CENTER FOR LONG-TERM CYBERSECURITY

CO-SPONSORED BY

TECHNOLOGY FOR GLOBAL SECURITY

CLTC WHITE PAPER SERIES

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

JONATHAN REIBER

CLTC WHITE PAPER SERIES

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

JONATHAN REIBER
Senior Advisor, Technology for Global Security
Visiting Scholar, UC Berkeley Center for Long-Term Cybersecurity

CENTER FOR LONG-TERM CYBERSECURITY
CO-SPONSORED BY
TECHNOLOGY FOR GLOBAL SECURITY

Contents

Executive Summary

In response to the increasing risk of cyberattack on human societies, nation-states have developed strategies and invested in capabilities to counter advanced cyberattacks on their interests. One of the most significant American investments includes the U.S. Defense Department's Cyber Mission Force, an elite force of 6,200 cyberspace operators tasked to blunt and disrupt incoming cyberattacks on the United States from abroad. Within the Cyber Mission Force, the Cyber National Mission Force has the mission of defending the United States against incoming cyberattacks and to prepare to "stop threats before they hit their targets" through forward defense campaigns, as the 2018 DoD cyber strategy states.[1]

While the United States government has made wise investments in cybersecurity capabilities and the Defense Department is uniquely authorized and equipped to disrupt adversary cyberspace infrastructure, the government does not own or operate most of the technological infrastructure of cyberspace, limiting its reach and situational awareness. Given the range of cyberthreats facing the United States, the government needs to work in partnership with the private sector to increase its ability to counter incoming cyberattacks on the nation.

One way to do so is for the public and private sector to plan and exercise together for combined, voluntary operations that the government and companies can prepare to conduct under their own legal authorities and terms of service agreements. There are precedents for such operations. In advance of the 2018 U.S. Congressional Elections, for example, U.S. Cyber Command conducted a counter-offense operation against the Russian Internet Research Agency, which had operated previously as an arm of Russian influence in the 2016 U.S. presidential elections, denying the Internet Research Agency's access to the Internet.[2] Separately, Microsoft and Facebook removed Russian operatives from their platforms to minimize Russia's ability to manipulate user and corporate data to influence the outcome of the elections.[3]

These actions together provide a potential blueprint for a new approach to combined, voluntary operations to counter cyberspace operations from abroad—to include destructive attacks conducted during a period of war, the likes of which the United States has not yet experienced in the digital age. Today, the United States is not in a state of war in cyberspace but rather in a "gray space" below the level of declared hostilities. At some point in the future the United States will likely enter into escalating hostilities with a cyber-capable adversary. 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.

Planning for such operations is harder than it first appears, however, as public-private cyberdefense cooperation presents a range of brand, market, and customer risks for companies and the government to consider. This study explores the issues inherent in public-private cyberdefense cooperation and recommends that the U.S. government focus on developing operational partnerships with the private sector that can augment those of the U.S. Cyber National Mission Force and other government agencies during a period of unfolding conflict or outright hostilities. There are obstacles to this cooperation, and this report highlights **four stories of trust, partnership, and mistrust** between the U.S. government and the U.S. technology sector from the last decade. These stories and others should inform the government and the private sector's approach to cybersecurity planning.

1. **The Basic-Input Output System (BIOS) Mitigation.** In 2010, the national security community and information technology community cooperated to close a vulnerability in the BIOS. They did so through the Enduring Security Framework,[4] a Department of Homeland Security-convened forum for the information technology sector and agencies of U.S. national security community to discuss best practices and emerging issues in cybersecurity. After the intelligence community identified that China had discovered a vulnerability in the BIOS, the two communities worked together to deploy a patch across hundreds of thousands of computers. The BIOS mitigation was widely heralded as showing the potential for advanced cybersecurity cooperation between the national security community and the information technology community.

2. **The Edward J. Snowden Intelligence Disclosures.** There is an old saying that trust is hard to build and easy to lose. After the successes of the BIOS mitigation, the U.S. government was on a trend-line to improve cybersecurity cooperation with the private sector just as the cyberthreat to U.S. interests was increasing in severity. Then in 2013, former Booz Allen Hamilton contractor Edward J. Snowden disclosed classified information regarding the U.S. government's work with the U.S. technology sector in collecting signals intelligence. The impact of this disclosure was both acute and long lasting. It led a number of global technology companies to end aspects of their cooperation with the national security community on cybersecurity.

   Two years after the disclosure, in a park outside of his office in Silicon Valley, a senior technologist with one of the world's leading software companies told this author, "I am a patriot and would have left my job and volunteered full-time to work with the government

on cybersecurity. After that, I told our company to stop working with the government." A few days earlier, a venture capitalist in Silicon Valley made a similar comment to a group of Defense Department senior officials, saying, "You cannot overstate the long-term negative impact [of Snowden] on the Valley's willingness to work with you."[5] The disclosures triggered deep feelings of betrayal across society.

3. **The Defense Contracts.** In 2018–2019, Google and Microsoft employees protested their companies' technology contracts with the Defense Department and, in Google's case, that protest led Google to end its participation in an artificial intelligence contract and to update its principles on artificial intelligence.[6] In response to the Google protest, a leaked Pentagon memo reflected the Defense Department's concern over its relationship with the private sector. "We will not compete effectively against our adversaries if we do not win the 'hearts and minds' of the key supporters," the memo read.[7] This story shows how employees' perceptions and views about the uses of their technology as well as their perceptions about threats facing the United States can impact a company's willingness to work with the U.S. national security community in meeting emerging security challenges.

   While Google withdrew its support for one of its defense contracts, Microsoft chose to sustain its work when it faced similar internal dissent over its own augmented reality contract with the U.S. Army. Both stories highlight the role that corporate leaders can play in navigating security policy issues, setting narratives, and shaping perceptions regarding cooperation, violence, and the use of force. It also shows the challenge that the national security community faces in trying to persuade the civil science and technology community to cooperate on advanced threats. Under what conditions does a threat become sufficiently severe to urge the best scientists and engineers to choose to take part in national defense? In part the answer rests on the nature of the adversary and their use or likely potential use of advanced weapons and other disruptive technologies.

4. **Combined Operations in Advance of the 2018 U.S. Congressional Elections.** If the Russian interference on the 2016 U.S. presidential election was a watershed moment in the world's awakening to the risks of the digital age, public and private sector actions to remove Russian operations from social media and technology company platforms in advance of the 2018 Congressional elections revealed a potential "new normal" of coordinated operations to counter malicious online activity. Building on history, this event provides a central test case for the future of operations.

Each story reveals obstacles for building trust and preparing for conflict in the digital age, as well as ways to build trust and capacity. Company employees may not trust the U.S. government; key corporate leaders may not trust their counterparts in the U.S. government; the American people may not trust companies or the government to secure their data or defend their interests; company employees may not trust their own corporate leadership. All of these conditions can shape U.S. national security planning. The most important condition for cyberdefense contingency planning, however, is for key leaders and key line officers in the national security community and major information technology companies to build trust between themselves.

POLICY RECOMMENDATIONS

This study focuses on the role of leaders and the development of close, trusting relationships for cyberdefense planning and operations. The public and private sectors in the United States share some interests, but in other cases their cultures, interests, and perceptions of the world differ significantly. The planning process can bring the two communities together and resolve a range of obstacles in trust, threat perception, and options development.

In summary, the research surfaces the following policy recommendations for the U.S. government and technology companies to pursue:

1. **The U.S. government and the private sector should make deliberate security planning a priority.** The planning process should focus on building trust, developing a shared understanding of the cyberthreat, and identifying downstream risks associated with public-private cyberdefense operations that a company may face. The process is as important as the substance. Companies and the government should devote personnel to building scenarios for small-group exercises and identifying options. Participants should be selected for their ability to build consensus, work with people of different cultural backgrounds, discover opportunity, and resolve conflict constructively. Technical acumen is far less important up-front. Over time, once teams coalesce, operators and technical experts should be brought in to work together on technical options.

2. **Companies should set clear terms of service for cyberdefense operations.** This policy should describe how a company will make decisions on a case-by-case basis for when and how the company will remove individuals', companies', or nation-states' access to products

and services. Microsoft has taken this position of adopting a "100% defense and zero offense" policy,[8] and provides a template for others to consider.

3. **Companies should design a public affairs strategy on cyberdefense cooperation with governments.** Public affairs postures should focus on the nature of the cyberthreat, and indicate that any states' unlawful action in cyberspace could present a risk to innocent lives, democracy, political stability, as well as to information technology and the future of innovation.

4. **U.S. government leaders should assign an appropriate leader to the Enduring Security Framework (ESF) for public-private planning.** The companies that are a part of the ESF have some of the most significant telecommunications and information technology capabilities in the world. A number of ESF participant companies were interviewed for this study and each expressed a desire to hold deliberate public-private cyberdefense planning, either through the ESF or a similar organization. There are multiple individuals within key information technology companies, telecommunications providers, and the U.S. government that want to begin to plan for cyberdefense operations. But since the BIOS mitigation, the Enduring Security Framework has not focused on developing cyberdefense partnerships for high-end contingencies. It provides a natural place to begin deliberations now, given its classified nature, historical precedent, and participation by key information technology companies.

