Passwordless Authentication (MICS Capstone Project)
- How Do Vulnerable Patients Understand Data Privacy as It Pertains to mHealth Interventions?
- Keystone: An Open Framework for Architecting TEEs
- Law Enforcement Access to Digital Data: Understanding the Everyday Processes
- Measuring and Defending Against New Trends in Nation-State Surveillance of Dissidents
- Novel Metrics for Robust Machine Learning
- Obscuring Authorship: Neural Methods for Adversarial Stylometry and Text-Based Differential Privacy
- Secure Authentication in Blockchain Environments
- Secure Machine Learning
- Data for Defenders
- Developing A Common Vocabulary Around Privacy and Security Concepts With Elderly Users
- Digital Tools for Decentralized Networks (in partnership with Build Belonging)
- Privacy-preserving Machine Learning for Autonomous Vehicles
- Understanding Online Reputation Damage and Repair for Student Activists

Cal Cybersecurity Fellow 2020: Nathan Malkin

Nathan Malkin, a UC Berkeley PhD student in the Department of Electrical Engineering and Computer Science, received the 2020 Cal Cybersecurity Research Fellowship to support his research on privacy controls for "always-listening" devices. Malkin is the second recipient of the Cal Cybersecurity Fellowship, which was made possible by an anonymous Cal alumnus, includes an award of up to $15,000, and is given to students or postdoctoral scholars to pursue cybersecurity research.

"With today's devices — for example, smart speakers like Amazon Echo and Google Home — you essentially have two modes: the device is listening, or it isn't," Malkin said. "What would it be like to have more fine-grained control over what the device is allowed to hear at any given moment? We think this is especially important as these devices evolve more 'passive listening' capabilities, analyzing conversations and other sounds that aren't necessarily directed at them."

RECENT CLTC NEWS

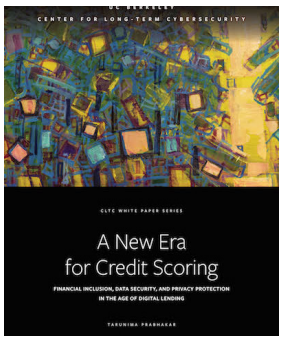
Visit our website and subscribe to our newsletter to stay up to date on CLTC news!

Kristin Berdan Joins Citizen Clinic

We are pleased to announce that Kristin Berdan, former lead cybersecurity counsel at Google, will be joining the Citizen Clinic team as a Research Fellow. Berdan helped Google transform into a multi-billion dollar company with scores of data centers and the world's largest and most advanced global computing network, operating in compliance with laws and regulations worldwide. Drawing on her legal background, extensive experience with internet infrastructure, and motivated by concern for public-interest cybersecurity, she will research how to effectively assess and prioritize needs, define and measure impact, and customize proposed security measures for journalists and newsrooms. A key objective is building collaborative relationships with other stakeholders in the public and private sectors, including corporate partners of CLTC, to align our work, while working closely with students enrolled in the Citizen Clinic program.

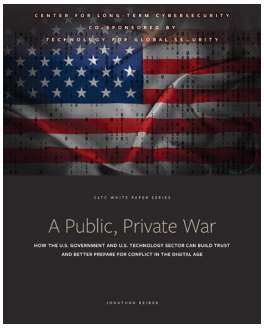
New Report on Digital Lending in India

In June, CLTC released a new report by Research Fellow Tarunima Prabhakar, *A New Era in Credit Scoring: Financial Inclusion, Data Security, and Privacy Protection in the Age of Digital Lending*, that explores the trade-offs inherent to digital lending apps, which are increasingly common in developing countries. Based on an in-depth analysis of lending apps in India, Prabhakar's paper explores how digital lending apps provide economic opportunity to people without credit scores, but they also represent a significant threat to privacy, as lenders use an array of mobile data — including age, location, and even personal contacts — to gauge an individual's willingness and ability to pay. "The example of India highlights how, in an emerging economy with relatively weak institutions and low financial literacy, credit scoring through alternate data creates the possibility for rapid progress in financial inclusion — but under weaker consumer protection standards," Prabhakar writes. "The constant threat of exposure of consumer information adds to the challenge...."



