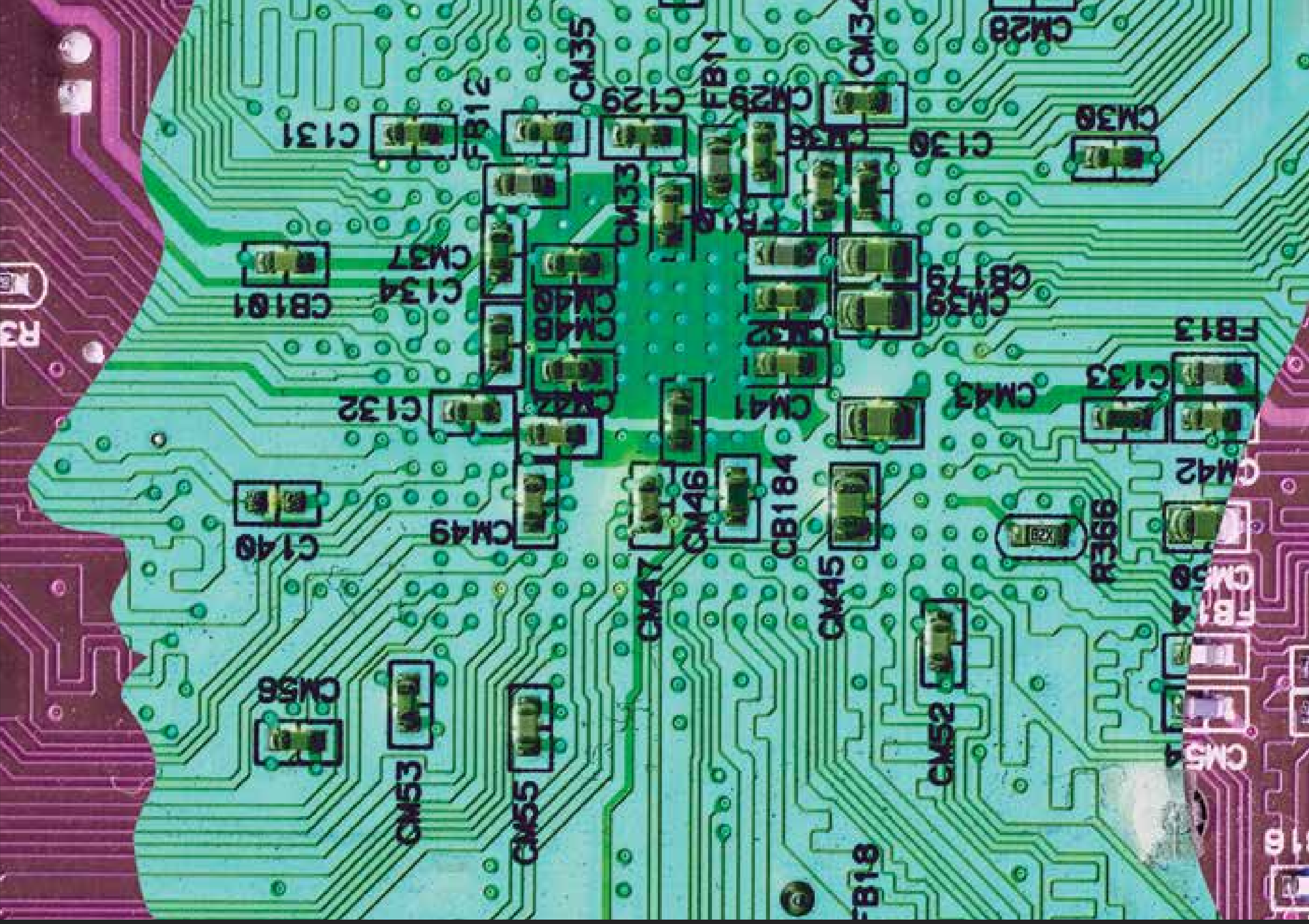


Center for Long-Term Cybersecurity

UNIVERSITY OF CALIFORNIA, BERKELEY

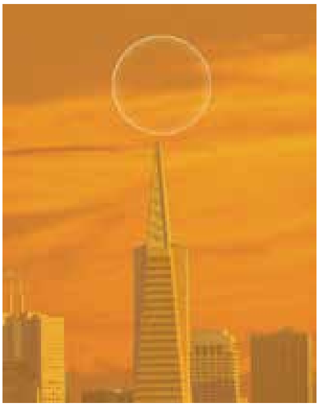
Research

CLTC supports research aligned with our future-oriented framework for cybersecurity. Our interests encompass not only computer science and engineering, but also economics, political science, law, psychology, and other domains. Questions our grantees are exploring include:

- How can organizations better detect spear-phishing cyberattacks?
- How could neural signals be used for online authentication?
- How effective are tactics such as financial account closures and asset seizures in deterring cyber criminals?
- What types of defenses could help protect at-risk activists and NGOs from state-level surveillance?
- How can corporations better understand and manage legal liabilities and other risks related to cyber attacks?

Omega

Data scientists of 2020 have developed powerful models capable of predicting—and manipulating—the behavior of individuals with a high degree of accuracy. Predictive analytics generate new security vulnerabilities that focus on people rather than infrastructure.



Bubble 2.0

Major web companies collapse, and criminals and companies alike race to gain ownership of underpriced but potentially valuable data assets. As vast troves of data change hands, the collapse of the industry leaves unemployed data scientists seeking new opportunities.

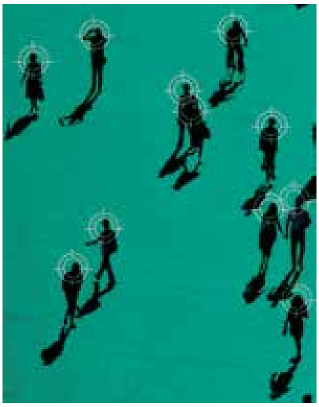
About the Center

The Center for Long-Term Cybersecurity is a research and collaboration hub housed within the University of California, Berkeley School of Information. Funded through a generous seed grant from the William and Flora Hewlett Foundation, CLTC seeks to design solutions to cybersecurity issues that arise wherever humans and digital systems interact, based on a long-term vision of the internet and its future.

Working with researchers from UC Berkeley and outside organizations, we are building a diverse community of partners to advance research, technologies, and recommendations that will help governments, corporations, and individuals better prepare for the challenges of cybersecurity throughout the 21st century. We focus our work on three streams of activity: research, education, and engagement.

THE SCENARIOS

CLTC has developed a set of scenarios—narratives depicting possible futures for the year 2020—to inform our research agenda and provoke dialogue among researchers, industry practitioners, and government policymakers.



The New Normal

Following years of mounting data breaches, internet users in 2020 assume that their data will be stolen and their personal information broadcast. Cyberspace is the new Wild West, and internet users who want protection and justice have to fend for themselves.

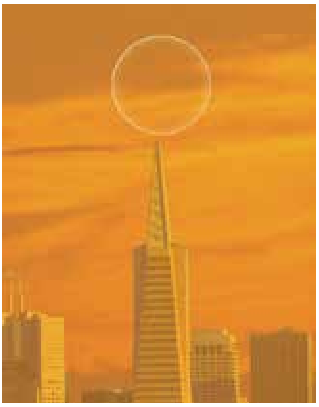
Education

Training diverse researchers and professionals is a core issue in the cybersecurity space. From our home in the UC Berkeley School of Information, CLTC is developing new programs to improve and expand education.

Among other activities, we are partnering with the I School and the College of Engineering to develop a new master's degree program in cybersecurity. We organize regular seminars led by experts from diverse fields, and we sponsor a reading group that meets regularly to discuss works related to emerging issues in cybersecurity. And we are developing a technical training for women and minorities who may be interested in making a lateral transition from other careers into the cybersecurity field.

Omega

Data scientists of 2020 have developed powerful models capable of predicting—and manipulating—the behavior of individuals with a high degree of accuracy. Predictive analytics generate new security vulnerabilities that focus on people rather than infrastructure.



Bubble 2.0

Major web companies collapse, and criminals and companies alike race to gain ownership of underpriced but potentially valuable data assets. As vast troves of data change hands, the collapse of the industry leaves unemployed data scientists seeking new opportunities.

Engagement

To ensure that our work extends beyond the "ivory tower," CLTC sustains partnerships with institutions from government, industry, and other sectors. We participate in research partnerships in the United States and globally; we hosted a meeting of the White House-led Commission on Enhancing National Cybersecurity; we participate in industry events and conferences; and we regularly invite guest speakers for seminars and presentations. Recent guests include:

- Admiral Michael Rogers, Commander, U.S. Cyber Command; Director, NSA
- Vinton G. Cerf, Co-founder of the Internet
- James C. Trainor, Jr., Assistant Director, Cyber Division, FBI
- Parisa Tabriz, Head of Information Security Engineering, Google
- David and Orion Hindawi, Co-Founders of Tanium

The Intentional Internet of Things

The Internet of Things proves powerful in addressing issues related to education, the environment, and other social challenges, but hackers find new opportunities to manipulate the vast network of devices, often in subtle and undetectable ways.

Sensorium

New devices for tracking biometric information—including hormone levels, heart rates, and more—enable the tracking and manipulation of people's underlying mental, emotional, and physical states. Managing one's public emotional state becomes intrinsic to cybersecurity.

CLTC

Center for Long-Term Cybersecurity

UC Berkeley

Center for Long-Term Cybersecurity

cltc.berkeley.edu

@CLTCBerkeley