5. **The government should assume the burden of risk during conflict in cyberspace, and not place unnecessary risks on the private sector.** It is the purpose and legal responsibility of the U.S. government and the U.S. military to defend the United States and its interests, and it is in the U.S. national interest for U.S. multinational technology companies to flourish and succeed in global markets. Information technology companies may be able to help the government achieve its national security missions in cyberspace and prevent a conflict from escalating, but the U.S. government should never ask the private sector to put itself at risk if other instruments of U.S. government policy can achieve the same effect without damaging partner companies.

Foreword and Acknowledgements

The purpose of this study was to identify obstacles and constraints for public-private cooperation in the event of escalating hostilities between the United States and a potential adversary, and to offer pathways for the government and the private sector to pursue going forward to improve the United States' collective defense.

The study emerged from three events. First, when Booz Allen Hamilton contractor Edward J. Snowden disclosed the activities of the National Security Agency in 2013, his actions frayed trust between the United States government and the American people, between the United States and its allies and partners, and, ultimately, between the U.S. government and the U.S. technology companies that build and operate so much of the infrastructure of cyberspace—and that are on the front-lines of defending their users against cyberattacks. The Snowden disclosures also led to a partial breakdown in public-private cybersecurity partnerships at an important time in the evolution of U.S. cybersecurity policy, a breakdown that only began to reverse itself following the significant and galvanizing impact of the Russian cyberspace influence operation and cyberattack on the 2016 U.S. presidential election.

Second, following the Snowden disclosures, I had a conversation in May of 2015 with a leading information security executive at one of the world's most influential information technology companies about why and how his company stopped cooperating with the U.S. government, and what it would take to bring him and his company back into defensive partnership. He began that discussion by venting his frustration over the government's actions—but by the end of our conversation, he expressed his willingness to explore a project focused on developing enhanced, public-private cyberdefense partnerships.

Third and finally, in 2016 the University of California at Berkeley's Center for Long-Term Cybersecurity (CLTC) hosted six executives from the public and private sectors to discuss the issues inherent in building voluntary, combined cyberdefense cooperation to defend the United States during a period of escalating tensions or outright hostilities. The positive disposition of the six leaders in that conversation proved that we had an opportunity to build a new approach

to cybersecurity planning: one that brought the national security community and the information technology community into a collaborative, deliberate process to plan for increasingly dangerous cyberattacks on U.S. interests. Thanks to the generous support of CLTC and the Smith Richardson Foundation, those conversations continued with other key leaders through 2019.

This report is the result of that work. The research process involved interviews with more than twenty leaders from the public and private sectors, including former and current government officials and senior officials from major information technology and telecommunications companies (all of whom were granted anonymity to speak openly); observations of cybersecurity table-top exercises with the public and private sector about election interference; a review of research on trust, operations, and issues in technology and security policy; and reflections on the last decade of public-private cooperation for cybersecurity and cyberdefense from my perspective, having served as an official in the Office of the U.S. Secretary of Defense in several policy roles, including as Chief Strategy Officer for Cyber Policy—and then working in Silicon Valley as head of cybersecurity strategy for a leading cybersecurity software provider.

A complex study like this requires foundation support, and I wish to thank Marin Strmecki, Vice President of the Smith Richardson Foundation, for graciously funding and supporting this study. I also thank him for his patience as I took on a new job in Silicon Valley, and then as the 2018 U.S. Congressional Elections became a surprising test case for the issues under review. Dr. Strmecki and Kathy Lavery at Smith Richardson deserve special thanks.

Thanks are due also to Phillip Reiner and Michael McNerney at Technology for Global Security for housing the author during the course of the grant, to Steve Weber and Ann Cleaveland at the Center for Long-Term Cybersecurity for agreeing to publish the paper, and to the CLTC's Chuck Kapelke, Matt Nagamine, and Rachel Wesen for their editorial, production, promotional, and moral support. Late breaking thanks to Christopher Kirchhoff and Benjamin Bahney for reading and commenting on the near final draft. Thanks to Steve Weber, Jesse Goldhammer (now at Deloitte, previously at Berkeley), and the group of public and private sector leaders who believed in this project and contributed early insights between 2016–2017. Finally, thanks to all of the individuals who took the time to be interviewed for this study or to read drafts. You were generous, thoughtful, and supportive. Any errors are the responsibility of the author alone.

There is a clear appetite for improving the public and private sector's ability to respond to complex contingencies in cyberspace. On the basis of the interviews and progress seen over the course of the last three years in particular, and the last decade more broadly, all indicators point toward the potential for progress—as long as leaders in the government and key companies commit to making change happen.

Jonathan Reiber
Senior Advisor, Technology for Global Security
Visiting Scholar, UC Berkeley Center for Long-Term Cybersecurity
November, 2019
Oakland, CA

Introduction: A Space of Our Own

The Internet was born on January 1, 1983, and from there it expanded from one to over four billion users in the fastest and most global technological change in history. If ever anyone believed that the Internet would create an online utopia devoid of conflict, however, that naïve aspiration has long since passed. Nation-state and non-state attackers steal, destroy, and manipulate data in cyberspace, a domain of conflict and cooperation like air, land, sea, and space. While war has yet to be formally declared through a cyberattack, adversaries flourish in a strange, hard-to-quantify gray area[9] below the level of outright conflict. Criminals, nation-states, and non-state groups often appear undeterred in pursuing their strategic objectives, from theft to media manipulation to disruptive attacks on critical infrastructure. With the Internet's rapid expansion, every part of connected civilization has become a potential target.

Unlike the operational domains of air, sea, land, and space, however, cyberspace is a man-made space of our own. The computer code we build is vulnerable, and the vulnerabilities in servers, data centers, and networks leave them open to hacking by malicious actors. Attack tactics range from the relatively simple to the complex. In a time-honored method, adversaries send phishing emails to unsuspecting victims with links on which individuals click; malicious software—"malware"—embedded in the link then burrows into an organization's networks, granting adversaries access to a treasure trove of data. At the higher end, governments may send covert operatives to physically implant malware through a thumb-drive onto a network, or even more exotic means.

Once inside, adversaries often dwell inside a data center for months, hunting around the interior until they find the high-value data they seek. Maybe they want to steal personnel data, as the Chinese did from the U.S. Office of Personnel Management.[10] Maybe they want to control the behavior of naval vessels by manipulating global positioning system data, as the Russians did in the Black Sea in 2017,[11] or shut off the networks and connections that power our infrastructure to stop a centrifuge from spinning in a nuclear weapons facility, as the Stuxnet attack achieved.[12] Or maybe they want to steal emails for a disinformation campaign to manipulate an election, as the Russians did to the United States in 2015–2016.[13]

So what is to be done to prevent attacks from succeeding? Solutions lie with both the government and the private sector—and often with the two communities working together to prevent a successful attack. While the two communities have made significant progress in improving the United States' approach to cybersecurity over the last decade—for example, by sharing information about threats and developing adaptive technologies for network defense—the major information technology companies and the U.S. government have not yet built the kind of trusting and operational partnerships that may be required to defend the United States and its interests in cyberspace during a period of escalating hostilities or war. Steps can be taken now to improve the United States' cybersecurity posture significantly by bringing the two communities together in a deliberate fashion to prepare for voluntary, combined cyberdefense operations to blunt incoming cyberattacks.

Why does this need to happen? Partly because the United States government cannot do everything on its own when it comes to cyberdefense. It is the responsibility of a government to conduct foreign policy, build a national response to deter foreign aggression, and, if necessary, use military options to defend a country's national interests, and the U.S. government has spent more than a decade developing the strategies and tools required for managing conflict in cyberspace. These include strategies for securing governmental networks,[14] supporting the private sector in securing its own networks, and planning to impose costs on potential adversaries that seek to penetrate American networks.[15] In response to cyberattacks, the U.S. government has indicted individual and state-affiliated hackers,[16] imposed economic sanctions to exact financial pain on a country or its businesses,[17] and conducted military cyberspace operations[18] to defeat a potential adversary's efforts to steal American data and influence American political perceptions. In the man-made domain of cyberspace, however, the U.S. government owns precious little of the technological infrastructure itself. Private companies own, build, and run most of the data, software, and infrastructure that underpin global telecommunications.

In the event of a cyberattack on the United States, given the diffuse nature of adversary command and control and the vulnerabilities of technology platforms, the U.S. government and the private sector can work together to defend the country as adversaries use a range of private infrastructure to conduct attacks. This could include the adversary's using an exploit to disrupt computer operations (as in the BIOS story), intruding into and dwelling inside servers and using them to steal or disrupt information (as China did in the case of Office of Personnel Management), or setting up fake accounts on an adversary platform to spread misinformation.

Companies can play a defensive role in each stage by patching vulnerabilities, quarantining infected servers, or denying adversaries access to services, but also by monitoring adversary behavior through early warning systems,[19] removing users from their platforms, or, for infrastructure companies, actively disrupting adversary access through temporary actions like Domain Name System (DNS) blocking,[20] Internet Protocol address blocking,[21] or Classless Inter-Domain Routing (CIDR) blocking.[22] The purpose of this paper is not to identify technical options; companies know their platforms and the infrastructure of the Internet, and defensive options should be discovered and analyzed within a public-private wargame scenario by technically savvy strategists and operators aware of their platforms and infrastructure.