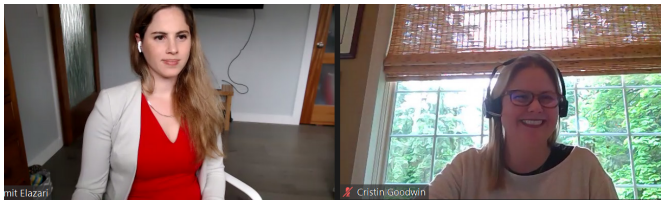
CLTC and Tech4GS Release "A Public, Private War" Report

A report co-published by CLTC and Technology for Global Security (Tech4GS) provides a blueprint for how the U.S. government and private-sector companies can collaborate to prepare for a cyberwar or other massive cyberattack on U.S. interests. Authored by Jonathan Reiber, former Chief Strategy Officer for Cyber Policy and speechwriter in the Office of the Secretary of Defense, *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* outlines a series of policy recommendations for both the government and companies to improve their preparedness. "At some point in the future the United States will likely enter into escalating hostilities with a cyber-capable adversary," Reiber wrote. "Public-private preparation for war is an uncomfortable but necessary process to prepare for that day or, better, help deter that day from ever arriving."



Virtual Event Features Experts from Intel, Microsoft

In May, roughly 50 attendees joined remotely as CLTC hosted Amit Elazari, Director, Global Security Policy at Intel Corporation (and the newest member of our External Advisory Committee) and Cristin Goodwin, Assistant General Counsel for Cybersecurity and Digital Trust at Microsoft, for a virtual conversation on recent trends in the landscape of international digital security policy amid COVID-19. The two experts discussed the evolving attack landscape, how governments and policymakers are responding to rapid changes from a cybersecurity regulatory lens, as well as how the pandemic crisis impacts the (near- and longer-term) horizons of the global security law and policy landscape. A video of the discussion is available at cltc.berkeley.edu.



CLTC Hosts 2020 Welcome Reception Featuring Royal Hansen, VP of Security at Google

In January, CLTC welcomed about 70 attendees for a reception to kick off the new semester and welcome and congratulate our 2020 grantees. This year's reception also featured a keynote address from Royal Hansen, VP of Security at Google, who discussed the importance of partnerships between corporations and academic institutions in shaping the future of cybersecurity, including tackling security challenges related to open-source hardware, key management and data encryption, digital forensics, group access management, and disinformation and data integrity.

Women in Tech Symposium: Reimagining Cybersecurity for All

CLTC co-sponsored the 4th annual Women in Tech Symposium, held in March, and helped organize the day's first panel titled, "What's at Stake? Global and Systemic Cyber Threats," featuring a distinguished panel of women at the forefront of the dynamic intersection between people and digital technologies. Fifteen percent of attendees at this year's Women in Tech Symposium said they are more likely to pursue a career in cybersecurity, and 42% said they are more confident about entering the field.

Citizen Clinic Hosts Panel on Indigenous Security

On February 11, CLTC and Citizen Clinic hosted a panel focused on the physical and digital security challenges that indigenous communities face, as well as possible solutions. The panel featured Daniel Kobei of the Ogiek Peoples' Development Programme (OPDP), a Kenya-based non-governmental organization working to support the rights of the indigenous Ogiek community; Jemimah Kerenge, Director of Enkishon Indigenous Initiative, which helps Maasai communities in Kenya to acquire social and economic equality; and Casey Box, Director of Land is Life, a global support organization for indigenous communities around the world. A video of the panel is available at cltc.berkeley.edu.

NEW "EXPLAINER" VIDEO ON DIFFERENTIAL PRIVACY

CLTC will soon be releasing a new animation as part of our "What? So What? Now What?" series, which aims to make cybersecurity concepts understandable to a general audience. The new video will focus on differential privacy, an approach that allows data scientists to derive insights from large data sets while protecting the privacy of individuals.

CLTC Research Fellow Publication on 5G Security Singled Out for Excellence

A publication by Melissa Griffith, CLTC non-resident research fellow and Ph.D. candidate in the UC Berkeley Department of Political Science, was singled out by the University of Pennsylvania's Think Tanks and Civil Societies Program, based on its 2019 Global Go To Think Tank Rankings Survey. Griffith's publication, *5G and Security: There is More to Worry About than Huawei*, explains how 5G would represent a significant challenge for American national security, even without China as a peer competitor.

Weber New Head of School of Information

Steven Weber, CLTC's Faculty Director, has been appointed Associate Dean and Head of School for the UC Berkeley School of Information. Steve will hold this position at a critical time, as the I School is integrating into the newly formed Division of Computing, Data Science, and Society (CDSS), an ambitious new structure to advance research where people, technology, and data science intersect, to help solve some of society's greatest challenges. Weber will hold the Associate Dean post until the end of 2020, when he will return to a sabbatical cut short due to the pandemic.

LOOKING AHEAD...

Save the Date for CLTC Research Exchange

The fourth-annual CLTC Research Exchange, our annual showcase of the work of our grantees, will be held on October 1. This year's conference will be entirely virtual, offering an opportunity for attendees around the world to learn about cutting-edge research from across the UC Berkeley campus. Registration will open soon. Stay tuned to the CLTC newsletter or visit https://cltc.berkeley.edu.

New Paper on 5G Security

In the coming weeks, CLTC will be releasing a new report on the security implications of 5G networks. The paper is authored by Jon Metzler, a lecturer at the UC Berkeley Haas School of Business, who conducted a survey of security risks posed by 5G wireless network deployments, as well as potential practices for risk mitigation. The research is in advance of commercial 5G network deployments and thus will have potential value to network operators, regulators and consumers.

Upcoming Virtual Arts Events

The second event in our virtual arts event series will be held on July 15. This event will feature Lauren McCarthy, an LA-based artist examining social relationships in the midst of surveillance, automation, and algorithmic living. (Register at https://virtualcaring.eventbrite.com.) The third event, featuring artist Greg Niemeyer, will be held on September 16.

A Partnership for AI in California

The AI Security Initiative is launching a new, year-long partnership with the California Department of Technology and the CITRIS Policy Lab to investigate and provide guidance for the uses of AI applications throughout California government agencies.

New Research in the Works

CLTC Faculty Director Steven Weber has new research forthcoming on diverse topics, including data sharing; the economic and cultural distributional consequences of machine translation, and the intellectual history of the relationship between privacy and privatization.

Visit the CLTC Bulletin!

Visit our blog (https://medium.com/cltc-bulletin) for insights, articles, and essays by our community of researchers, faculty, students, and collaborators.

Thank you, Corporate Members!

CLTC is grateful for the support of companies in our Corporate Partnership Program! Visit our website (cltc.berkeley.edu) to learn more.

SUPPORT CLTC

CLTC helps people address tomorrow's information security challenges, train the next generation of cybersecurity leaders, and amplify the upside of the digital revolution. Together with individual supporters and valued corporate partners, your support helps us:

- Inform future-focused research and policy agendas across government, industry, and civil society.
- Advance diverse and multi-disciplinary original cybersecurity research through the CLTC Grants program.
- Help politically targeted organizations to stay safe online through Citizen Clinic.
- Analyze global impacts of artificial intelligence through our AI Security Initiative.
- Illuminate the cultural dimensions of cybersecurity through our Daylight Security Research Lab.

Gifts of all sizes help our students and faculty advance groundbreaking research, train larger numbers of future information security professionals, and expand our outreach to support civil society organizations.

Learn more at cltc.berkeley.edu/give

Contact Us

Do you have questions, ideas, or other feedback? Feel free to contact us—and be sure to sign up for our newsletter and follow us on Twitter and Facebook to receive updates on news, events, job opportunities, and more.

cltc@berkeley.edu
https://cltc.berkeley.edu
@CLTCBerkeley

Berkeley SCHOOL OF INFORMATION