Cybersecurity Futures 2020

CENTER FOR LONG-TERM CYBERSECURITY
UNIVERSITY OF CALIFORNIA, BERKELEY

It's the Year 2020 . . .

How might individuals function in a world where literally everything they do online will likely be hacked or stolen? How could the proliferation of networked appliances, vehicles, and devices transform what it means to have a "secure" society? What would be the consequences of almost unimaginably powerful algorithms that predict individual human behavior at the most granular scale?

These are among the questions considered through a set of five scenarios developed by the Center for Long-Term Cybersecurity (CLTC), a new research and collaboration center founded at UC Berkeley's School of Information with support from the Hewlett Foundation.

CLTC's mission is to develop a deeper and broader understanding of how the future of cybersecurity could unfold differently from today. At the heart of our approach is *scenario thinking*, a proven methodology for identifying driving forces and unexpected permutations of causes that could shape the future.

With the help of a diverse set of experts, CLTC developed five scenarios for the year 2020. These scenarios are not predictions—it's impossible to make precise predictions about such a complex set of issues. Rather, the scenarios paint a landscape of future possibilities, exploring how emerging and unknown forces could intersect to reshape the relationship between humans and technology—and what it means to be "secure."

These scenarios will inform CLTC's research agenda and serve as a starting point for conversation among academic researchers, industry practitioners, and government policymakers. They provide a framework for questions we should be asking today to ensure a more secure information technology environment in the future.

We welcome your feedback and questions via email at cltc@berkeley.edu.

Sincerely,

Steve Weber
Faculty Director

Betsy Cooper
Executive Director

SCENARIO 1

The New Normal

Following years of mounting data breaches, internet users in 2020 now assume that their data will be stolen and their personal information broadcast.

Law enforcement struggles to keep pace as larger-scale attacks continue, and small-scale cyberattacks become entirely commonplace—and more personal. Governments are hamstrung by a lack of clarity about jurisdiction in most digital-crime cases. Hackers prove adept at collaborating across geographies while law enforcement agencies do not.

Individuals and institutions respond in diverse ways: a few choose to go offline; some make their data public before it can be stolen; and others fight back, using whatever tools they can to stay one step ahead of the next hack. Cyberspace in 2020 is the new Wild West, and anyone who ventures online with the expectation of protection and justice ultimately has to provide it for themselves.

KEY QUESTIONS

- What are the implications for commerce, politics, social relations, and privacy when insecurity is accepted as the starting point and prevailing norm of internet life?
- What changes will be required for infrastructure to adapt to a world where the internet is ubiquitous, insecure by assumption, and "unfixable"?
- How can we identify the warning signs and tipping points that will lead to a wholesale change in attitudes and behaviors about cybersecurity?

SCENARIO 2

Omega

Data scientists of 2020 have developed profoundly powerful models capable of predicting — and manipulating — the behavior of single individuals with a high degree of accuracy.

The ability of algorithms to predict when and where a specific person will undertake particular actions is considered by some to be a signal of the last—or "omega"—algorithm, the final step in humanity's handover of power to ubiquitous technologies.

For those responsible for cybersecurity, the stakes have never been higher. Individual predictive analytics generate new security vulnerabilities that outmatch existing concepts and practices of defense, focus increasingly on people rather than infrastructure, and prove capable of causing irreparable damage, financial and otherwise.

KEY QUESTIONS

- What new kinds of attack vectors could emerge in an age when computers have the potential not only to predict behavior, but also to shift in precise ways the behavior of individuals or groups?
- How might the rise of predictive technologies reconfigure power within the international order, for example from developed to developing countries, or from government to private sector?
- What regulation schemes are likely to be most effective for governing predictive technologies?

SCENARIO 3

Bubble 2.0

Two decades after the first dot-com bubble burst, the advertising-driven business model for major internet companies falls apart.

As overvalued web companies large and small collapse, criminals and companies alike race to gain ownership of underpriced but potentially valuable data assets. It's a "war for data" under some of the worst possible circumstances: financial stress and sometimes panic, ambiguous property rights, opaque markets, and data trolls everywhere.

In this world, cybersecurity and data security become inextricably intertwined. There are two key assets that criminals exploit: the datasets themselves, which become the principal targets of attack; and the humans who work on them, as the collapse of the industry leaves unemployed data scientists seeking new frontiers.

KEY QUESTIONS

- How might cybercriminals adapt to a more open and raucous data market?
- If governments want to prevent certain datasets from having a "for-sale" sign attached to them, what kinds of options will they have?
- What new systems or standards could emerge to verify the legitimacy or provenance of data? What does "buyer beware" look like in a fast-moving market for data?
- What role should government play in making markets for data more efficient and secure?

SCENARIO 4

Intentional Internet of Things

In 2020, the Internet of Things (IoT) is a profound social force that proves powerful in addressing problems in education, the environment, health, work productivity, and personal well-being.

California leads the way with its robust "smart" system for water management, and cities adopt networked sensors to manage complex social, economic, and environmental issues such as healthcare and climate change that used to seem unfixable. Not everyone is happy, though. Critics assert their rights and autonomy as "nanny technologies" take hold, and international tensions rise as countries grow wary of integrating standards and technologies.

Hackers find countless new opportunities to manipulate and repurpose the vast network of devices, often in subtle and undetectable ways. Because the IoT is everywhere, cybersecurity becomes just "security" and essential to daily life.

KEY QUESTIONS

- How will device makers install patches to secure software as the number of networked devices grows exponentially?
- How might the ubiquity of networked devices and sensors change the scale and nature of cyberattacks and the skills required of cybersecurity professionals?
- What, if any, public backlash will arise in a society that is increasingly monitored, managed, and at the same time tangibly improved through network-based systems?
- How might existing methods of breaching networks—e.g., phishing attacks— adapt and evolve in a world of ubiquitous IoT technologies?

SCENARIO 5

Sensorium

In 2020 wearable devices won't care about how many steps you take; they will care about your real-time emotional state.

With devices tracking hormone levels, heart rates, facial expressions, voice tone, and more, the internet is now a vast system of "emotion readers," touching the most intimate aspects of human psychology. These technologies allow people's underlying mental, emotional, and physical states to be tracked—and manipulated.

Whether for blackmail, "revenge porn," or other motives, cybercriminals and hostile governments find new ways to exploit data about emotion. The terms of cybersecurity are redefined, as managing and protecting an emotional public image and outward mindset appearance become basic social maintenance.

KEY QUESTIONS

- How might biosensing technologies evolve, and what would be the impact of sensors that track emotion and mental states at a large scale?
- How will people respond when their most private and intimate experiences are understood by the internet better than they understand those experiences themselves?
- How might virtual reality, sentiment analysis, wearable devices, and other "sensory" technologies intersect with domains such as marketing, politics, and the workforce?
- What are the potential cybersecurity risks and benefits that could come with the proliferation of sensors capable of capturing and interpreting emotions?

CONTACT

For more details on and the full text of the scenarios, please visit our website at cltc.berkeley.edu.

Postal Address School of Information
University of California, Berkeley
102 South Hall #4600
Berkeley, CA 94720-4600

Voice: (510) 644-7506
Fax: (510) 642-5814

Email: cltc@berkeley.edu

CLTC

Center for Long-Term Cybersecurity

UC Berkeley