Regardless of a company's capabilities, however, it is the purpose of the U.S. government and the U.S. military to defend the United States and its interests; information technology companies may be able to help the government achieve its national security missions in cyberspace and to prevent a conflict from escalating, but the U.S. government should never ask the private sector to put itself at risk if other instruments of U.S. government policy can achieve the same effect and do so without damaging the partner company. It is not in the American national interest for the U.S. government to ask a company to take a cyberdefense action that could damage the company unnecessarily. If an information technology company can contribute to U.S. national security by conducting a cyberdefense action without damaging its own economic interests and without escalating a conflict, however—and if those actions can prevent a potential loss of life or damage to U.S. national interests—such options can and should be discovered. **To set the conditions for that discovery is the purpose of this paper.**

Companies and the government independently conduct exercises to prepare for a range of cybersecurity incidents.[23] They do not, however, regularly work together to plan combined operations and technical options to limit an adversary's ability to operate in cyberspace during a conflict. Cyberthreats to the United States have increased in severity, and the time has come for corporate leaders and strategists in both sectors to imagine a high-end military conflict in the cyber age. If to date the majority of attacks against the United States have occurred in a "gray space" below the level of outright hostilities, what might a more hostile scenario look like?

As just one example, imagine a conflict scenario in which the People's Republic of China moves its naval vessels into the South China Sea and initiates kinetic military and cyberspace operations against the U.S. military and its allies. China, preparing to attack U.S. and allied

interests, uses American telecommunications networks, data, and servers to attack American interests by disrupting the banking and energy sectors, manipulating news media and demographic data, and disrupting commercial logistics support for the U.S. military.[24]

What might public-private cooperation look like to counter an incoming Chinese attack in such a scenario? At a basic level, it could include the U.S. military conducting cyberspace operations to blunt an adversary's command and control infrastructure by penetrating the adversary's servers and manipulating operational data. Through coordinated efforts, an information technology company (or companies) could then use their own infrastructure in a defensive manner, under their own terms of service, to cut off an adversary's access to their information technology products and services, therefore limiting the adversary's freedom of movement in cyberspace.

We have a recent historical precedent of exactly that. In advance of the 2018 U.S. Congressional Elections, Microsoft and Facebook removed hostile Russia-affiliated actors from their platforms to prevent influence operations or cyberattack on the electoral process.[25] Concurrently with Microsoft and Facebook's actions, U.S. Cyber Command disrupted the Russian Internet Research Agency's access to the Internet,[26] altering the Russians' command and control. The companies operated within their terms of service agreements and under their own authority. The government did the same. Together, they helped achieve a significant effect: defending the U.S. democratic process in advance of the 2018 election.

On the face of it, planning for such a scenario may not sound particularly complex. But the history of the U.S. government's relationship with the information technology sector, cultural differences between the national security community and the technology community, and market risks facing information technology companies partnering with the U.S. government complicate the proposition.

What are the issues at stake for the U.S. information technology community and the U.S. national security community in building operational trust and preparing for war in the cyberage, and what is the best way forward?

THE STATE OF THE RELATIONSHIP

The U.S. information technology sector and government face significant obstacles—in matters of trust and shared threat perceptions, in particular—that limit their ability to counter

advanced cyberthreats against the United States. While significant progress has been made in recent years to build a constructive relationship, the two communities have not created the partnerships required to develop and conduct effective combined cyberdefense operations in the event of escalation or outright conflict involving a near-peer adversary like China or Russia. To prepare in advance for a complex contingency demands that companies and the government deepen trust, build shared perceptions of the cyberthreat through exercises that address the indicators and behaviors accounting for significant hostilities, and develop options to deter and defeat cyberattacks on the United States. Such cooperation presents a logical next step in the development of a comprehensive U.S. cyberdefense strategy.

The most important ingredient is for key leaders in the government and the information technology sector to deepen trust between themselves and each other through regular strategic conversations and by participating in planning exercises. These ties will allow for leaders and organizations to develop bonds that can withstand periods of friction, and enable cooperation throughout diffuse organizations that do not always share the same set of interests.

Cooperation will occur, however, amidst a backdrop of prevailing popular mistrust of the government and private corporations for meeting society's needs. In its 2019 global Trust Barometer, the public affairs firm Edelman's indicated that only twenty percent of the population believes that "the system" is working for them, while half believe that the system is failing.[27] The Edelman report also indicates that populations want their business leaders to watch out for the public interest as well as profitability. Business leaders have an opportunity to take a leadership role in improving customer cybersecurity and national cybersecurity by navigating this terrain in a balanced way. While public trust can facilitate partnerships and opportunities for U.S. national security, it's not necessarily required for developing niche, classified technical options, as we shall explore. It is far more important that leaders foster a high degree of trust between themselves to make measured decisions about the conduct of war during a crisis.

The public and private sectors have worked well together on cybersecurity incidents at a number of points in recent history. At other points, mistakes have set the partnership back. This study explores four stories that offer lessons for the future of public-private partnership. They reveal some of the risks and opportunities that emerge when institutions with different values and interests try to cooperate. They also reveal important socio-political pressure points that will impact leaders and organizations as they analyze and make decisions about security challenges.

As the aphorism known as Miles' Law states, "where you stand is based on where you sit." Individuals and organizations have stories that they tell themselves about the world, and while some are more true and valid than others, they impact how we interpret the world and respond to the risks and opportunities we face. National security planners in Washington, D.C, and technologists based in California and across the United States often see the world and each other through the prism of different worldviews. With the exception of a few employees on a company's security team, most technology company employees do not wake up everyday thinking about terrorism, Vladimir Putin's global strategic goals, or the ways in which extremist organizations from the United States to the Middle East use technology to find targets and conduct violence. They are more likely to think about their daily job requirements in product development, marketing, or business strategy. Similarly, security planners in Washington think about deterrence, conflict, and long-term peace and stability, and think less about technology creation, marketing, or meeting their quarterly sales numbers.

How might these different perspectives impact the creation of an effective public-private partnership for cyberdefense? As one senior security leader at a major information technology company said in thinking about whether or not her company would support the U.S. government in countering a malicious cyberattack from abroad, "No one from [our company] will ever do this. If it were World War III, it would be different. But the engineers won't lead the way. They don't see the world in the same way."[28] You need to get the right people around the table to think about the issues.

This is not to suggest that technologists don't think about ethics and politics, or that government workers don't think about technology and marketing. Rather, technologists in the private sector do not feel the pressure of national security decision-making, and national security professionals do not feel the pressures of meeting shareholder or customer needs. Where you sit in a company or the national security community plays a large part in determining the institutional influences around you, your understanding of reality, and, ultimately, your policy decisions.

In 2016, a threat drew the communities closer together. In a history that is now well-known to many in the United States, on the express direction of Russian President Vladimir Putin, Russian military intelligence conducted cyberattacks on the networks of U.S. political organizations and political leaders and exploited social media business practices by purchasing ads to spread propaganda and foment mistrust within the American population.[29] The Russian operation hit

three parts of the American strategic "center of gravity"[30] during a period of acute political transition: the American population, the American political leadership, and key American technology companies. The attack undermined confidence in the democratic process, the country's leaders, and technology companies themselves. It was one of the most impactful cyberspace operations in history.[31]

The attack occurred concurrently with the election of Donald J. Trump as the American president. These two surprise events—a significant cyberattack on the democratic process, and the election of a populist candidate—destabilized America's political narrative and shocked parts of the American population. Questions plagued former members of President Barack Obama's administration in the years that followed—could they have taken action against the Russians sooner?[32] For social media and information technology companies, technologists questioned the impact of their creations on world affairs, as the tech sector itself experienced skyrocketing levels of public disenchantment and hostility. The events of 2015–2016 became a watershed moment in the world's understanding of the risks posed by cyberspace, an awareness that led to increased vigilance and cooperation regarding Russia's actions in advance of the 2018 U.S. Congressional Election.[33]

These events all occurred within the context of an expanding Internet and, with it, a commensurate expansion of cybersecurity risks to society from influence operations, domestic extremism, and cyberattacks on critical infrastructure.[34] The cyberthreat is now a top-tier challenge to international security and the problem seems unlikely to go away as technology expands and as more users come online across the globe.

The public and private sectors need to prepare for a future in which hostile actors use the internet and cyberspace in new and dangerous ways, from the spread of propaganda to autonomous weapons. Given the range of national security challenges facing the United States, the government and the technology sector should prepare for conflict scenarios in which the most cyber-capable adversaries—Russia, China, Iran, and North Korea—use kinetic military operations combined with cyberspace operations to achieve a strategic effect on American interests. Such a scenario may include military operations against U.S. forces in theater, as well as cyberattacks on American and allied assets in the U.S. homeland and/or abroad. The first purpose of an improved, cooperative partnership is thus for the U.S. government and the U.S. technology sector to better understand how future conflict might unfold and how technology and technology companies may be drawn in. The second purpose is to develop confidential (if not classified) strategic options to blunt and disrupt adversary cyberspace operations.

STRATEGIC CONTEXT: THREAT ENVIRONMENT AND ROLES AND MISSIONS

Before turning to the process of building partnerships for combined operations, we should first understand how the cyberthreat has evolved and become so dangerous. The following sections serve that purpose; they also outline roles and missions for cybersecurity for the general reader to understand the need for new partnerships.

In the last seven years alone, adversaries have conducted cyberspace operations for mass intellectual property theft, conducted destructive data attacks, and manipulated political and social perceptions through the media. Specific attacks on U.S. and allied national interests include China's ongoing campaign to steal U.S. intellectual property from U.S. organizations, including the theft of data for the construction of the U.S. military's Joint Strike Fighter (F-35);[35] Iran's 2012 cyberattack on the hard drives of the Saudi Arabian oil conglomerate, Saudi Aramco,[36] and its denial of service attacks on the U.S. financial sector in 2012-2013 that slowed banking traffic;[37] North Korea's theft of $81 million from the Bangladesh Central Bank and U.S. Federal Reserve in 2015;[38] China's penetration of the U.S. Office of Personnel Management (OPM) and the theft of 21.5 million federal personnel records;[39] Russia's disruptive cyberattacks on the Ukrainian electric grid in 2015 and 2016,[40] and its implantation of malware on parts of the U.S. electric grid over the course of 2014–2018.[41]

Nation-state actors like Russia, China, Iran, and North Korea present the greatest threat to U.S. interests in cyberspace. They have invested in the resources to put hackers on salary and can work diligently over time to penetrate a target. Often part of a country's intelligence community or military, nation-state hackers have benefits like retirement accounts and, most importantly, they have vested interests in their nation's success—incentives that make them into a powerful class of professional operators.

In recent years, countries have shifted their focus from data theft and destruction to data manipulation of political and media targets. Actors seek to alter how populations perceive political events and the nature of society writ large. The Russian hack of the 2016 U.S. presidential election is the most notable example, but other states have since taken similar, smaller-scale actions to mirror those of the Russians; China reportedly penetrated Cambodia's electoral networks in 2018, affording it the potential ability to manipulate Cambodia's election.[42] As the internet expands—particularly in Asia—the potential for manipulative attacks will increase.

Access to data has grown globally without a commensurate or popular understanding of the risks posed by cyberspace to human societies, whether from the vulnerabilities of computer code or the impact of social media enclaves on socio-political identity formation and discourse.[43] Networks, data centers, and cloud environments are insecure and vulnerable to breach. The world is consequently vulnerable to a range of attacks—from destructive hacks to influence operations to attack vectors we have not yet imagined.

Private Sector Roles and Missions

The world has not stood by flat-footed in the face of the cyberthreat. Corporations and government agencies have invested in organizations, teams, and technologies to secure data, deter adversaries, and, if necessary, respond to espionage and attacks. What are current roles and missions for the public and private sectors when it comes to cybersecurity?

The government cannot monitor and control all the private infrastructure within the United States; to try to do so outside of a state of national emergency would conflict with America's civil liberties and the values of freedom of expression enshrined in the U.S. Constitution.[44] Nor could the government do the job effectively given the immense scale and costs of such an endeavor. From telecommunications providers to social media companies to banks, private organizations are responsible for securing their own networks against intrusions and cyberattacks of any kind. They invest in the people, processes, and technology required for effective cybersecurity. Organizations can mitigate individual hackers, criminal organizations, and nation-state actors from causing significant damage if they invest in appropriate cybersecurity technologies.

Large technology companies and global corporations have a unique and important role to play in the cybersecurity story. Companies like Microsoft, Amazon, Apple, Google, Facebook, Akamai, and others provide technological tools and services for billions of individuals and millions of companies across the globe and they focus on securing their own platforms and services for their users first and foremost. Internet service providers and wireless providers secure their own networks and try to prevent the spread of malicious software.[45] In addition to technology companies, for purposes of national security, large critical infrastructure organizations in the energy, banking, health, electoral, and transportation sectors need to invest in cybersecurity given the critical roles that they place for society.[46] A lack of investment by the Singaporean health company SingHealth, for example, left the company's data centers

vulnerable to breach and allowed a hostile actor to move internally from server to server until they found the health records for 1.5 million Singaporeans, including the Prime Minister.[47] Similar attacks occurred on the U.S. Office of Personnel Management[48] and the American retail company Target. The private sector is therefore exposed if it fails to plan a range of cyberattacks on its infrastructure.

One of the most notable examples of private sector vulnerability comes from Russia's interference in the 2016 U.S. presidential election. The Russians found that they could use social media companies' business practices to buy ads and conduct cyber-enabled influence operations to manipulate the American population and influence the outcome of the election. In adding to buying ads on social media platforms, they concurrently ran a phishing campaign against a senior civilian political leader's Gmail account to steal his emails and also penetrated the servers of the Democratic National Committee, a political organization that is separate from the U.S. government. None of these organizations and individuals was prepared for cyberattacks or influence operations; the Russians carried out their missions for months, and the gravity of the threat did not become clear to the victims or to the U.S. government until it was too late. [49]

U.S. government cybersecurity roles and missions

Over the last decade the U.S. government has evolved its roles and missions for cybersecurity. The Department of Homeland Security (DHS) takes the lead for domestic incident response and coordination with the private sector.[50] The Federal Bureau of Investigation (FBI) is responsible for domestic criminal investigations and domestic cyberspace operations. The Department of Defense is responsible for defending its own networks, for deterring and defeating foreign attacks on the United States, and for providing cyberspace operational support to military forces in theater. The FBI and Central Intelligence Agency work closely with the Department of Defense to counter incoming attacks from abroad. The National Security Agency serves as the nation's premier intelligence organization responsible for signals intelligence on key foreign targets, surveillance, and cybersecurity intelligence. It provides cybersecurity technical assistance to agencies across the U.S. government if requested. The White House leads the development of national policy and plays a coordinating role for incident response when attacks involve nation-state actors and carry significant foreign policy and national security implications that require multiple agencies of the government to respond.

In the event of escalating cyberattacks, the United States has chosen largely non-military tactics in response to date. The United States has declared that it will respond in a time, manner, and place of its choosing to cyberattacks[51] just as in other domains, and policy choices have been made on a case-by-case basis for the actor and intrusion in question. In response to intrusions, the U.S. government has indicted Chinese military operatives for intellectual property theft,[52] indicted Iranian government cyberspace operators for attacking the financial sector,[53] sanctioned the Russian government for its election intrusions and intrusions onto the electric grid, and sanctioned North Korea for its attack on Sony Pictures Entertainment. In 2018, in advance of the U.S. Congressional Elections, following the release of the Defense Department Cyber Strategy in October of 2019, U.S. Cyber Command took its first counter-offense action to "stop a threat before it hits its target" by disrupting the Russian Internet Research Agency's access. There may come a time when the U.S. government could also use military force in response to a cyberattack, as when Israel conducted a missile strike on Hamas's cyberspace operational wing in May of 2019.[54]

CURRENT PUBLIC-PRIVATE CYBERSECURITY COOPERATION

What cooperative activities currently exist between the public and private sectors? Current activities include (1) steady-state, peacetime operations, like sharing information about threats and best practices; and (2) "incident response" operations that require companies and the government to work together in response to a cyberattack below the level of outright conflict.

Steady-state, peacetime public-private cooperation involves a wide array of cybersecurity activities. The public and private sectors regularly share threat information through formal mechanisms like the Financial Services Information Sharing and Analysis Center,[55] which shares threat information among companies and organizations in the financial sector and the U.S. government regarding threats to the financial sector. Similar information sharing and analysis centers exist in other sectors, like electricity or transportation. Sharing information about threats and methods of attack helps financial companies and the government to secure their networks against known risks, and the maturity in the financial sector has set a standard for public-private information sharing.

The **Enduring Security Framework** is an important steady-state, U.S. government-convened cooperative forum. In Enduring Security Framework meetings, which occur multiple times each year at the executive level and include regular working group collaborations, participants are

given security clearances to receive briefings from the intelligence community about advanced cybersecurity threats to the nation and to discuss mitigation mechanisms. (It was through the Enduring Security Framework that the information technology community and the national security community worked together on the BIOS mitigation, which we will review in-depth.)

Another steady-state public-private forum is **the vulnerabilities equity process**, or VEP, which is led by the White House and brings the government and the private sector together to discuss vulnerabilities that the U.S. government has discovered in technology platforms, If government agencies discover a vulnerability, they decide whether and how the U.S. government has an intelligence or operational need for the vulnerability (for example, to gain intelligence on a high-value target or to prepare to disrupt aspects of a country's infrastructure for defensive purposes). The overarching objective of the VEP is to close vulnerabilities for the public good, assuming there is not a strong U.S. governmental operational need.[56] The government engages major technology companies including Microsoft, Apple, and Amazon, about its findings. When it comes to the trade-offs that the VEP considers, as then-White House Cybersecurity Coordinator Michael Daniel outlined in 2014, the principles of the U.S. government are to disclose as much as possible: "Building up a huge stockpile of undisclosed vulnerabilities while leaving the Internet vulnerable and the American people unprotected would not be in our national security interest," Daniel wrote in 2014.[57]

The public and private sectors also work together on **regulatory projects**. These include the 2012 National Institute for Standards and Technology Cybersecurity Framework that outlines industry and government-vetted best practices for cybersecurity,[58] and on cybersecurity legislation within the states and federal legislature, like the Cybersecurity Information Sharing Act of 2014,[59] to improve the country's cybersecurity and information-sharing processes between entities. Cooperation in these activities involves sharing lessons and gaining agreement on cybersecurity principles and frameworks, and has led to a steady increase in information sharing about threats and defensive practices and an elevation of cybersecurity awareness globally.

One way to measure this increased awareness is by examining public- and private-sector **spending for cybersecurity**. In late 2018, the market analysis firm Gartner reported that "worldwide spending on information security products and services [reached more than] $114 billion in 2018, an increase of 12.4 percent from [2017] . . . In 2019, the market is forecast to grow 8.7 percent to $124 billion."[60] One of the largest cybersecurity investments came from the U.S. Defense Department, which allocated $1.8 billion to fund the Cyber Mission Force, or CMF, over fiscal years 2014–2018.[61]

To date, the U.S. government and the private sector have not developed a robust, formal method for planning combined counter-offense operations. What if companies and the government are called to cooperate in such a combined manner again, but in a more complex scenario? What if a foreign government plans to disrupt aspects of U.S. critical infrastructure to achieve a strategic effect against U.S. forces or economic interests during a conflict in the South China Sea involving the People's Republic of China? Have companies considered how their technologies could be used to achieve positive cybersecurity results in such a scenario? What complications might arise for a major information technology company, and how can companies and the government work together to get ahead of the issues?

Before conflict unfolds, the U.S. government and U.S. information technology companies can work together to develop insights into hostile actors' behaviors and prepare options to monitor and terminate a potential adversary's use of cyberspace before they can attack U.S. interests. This is true for countering influence operations but also for disruptive attacks on infrastructure that could impact public safety.

The Removal of Obstacles

How can the public and private sectors work together in advance to prepare?

The first step is to identity obstacles to effective cooperation and to determine ways to either remove or resolve them. These obstacles (and others that participants might identity) should be addressed before the government and private sector can build strategic defensive options together.

1. **A shared sense of trust.** The two communities operate in different environments—as public institutions upholding the Constitution and serving the public good, and as private institutions developing goods and services for the market, employing personnel, and meeting shareholder expectations. Given the different aims and interests of the two sectors, bonds of trust can only develop through regular information sharing and cooperation, cultivated over time.

2. **A shared perception of the threat.** If the parties do not see the world the same way, they will not be able to act in a unified, coordinated manner. Do the relevant constituencies share a perception of the threat in a way that can drive them toward cooperation or clear analytical decision-making? If not, how can threat perceptions be changed?

3. **A common understanding of the potential market impacts of cyberdefense action or inaction.** Before working with the U.S. government on any combined operation, companies will want to conduct a thorough cost-benefit analysis to imagine potential impacts on their global bottom line—including their existing customer base, future potential markets, and the potential loss of any technological capabilities. As one executive at a major American telecommunications servicer provider said, "We're part of the global community as well. We want to be patriotic but we are global operators."[62] Global concerns impacted every multinational technology leader interviewed for this study.

We will treat each of the above issues in turn.

THE NATURE OF TRUST

In building a combined operational partnership to help secure the United States against major cyberattacks, leaders and operators in the two communities need to be able to trust each other during planning discussions and security operations. Cooperating on a cyber threat or cyber incident requires that companies and the government trust, *inter alia*, the forensics and attribution of the threat and the threat actor; that shared information will be protected and held confidential; that each partner will deliver on their operational and other promises (i.e., that they will follow the protocols of policy process, that they will consult one another at appropriate times and consider each other's interests, and that they will coordinate on important policy documents like public affairs statements); and that, beyond senior leaders, line officers in each institution will work to meet the intentions of their leaders. If trust is non-existent or broken between leaders and institutions, operational planning becomes far harder, if not impossible to achieve, to the detriment of everyone, including the American people and others that could be impacted by a disruptive cyberspace operation.

What does trust mean in the context of public-private operations? Trust is the assumption that entities you do not control will act in an expected manner that is favorable to your cause.[63] Leaders need to trust each other to plan operations, yet by trusting someone with sensitive information that could impact your organization's well-being, trust increases the risk that people will let you down or betray you, and therefore exposes the truster to vulnerability. This, too, will factor into a company's cost-benefit analysis for partnering with the government. History shows how a breach of trust can impact cooperation, as one of our stories shows.

FOUR HISTORICAL STORIES OF PARTNERSHIP AND TRUST

The below four stories from the last decade show how issues of trust, threat perception, and potential market impact factor into the equation.[64]

The Basic Input Output System (BIOS) Mitigation. In 2010–2011, the U.S. intelligence community learned that China had discovered a vulnerability in the code of the Basic Input-Output System (BIOS) of computers.[65] The BIOS is a type of firmware that facilitates start-up and the computer's operations. Under the rubric of the Enduring Security Framework (ESF), a public-private organization of leading IT companies and national security organizations in the U.S. government, the intelligence community briefed information technology companies

about the BIOS threat and companies made the decision to patch computers across the United States at scale.

The Edward J. Snowden Intelligence Disclosures. In 2013, Booz Allen Hamilton contractor Edward J. Snowden stole information from the National Security Agency regarding its intelligence collection programs, including, among other things, the NSA's bulk metadata program, which collected information about American citizens and their contact with foreigners. The Snowden disclosures revealed how the American government requested information from leading technology companies for national security purposes, and also how the government gained access to private-sector infrastructure, including that of Google, without the company's permission.[66] The Snowden disclosures triggered pre-existing feelings of mistrust among companies, the public, foreign countries, and the U.S. government regarding the government's role in surveillance and breaches of privacy, and led to a range of policy changes within the executive branch regarding the governance of U.S. intelligence activities.[67]

The Defense Contracts. Two recent technology company defense contract cases reveal how companies have struggled to partner with the U.S. government on security issues given issues of corporate culture and threat perception.

First, in 2018, Google decided to cancel its participation in Project Maven, a Defense Department effort to develop artificial intelligence systems that could help identify potential threats through analysis of military video feeds. When Google employees discovered the contract, a subset of employees signed a dissenting petition and protested that Google should withdraw from it on the grounds that Google as a company should not participate in the development of any weapons programs.[68] Google then drew up a list of ethical principles for its artificial intelligence programs, including a statement that its artificial intelligence programs would not be intended to cause harm or contribute to weapons programs.[69] The episode led the sitting Chairman of the Joint Chiefs of Staff to question the patriotism of Google and accuse it of being willing to help the Chinese government but not the U.S. government.[70] According to a leaked internal memo within the Pentagon, officials within the Defense Department recognized that they had suffered a loss when Google employees protested and Google withdrew from the contract. "We will not compete effectively against our adversaries if we do not win the 'hearts and minds' of the key supporters," the memo read.[71]

In another case, employees at Microsoft voiced dissent over a contract through which Microsoft would provide a virtual augmented reality capability to the U.S. Army. Microsoft CEO Satya Nadella overruled the employees' protest, saying, "We made a principled decision that

we're not going to withhold technology from institutions that we have elected in democracies to protect the freedoms we enjoy."[72] Microsoft President Brad Smith provided further detail, saying "we believe that the people who defend our country need and deserve our support." He continued, "to withdraw from this market is to reduce our opportunity to engage in the public debate about how new technologies can best be used in a responsible way. We are not going to withdraw from the future. In the most positive way possible, we are going to work to help shape it."[73] The two companies have different cultures and different views of their responsibilities. The story shows how views of government and security threats can impact companies' cultures and pressure corporate leaders.

Combined Operations in the 2018 U.S. Congressional Elections. The fourth story is of the U.S. government and the private sector's response to Russia's operations during the 2018 U.S. Congressional Election. It illustrates how the public and private sector can coordinate their actions in advance of an impending attack. Following Russia's influence operation and cyberattacks during 2016 U.S. presidential election, the U.S. government worked together with companies throughout 2017–2018 to counteract influence operations on the United States. As we have discussed, in 2018, Microsoft, Facebook and others removed Russian operatives that were using their social media platforms for malicious purposes.

Separately, after months of planning, U.S. Cyber Command conducted a counter-offense operation against the Russian Internet Research Agency to remove the Russian organization's access to the Internet and prevent it from conducting operations during the election. These actions were taken by each organization under its own authority as a public or private entity; the manner in which they planned together points toward an effective, combined approach for cyberdefense cooperation.

THE IMPACT OF TRUST ON OPERATIONS

These stories surface at least four salient layers of trust that could play into future public-private cybersecurity cooperation: (1) trust between a company and the government; (2) trust between divisions or employee groups within a company itself; (3) trust between the company and its shareholders and customers; and (4) trust between the government and the public. To varying degrees, each could impact how corporate and government leaders will think about building cyberdefense cooperation and make decisions in preparation for potential conflicts that have not yet materialized.

Trust between a company and the government. Perhaps most important for operational planning, trust between a company and the government includes trust between key leaders that share a perspective and responsibility for risk management, such as IT company CEOs and Cabinet secretaries. These relationships are the most important for identifying threats, sharing perspectives, and agreeing on strategic options for cyberdefense. In the classified Enduring Security Framework deliberations over the nation-state threat to the BIOS, for example, company executives and key government leaders could share views about specific nation-state actors. There is much that can be achieved through regular, classified information sharing and partnership building.

Trust between divisions or employee groups within the company. In making decisions regarding war and peace, technology, and violence, issues of trust may arise between employees that work for a company, American and non-American, and the executives that make policy decisions for the company. The case of Google cancelling its AI contract with the Defense Department[74] and Microsoft CEO Satya Nadella sustaining an Army contract show how executive perspectives and decisions matter. The government should keep corporate culture in mind as it plans for digital threats and tries to work with companies on an increasing array of technological challenges and opportunities.

Trust between the company and its customers, shareholders, and the public. In addition to the nature of its action, a company's public affairs posture helps a company sustain trust with its shareholders and its customers and the public. How the company explains its internal actions or interactions with the government is vital to the company's ability to operate and sustain its market trust and market standing.

Trust between the government and the public. The public's trust and support of the government can strengthen or hinder the government's ability to operate. How is the government perceived to be acting in the nation's interests, including for protecting individual users' data and interests? Success depends in part on the government's ability to build and sustain legitimacy for an operation; companies and the public need to understand how the operation would meet their interests and that of the country as a whole.

There is a tremendous amount of research dating back to the Civil War for how the U.S. government builds support within the American population for prosecuting a conflict.[75] Factors of support include the population's perception of the adversary (including the behavior of the regime and its military power), the opinions of the elites that shape society's thinking,

and individuals' perceptions of their own lives, among others. During a period of escalating tensions, the U.S. government may have an easier time building support for a cyberspace operation against a country that has long-standing hostile relations with the United States, like North Korea, Iran, Russia, or Syria for example. Their governments have isolated themselves through invasion, terrorism, and civil war. North Korea, Iran, and Russia have all also used cyberspace operations against the United States. If tensions escalated, the U.S. government would have significant history to build a case for a cyberdefense operation.

After the effects of Russian interference in 2016, for example, the American public may have been more inclined to support companies and the government in taking action to defend U.S. democratic processes and institutions. In advance of the 2018 election, the U.S government conducted a counter-offense operation against the Russian Internet Research Agency, but the operation occurred within a broader, public narrative and public concerns regarding Russian cyberspace operations against the U.S. election.

If tensions escalated with China, however, and China began to take more hostile actions in cyberspace, the case might be more complicated for an information technology company. As one former senior White House official said on this topic, "Russia is an easy case. China is a whole different matter—and far more complicated given its economic role."[76] China is one of most important markets for many multinational information technology companies operating today. For a company to begin advanced planning with the U.S. government today in anticipation of a potential Chinese cyberattack would place a greater demand on the U.S. government to make its case. We will explore this issue in greater detail when we turn to analytic ingredients for scenario planning and exercises.

TRUST AND GOVERNMENT SUPPORT IN THE FOUR STORIES

How did questions of trust and threat perception play out in the four historical stories highlighted above, and what lessons can be drawn from those stories for the future?

The BIOS Mitigation fostered a significant level of trust between key leaders in the public and private sector, thanks to a shared perception of the threat and the relatively simple defensive action required to mitigate it; the operation was essentially a scaled network defense action to close (or "patch") a vulnerability in the computer code across hundreds of thousands of computers. This is a far less complicated operation than if the government asked a technology

company to shut off parts of its own technological infrastructure to isolate or degrade an adversary's ability to operate online. In the BIOS story, the national security community and the private sector had a shared view of the threat, and China's access to the BIOS exploit and the scale of the vulnerability made the threat acute.

Responsibilities were also clear. While the government could have conducted a cyberspace operation action against the Chinese government's networks to deny access, that would have been an overly aggressive and disproportionate action. While China had been stealing intellectual property from the United States for years, the two countries were not in a state of hostilities to necessitate an escalation at that time. Secondly, the U.S. government was not in a position to close the vulnerability itself; the onus was on the private sector to do so, as the private sector built and managed the vulnerable computers. Finally, "trust" hinged mostly around the private sector's trust in the intelligence community's findings about the threat. The companies operated on their own to close the threat; they did not touch any adversary infrastructure, only their own. The decision was made in a closed, classified environment with the support of the companies and government agencies involved and only later revealed to the public.[77]

Edward Snowden's intelligence disclosures of 2013 is the most well known of the four stories. It led to the most dramatic breaks in trust. Why? While significant components of the NSA's intelligence collection activities were undertaken legally through court-ordered requests, others occurred without the knowledge of the technology companies; in other instances, as in the case of the U.S. government collecting signals intelligence on its allies (including the German Chancellor Angela Merkel's cell phone)[78] and the nature of the metadata collected, the intelligence disclosures revealed an unbridled approach to signals intelligence. The disclosures frayed trust between the government and the technology sector, between the U.S. government and the global public, between employees who were unaware that their employer was cooperating with the government, and between the technology sector and the public.[79] The disclosures downgraded the government's ability to build relationships with parts of the technology community for a range of activities. The event led to necessary reforms (some of which are still ongoing), but relationships were frayed and time was wasted.[80]

Company and government actions in advance of **the 2018 U.S. Congressional Elections** point towards the benefit of shared threat perceptions and the future of public-private cooperation. Since its attack on the 2016 U.S. presidential election, Russia has proven itself a dangerous threat to U.S. interests. Following a range of investigations within technology companies, by

Congress, and through the media, American society was keenly aware of the threat to future elections. Contact between technology companies and the federal government in advance of the 2018 Congressional election led to an increase in familiarity between the civil servants responsible for cybersecurity and their counterparts in the technology sector.[81] In advance of the election, Microsoft[82] and Facebook[83] removed Russian actors from their platform under their own authority; U.S. Cyber Command conducted an operation against the Russian Internet Research Agency under its own authorities.[84]

The actions by the companies in advance of the election portrayed a level of seriousness and commitment to counter the threat. The operations occurred within a media narrative of American anxiety over Russian interference, and met with support from experts in the community and the public at large. U.S. Cyber Command's operation may also have bolstered perceptions that the U.S. military takes the problem seriously and built legitimacy for future operations.

The **defense contract** narrative shows how employees in the technology sector may resist any cooperation with the government on matters of national security, including cyberdefense, and points towards the need for deeper understanding and conversation between the two communities on matters of violence, the use of force, and the role of technology in world affairs.

History shows that if a weapon can be invented, it will be invented, whether that technology is the nuclear bomb, a biopathogen, a strain of destructive malware, or a strong AI that can provide a government with a competitive advantage in matters of war. Scientists throughout history have lent their analytic support to governments during times of war to create technologies for purposes of military operations, the creation of the nuclear bomb being the most dramatic and well-known example.

For an individual scientist, the decision to work on a security technology will be deeply personal and reflect her or his ethical and political views on the use of force, politics, and international relations. Considerations may include whether they trust the institutions for which the weapon has been produced to be judicious in its use, how the technology could be used maliciously, and whether the proliferation of the weapon can be controlled.

Yet the nature of the adversary or potential adversaries is paramount. In the case of the nuclear bomb, for example, the dangers of the Nazi regime and of the emerging Soviet power helped drive scientists like Albert Einstein and Robert Oppenheimer to contribute their knowledge.

The scientists determined that it would have been far more dangerous for the Nazis to develop the bomb before the Allies in World War II, and opted to give their support to the Manhattan Project.[85]

In a democracy, particularly in a democracy in a political condition outside of a state of total war like World War II, it is the prerogative of a commercial company to decide what technologies it will or will not produce, and it is the right of a scientist to opt out of a project if they prefer not to work on technologies designed for military purposes. In the case of Project Maven, Google's deeply engrained cultural ethos of "don't be evil" led a number of employees to withhold their support for intentionally developing technologies for use in what they perceived to be a weapons platform.[86] Microsoft, on the other hand, chose "not to withhold" technologies from the institutions that support the United States' democratic freedoms.

From the outside it is difficult to assess how and why a single leader made one choice over another. Company employees in both cases opposed the contract. The Google employees were organized and forceful in their opposition, as a long investigative report in *WIRED* magazine revealed,[87] and that opposition helped drive Google to draft its specific principles for artificial intelligence. Microsoft made a "principled decision" to support the government and try to shape outcomes as best it can.

These two cases involved the intentional *creation* of new technologies for purposes of supporting the military. What about when technologies created for a civil purpose are weaponized for malicious ends? In such instances, companies and the government try to limit the negative effects of that technology, either by altering the technology itself (i.e., sending out a patch, as in the BIOS example), penalizing through non-military means those that use it in an illegal manner (i.e., sanctions and indictments) or disrupting the adversary's use of it through military means (i.e., as U.S. Cyber Command disrupting the Russian Internet Research Agency). Like the internet, radio in and of itself is not an evil tool, yet the Hutus operating during the Rwandan genocide of 1994 turned the radio into a tool for fomenting hate and inspiring violence against the minority Tutsi population in Rwanda.[88] Every student of history looks back and wishes that someone had shut off the Hutus' radio platform, Radio Télévision Libre des Mille Collines, through a missile or jammer to prevent the spread of the violent ideology.[89]

A range of actors—from violent extremists to the U.S. government intelligence services—use Google Search to research their targets, yet Google Search was not created with those purposes in mind. Similarly, social media companies were created to connect people, yet

they became enclaves that facilitated the spread of disinformation and enabled the Russian intelligence services to spread propaganda within the American population. The internet was first created as a tool for connecting scientists, yet the vulnerabilities within it now allow for a range of negative uses. Attackers find exploits to disrupt elements of critical infrastructure, as Iran did to Saudi Aramco or the Russians did to the Ukrainian electric grid. When a technology reveals its danger, someone needs to make the case for that technology to be changed. Sometimes, someone needs to make the case for shutting it off or disrupting it.

Given a cultural difference like that between elements of Google and the U.S. government on the use of artificial intelligence, how would the U.S. government make its case to win over Google or another company's support for a cybersecurity operation to disrupt hostile activity in the event of escalating tensions with an adversary—particularly if the adversary isn't attacking the United States *today*, and it takes time to develop effective cyberdefense options?

Part of the answer rests in sharing stories and perceptions. As one technology company executive said during the course of the interview process, some corporations would only take part in a cyberdefense planning process if "World War III" were underway. Historically, Einstein and Oppenheimer felt compelled to join the nuclear effort because the threat was clear and present. Today in cyberspace operations (and artificial intelligence), we know that advanced attackers will use digital tools against U.S. interests in the future. We will certainly know World War III when we're in it, but in advance, nations are investing in dangerous technology behind closed doors, and the United States still needs the best and brightest scientists to support the national security community to plan in advance.

Would a more aggressive and hostile threat drive Google scientists and engineers to change their view of cooperating with the United States on artificial intelligence, just as Einstein and Oppenheimer did in the 1930s and 1940s in the face of Nazi aggression? Perhaps, but the path towards conflict can be hard to perceive. The unfortunate truth, as Benjamin Franklin is reported to have said, is that "by failing to prepare, you are preparing to fail." In the technological age in the United States, the act of preparation presents an acute and vexing problem. The private sector owns and operates the terrain of cyberspace, and adversaries have seized on that opportunity; they recognize that they can technologically exploit private infrastructure and, perhaps more importantly, they can exploit the wide chasm that exists between the U.S. technology community and the U.S. government on matters of peace and war. The state of the world can change quickly. If companies and the government do not work together to prepare strategically and technologically, they will be flat-footed when real conflict comes.

Recommendations: Change Worldviews, Shape Policy, Build Defense Options

Culturally, how an organization's leadership perceives risk often informs how the organization will plan for risk. The manner through which a leadership team imagines the potential of cyberattacks occurring will inform how the organization understands and responds to incidents. Aspects of the four historical stories cited show how threat perception can affect public-private partnership. In the BIOS mitigation, for example, the public and private sectors shared threat perceptions through classified briefings and identified means to take action. Russia's operations in 2015–2016—and the lack of cybersecurity preparation by campaigns and social media companies—spurred an increase in public-private cybersecurity cooperation in advance of the 2018 U.S. Congressional Elections. The 2016 attack made clear the threat and drove companies and the government to work together.

Interviews for this study reveal that a sub-set of the private and public sectors already understand the threat and want to prepare for potential hostilities. Multiple technology leaders indicated that they would like to meet regularly to plan operations to prevent a hostile actor from conducting an aggressive attack. One went so far as to say in December 2018 that, "I expect that they would want to do exactly this kind of work," and wondered why his company hadn't been called and why formal government organizations had not initiated deliberate planning previously.[90] Public- and private-sector personnel with a background or exposure to the workings of government, strategic planning, or the military were particularly supportive. They provide a foundation for effective planning.

Other director-level leaders expressed support but found opposition within their broader corporations. After a daylong briefing on the issue and multiple conversations, one technology leader edited a draft proposal, began to think about budgeting options to work on it, and briefed the program into her organization, advocating that her company embark on a process of deliberate planning. In a separate component of the company, however, she encountered resistance—and that ended the conversation for that moment.[91] Government personnel in the

White House National Security Council, U.S. Cyber Command, National Security Agency, and the Office of the Secretary of Defense all expressed support for the concept of building robust partnerships[92]—but given the demands of their jobs, they seemed to lack the time to build the necessary relationships of trust that would lead to the development of tactical, strategic options for specific operations.[93] The most important step may therefore be for a governmental staff member to have public-private operational planning as a part- or full-time responsibility.

IMAGINE UNTHINKABLE SCENARIOS

Practically, then, how can the public and private sector deepen their understanding of hostile actors and potential risks in cyberspace? One way is by conducting regular exercises for a range of attack scenarios. Small, pre-planned scenario exercises should bring representatives from public- and private-sector organizations together to develop and conduct exercises and discover viable options to blunt incoming cyberattacks, including influence operations and destructive attacks on infrastructure. The U.S. Defense Department and the intelligence community are planning organizations; they think about future risks, build strategies, and exercise to prepare for them. Technology employees focus their strategic thinking on competitors, changes in the market, or technology-focused product innovation. Security-focused exercises can help company executives and government partners to think about security issues together.

So what should they consider? Scenarios should focus on surfacing issues of market, customer, technological, and security risks of action or inaction for the participating technology companies. If the U.S. government has indications and warning that China will conduct a destructive cyberattack on American interests, for example, and the government asks an American company to limit or shut off China's access to their infrastructure, any perceived cooperation with the U.S. government could impact a company's market access. As one senior security leader at a major information technology said in 2018, if the U.S. asked a company to take a counter-offense action against another country, "There will be escalating impacts. Ultimately you're asking a multinational corporation with global business footprint to pick winners, and that's clearly not in the long-term best interest of our business."[94] He also pointed out that many IT companies need to "comply with any court order from a jurisdiction," and if they have two competing orders from two countries, they are essentially required to pick a market. Companies need to consider how a cyberdefense option could impact their business.

A clear risk of a cyberdefense action could be unintended or disproportionate effects on the target population. As the chief security officer at an internet infrastructure provider said, "The only thing I'd recommend in the infrastructure itself, if you have their address space, you tell all the carriers (internet service providers, telecommunications carriers, others) that they are not allowed to provide reachability. You are not allowed to send or deliver anything to or from [that country]. You don't want to do it in the routing system, but if you do it on a geographic basis, there's nothing over there we want content wise, it would work. But, "it would break citizen access."[95] Cyberdefense options could carry negative impacts for a nation's citizens and any option would need to be measured from within the Law of Armed Conflict. Like sanctions that prevent goods from flowing into a country, a loss of internet or technology services could spur citizens to pressure their government to change—or it could carry unacceptable consequences for civilian infrastructure.

Narrative-focused scenario exercises can also help surface indicators of a conflict unfolding over time[96] and walk participants through the steps that an adversary might take as events unfold.[97] A senior leader from a major telecommunications provider believes that this is the right course for the U.S. government and companies to pursue. "We can block things at our peering points if we want to," he said. The question is, "What is it going to look like? What technical capabilities would it look like if we stop it? What unintended consequences would we face?"[98] The only way to get ahead of the problem is to think it through.

One senior leader outlined how he would think about a national security situation in which his company was asked to block traffic to assist the U.S. government. "We have worked on [fewer than ten] cases on particular takedowns and threats. We're not the only company that does that. I cannot get into the cases."[99] But he outlined the steps that he considers. "This is how we work our way through in these cases. Is it legal? Is it legit? How will this play when it hits the headline that Ellen Nakashima [of *The Washington Post*] writes about it? How is the world going to react to that? How will the customer base react to it? Were there any privacy concerns? All those things need to be considered, to ensure that it's legit, it's lawful, and we're not going to suffer."

When asked how his company considered such actions, he said, "It takes a lot of planning and effort. For what you're thinking, I assume it would be a matter of some urgency, the linkages would need to be put in place so that you can assess the legal risks, asses the consequences. We need to build the confidence that what you're saying is timely and serious. It's not just 'let's go after the criminal.'" His process reflected that of other technology leaders; if "World

War III" was upon us, it would trigger a willigness to take action. As one software company cybersecurity strategist said, "We need to think about that. I don't want to. No one wants to. But we need to think about it."[100]

Many leaders immediately recognized the need for lawyers to be present for the discussion. "We'd want lawyers to be there to talk about how we've done them in the past and we'd obviously want to run it by the legal team about how we do this kind of stuff," one senior leader said. But would his company be willing explore this kind of planning now if the government called? "We would be in favor of doing that."[101]

In addition to scenarios narratives, large technology companies should adopt the process of **thinking like an adversary** and **regularly red-team their business operations for vulnerabilities**. To "red-team" your operations means thinking about the platform from an adversary's perspective by considering the adversary's political and social goals and objectives and how they may seek to exploit a platform for their own purposes. For example, in advance of the 2016 election, if Facebook had taken on an adversary mindset, it perhaps could have surfaced how adversaries like Russia would purchase political ads online to manipulate the election, or how a company like Cambridge Analytica could have acquired, stored, and used private user data from a third-party for election-related data analysis that breached Facebook's privacy rules.[102]

Large multinational IT companies need to make regular scenario and red-team planning a priority to look across platforms and business practices. Companies can work internally to draft escalatory scenarios in which the government calls and asks them to take action to shut off infrastructure, redirect traffic, or use their analytical platforms to anticipate and blunt an incoming attack. Exercises and scenarios get everyone ready for surprises. If companies can build bonds of trust and work together internally to imagine the unthinkable, senior leaders, middle managers, and engineers will be better prepared to deal with whatever comes.

THE CASE OF CHINA

Of all of the potential adversaries and cyberdefense contingencies that could come to pass, the act of planning in advance for a future conflict with China would carry the greatest amount of risk due to China's market size,[103] military forces and military objectives,[104] dynamic economy, and high levels of global influence. China therefore provides an appropriate test case for our

problem. As one senior leader at a major telecommunications company said, "There is a big concern about China and what to do about it. The government is concerned that the Chinese are taking over the world." How would planning for a China conflict present a risk to American information technology companies, and what can companies do to mitigate those risks?

China is the world's second largest economy—the largest if measured by purchasing power parity[105]—and for a U.S. information technology company seeking to do business in China, any perception that the company plans with the U.S. government for a potential cyberdefense operation could trigger a response from the Chinese government, potentially leading to charges of complicity that would mirror claims made by the United States government against Huawei operating within the United States.[106] China has long suspected American private companies, and has banned many major American IT and media companies from operating on the Chinese mainland, incluing Google, Facebook, Instagram, SoundCloud, and *The New York Times*.[107] Speaking at a 2018 trilateral dialogue with Chinese, Indian, and American delegates, a Chinese academic referred to Facebook, Twitter, LinkedIn, and other American information technology companies as components of the United States' "aggressive internet freedom agenda."[108]

STATEMENT OF CYBERDEFENSE POLICY

The first task facing an American information technology company in planning for cyberspace conflict with a nation-state is to develop a clear statement of policy regarding defensive operations and an accompanying public affairs strategy. Companies can make it a matter of public policy to block any hostile actor from using the company's platform for malicious purposes. Clearly delineated terms of service can clarify the company's position for shareholders, the public, foreign countries, and the U.S. government.

Some corporations have already set clear cyberdefense policies. In 2017, for example, the president of Microsoft, Brad Smith, said technology companies must be committed to "100% defense and zero percent offense." In setting a defensive policy, companies could argue that any time a nation-state tries to use its infrastructure for malicious purposes, they will remove the hostile actor's access to that infrastructure.[109]

Microsoft took action along those lines in 2017 and 2018. In 2017, the company found that unnanmed hostile actors associated with an unnamed nation had "registered internet domains

using names that included Microsoft and other companies' trademarks."[110] Microsoft obtained a court order and sought the appointment of a Special Master to oversee and expedite motions in the case. With a court order in place, Microsoft then notified internet registries whenever the group registered a fake Microsoft domain and requested that control of that domain be transferred to a sinkhole—a domain name system (DNS) server that gives out false information to prevent the use of another domain name—operated by Microsoft's Digital Crimes Unit. With that sinkhole in place, Microsoft could then disrupt the nation state's use of the domains within 24 hours to prevent hostile action. The company pursued a similar course of action in 2018 through its Digital Crimes Unit to prevent hostile actors from interfering in the 2018 U.S. Congressional Elections.[111]

How would a clear statement of policy play out in a contingency between the United States and China? If a company decides to begin public-private contingency planning for a potential conflict with China, the same "100% defense" policy could form the basis of a public affairs strategy; a company could argue that it will block any malicious traffic that falls outside of a company's terms of service. A company should treat any counter-offense operation on a case-by-case basis, but statements of policy can give the company a public affairs position with regards to potentially aggressive countries.

KEY QUESTIONS TO CONSIDER

What are some other questions for companies to consider as they plan for potential cyberdefense cooperation with the United States?

1. **Risks to foreign national personnel within a company.** If it were ever disclosed that a company was planning for a contingency with China, it could trigger internal dissent within technology companies that have Chinese staff, and potentially place an ethical burden on Chinese personnel (similar to those felt by Google employees during the Project Maven protests) who feel patriotic to their country and betrayed or unwelcome given their company's policy. The story would be the same for personnel from other countries. The case of China rises specifically because a large number of Chinese personnel work in American technology companies compared to other foreign nationals.[112]

2. **Allied requests for assistance.** What if an American-allied government like the United Kingdom, Canada, Australia, or New Zealand asks for cyberdefense assistance? Assuming

the partner country is doing so legally within the Law of Armed Conflict and for legitimate purposes against a hostile actor, these requests would seem justifiable under a "100% defense" terms of service statement. By setting clear policies, companies can prepare in advance for requests for help.

3. **Rejecting American government requests for assistance.** In the circumstance that a U.S.-owned technology company were to reject the U.S. government's request to use its infrastructure for some defensive purpose, the U.S. government could take the company to court to try to force compliance with U.S. government mandates. This problem should be considered in advance by both government and private-sector entities as the U.S. government prepares for potential contingencies. Courts could force a company's hand for national security requirements, but would come with costs to both the government and the company.

PLANNING EXERCISES AND OPERATIONS

As government and private-sector leaders begin to plan for cyberspace conflict, escalation scenarios should include some of the following variables, among others:

- **The military, political, and economic conditions involved in conflict escalation**, to include macro-economic trends that would drive or be driven by the conflict, key foreign leader and social group behaviors, and country-specific triggers (i.e., tensions between North and South Korea or Russian incursions into Ukraine).

- **Indicators of conflict escalation**, to include weapons likely to be used, to pre-deployed forces that could be targeted, countries that may be drawn into the conflict, and violent actions that could be conducted on forces, populations, and economic centers as the conflict begins.

- **U.S. and allied cyberspace infrastructure that could be targeted**, to include U.S. and allied critical infrastructure owners and operators in the U.S. and in third-party nations (neither the adversary nor the victim), as well as U.S. military and allied forces deployed in theaters of operations. For any conflict preparation, information technology companies should identify in advance major U.S. and allied critical infrastructure targets and operators that use their services. Some companies will be more likely to be targeted through

information technology than others, including major financial services, energy systems, and government agencies that support U.S. health and safety, as well as media and political campaigns.

- **Playbook of cyberspace capabilities that can be used to analyze, identify, and blunt an adversary offensive operation**. Companies and the government should come to a scenario exercise with a playbook of strategic capabilities that they can use on their platforms to anticipate, analyze, and respond to a cyberattack. They should be prepared to present options to the group. This discussion will be sensitive for the company and classified for the government, and will likely only be possible in a classified, small-group setting that allows participants to deliberate around the narrative over time.

The Enduring Security Framework will be a natural forum for this partnership to unfold. It is defensively focused and provides a mechanism for building relationships between the government and the private sector around a range of cybersecurity issues. It allows for a classified exchange of views; provides regular contact between the constituents through biannual senior leader meetings with companies and agencies; and builds ties between more junior employees in the public and private sectors. It also gives senior leaders an opportunity to build bonds of trust through one-on-one conversations.

LEADERSHIP FOR SUCCESS

Sustained leadership is the most important ingredient for building effective public-private partnerships. Close bonds between key leaders are vital. Leaders and individuals build trust between themselves first and then, over time, between the groups, organizations, and countries that they lead.

What are some conditions for leaders to keep in mind as they try to build trust? There is a rich field in business and leadership studies on this subject, but a short review of the literature indicates that to build and sustain trust requires that individuals can 1) be vulnerable to others (making ourselves vulnerable to being let down or to betrayal); 2) think well of others and their ability to respond to our expectations; 3) be optimistic that they will be sufficiently competent in certain respects of the relationship to deliver on our expectations; and 4) that they will strive consistently to meet the other's expectations or explain in advance when those expectations cannot be met.[113]

We know that effective public-private bonds can be built. The BIOS mitigation gave us our first indicator. The Snowden disclosures set cooperation back, but over time and through repeated conversations to rebuild trust, multiple private-sector leaders have expressed support for building defensively focused partnerships. Patriotism and a shared view of the cyberthreat provided a strong foundation on which to build. Russia's actions in 2016 and its continued aggression toward the United States—including penetrating the U.S. electric grid and trying to manipulate the electoral process through 2018—helped drive the public and private sectors to seek the same goals in 2018 and in advance of 2020: to prevent foreign meddling and cyberattacks on the U.S. election. Now the question is whether the two communities will seize on the opportunity to move forward together.

Other basic business practices will prove valuable to trust building. Participants will need to value people as people, not as means to an end; act as role models for the kind of relationships they seek to build; admit mistakes when they happen; be as honest as possible in the course of the discussion; and be curious about the people involved and the nature of the conversation.[114] