The University of California, Berkeley Center for Long-Term Cybersecurity was founded to develop and shape the next generation of cybersecurity research and practice based on a long-term vision of the internet and the future of digital technology.

Cybersecurity, in our view, will encompass the key issues—those important enough to deserve the word "security"—that emerge at the intersection between technology and people. Attacking and defending today's (and tomorrow's) computers and networks is a part of that story, but only a part. In the not-so-distant future, most things (and most people) will be connected to digital networks. "Cyber" will become a baseline assumption. "Security" will also undergo a reformulation much like what happened to "national security" after the end of the Cold War, in which a term once focused on superpower nuclear deterrence grew to encompass a much broader agenda, including environmental security, economic security, and "human" security.

For these reasons we believe the cybersecurity research and policy communities will soon confront a much more diverse set of problems and opportunities than they do today. To shed light on that emerging landscape, we have developed a disciplined, imaginative approach to modeling what cybersecurity could mean in the future (which we define for purposes of this report as the year 2020).[1] Our goal is to identify emerging issues that will become more important; issues on the table today that may become less salient or critical; and new issues that researchers and decision-makers a few years from now will have wished people in the research and policy communities had noticed—and begun to act on—earlier.

To this end, we are using scenario thinking, a proven methodology for investigating expansively and purposefully how cybersecurity future(s) might unfold. Scenarios traditionally have been used by organizations to develop long-term strategies; this may be one of the first attempts to use scenarios in an academic context to help shape a policy-relevant research agenda.

In this Introduction, we review why and how we engaged in scenario thinking, the methods we employed, and the preliminary outcomes of that process.

SCENARIO THINKING AND THE FUTURE OF CYBERSECURITY: WHAT, WHY, AND HOW

Scenario thinking is a *tool for ordering arguments about alternative future environments* in which today's and tomorrow's decisions will play out. Whether used for strategic planning or identifying research priorities, scenario thinking is based on three core propositions.

1. Change and surprise in fast-moving socio-technical environments are often a consequence of unexpected and/or unexamined *permutations* among seemingly disconnected or unrelated forces of change. The world is never shaped by "just" technology, human behavior, regulation, or business models; rather, it is shaped by all of these at once, in overlapping fashion. In other words, many drivers of change work together to create new opportunities and constraints, causing new problems to arise and others to recede.
2. Some of the most important driving forces of change come from diverse domains—healthcare, markets, social norms, and the like—outside the immediate, day-to-day, tactical environment where cybersecurity experts and organizations naturally tend to focus. Analysis of these driving forces often needs to be "stretched" further than is comfortable in order to identify edge-cases where potential sources of change become most visible.
3. New, relevant, and sometimes inspirational research programs and policy concepts develop out of constructive engagement with models that incorporate these multiple dimensions of uncertainty and emphasize how the future could be different from the present in significant and discontinuous ways. In other words, scenarios are heuristic devices that highlight new hypotheses, insights, and ideas about the future.

Royal Dutch Shell pioneered the use of scenario thinking in corporate planning during the 1970s, when multiple oil shocks followed from dramatic shifts in the political, economic, social, technological, and military (among other) determinants of the global energy system. The methodology was further

developed in the 1990s by Global Business Network and was employed in a wide variety of corporate, nonprofit, and government settings. Over time, practitioners of scenario thinking determined that scenarios work best when they are treated as *hypotheses*, not predictions, and when they are used to segment, highlight, and compare some of the very different possibilities for a changed environment.

To emphasize the point: scenario thinking is *not* an attempt to predict the future or create "the" single answer to the "What will cybersecurity be in the future?" question. And it is certainly not an attempt to understand that future as a direct or linear extrapolation of current trends. Instead, scenario thinking focuses on how causes from different domains and directions intersect with one another to create discontinuities that might change what cybersecurity means. Scenarios then become a tool for investigating what needs to be understood, and what needs to be done, in order to prepare for an uncertain future as it begins to unfold and undermine assumptions that govern thinking and action today.

If we are right in our starting proposition that "cybersecurity" could mean something quite different in 2020 than it does today—both conceptually and operationally—then the value of suspending disbelief to "live in" and understand these alternative future scenario worlds becomes clear.

It is not particularly useful to debate whether one scenario is more or less likely than another—or whether these are mutually exclusive and/or comprehensively exhaustive pictures of the future. No model we know of could achieve those goals. We aim instead to provoke a discussion about what the cybersecurity research and policy communities need to do *now* in order to be better positioned for a world that might very well include some of these scenario elements.

The test of scenario thinking is not whether it predicts or portrays the future accurately. The measure of a successful set of scenarios is this: enabling people and organizations to gain insight into possible futures in which "cybersecurity" means something different than it does today, involves a broader set of actors, has meaningfully greater stakes, sits on different technological foundations, and engages core human values in a novel way.

We hope you will read and use these scenarios in that experimental spirit, and that you will share with us your reactions, questions, insights, and inspirations about both research and policy choices.

METHODOLOGY AND ASSUMPTIONS

Scenarios typically embrace qualitative perspectives and the potential for sharp discontinuities that more formal planning tools and models tend to exclude. We present these scenarios as a set of stories with causal narratives that are internally valid and logically consistent. The stories are sprinkled with indicative examples of the kinds of events and behaviors that would logically follow from the core driving forces that make up the model embedded in each scenario. These examples represent the kinds of data that would be observable indicators of a particular model but are not, again, point predictions. It is the *differences* between indicators in the five scenarios that are most important, rather than the precise examples per se.

Like any good model, scenarios also are used to generate implications. Here, those implications focus on the nature and scope of cybersecurity in each world. What cybersecurity challenges and objectives rise to the fore, and what needs to be done, by whom, in order to pursue them?

These scenarios were developed out of a process that began in May 2015. The Center for Long-Term Cybersecurity brought together a broad interdisciplinary group from universities, the private sector, nonprofits, and governments, and drew on their varied points of view and expertise to develop five prototype scenarios. Working with graduate students, the Center then elaborated on the drivers of change that were *most uncertain* and *most important* in these scenarios to refine the causal logics and illuminate their potential impacts. We tried to strike a balance between developing the richness and complexity of each narrative and making them accessible and digestible to the public as well as to professional communities. An early version of the scenarios was then made available, on a restricted basis, to key stakeholders and academics for engagement, commentary, and further refinement in late 2015 and early 2016.

Our aim in writing these five scenarios is to create a usable representation of an imaginative map of the possibility space—stretched in some respects to the boundaries of plausibility—that researchers, decision-makers, and policymakers can use to help navigate the future. As a modeling exercise, the discipline of "simplify, exaggerate the most important elements, and add the complexity back in" applies. We hope that in reading these scenarios you will seek not only to understand the core characteristics of each model that we present, but to ask yourself, "What would I need to understand and do differently if a world like this were to come into being?" Multiple answers to those questions will contribute to a forward-looking research and policy agenda that should be more robust, both intellectually and practically.

We welcome further engagement with and feedback on the scenarios via our website at cltc.berkeley.edu or via email at cltc@berkeley.edu.

ACKNOWLEDGMENTS

The Center for Long-Term Cybersecurity would like to acknowledge UC Berkeley School of Information graduate students Daniel Griffin, Elaine Sedenberg, and Richmond Wong, who wrote the first drafts of these scenarios with guidance from Professor Steve Weber, Associate Dean Jesse Goldhammer, and CLTC Executive Director Betsy Cooper; Jonathan Reiber, who provided useful consultative advice on the structure and implications of the scenarios; Faith Hutchinson and Jackie Jones, who provided stunning design assistance for this publication; Chuck Kapelke, Jenny Johnston, and Nader Namini Asl, who edited and shaped the scenarios and provided outstanding technical support; and the Hewlett Foundation, which funded this research. CLTC would also like to thank the more than 100 contributors, too many to name, who helped imagine, develop, analyze, critique, and extend the scenarios. CLTC is grateful to each and every one of them for their support.

EXECUTIVE SUMMARY

The five scenarios developed from this exercise are as follows:

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.

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..

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.

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.

SCENARIO 5: SENSORIUM (INTERNET OF EMOTION)

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.

1. We recognize that the year 2020 is a relatively near-term horizon, and that other scenario projects could look farther into the future.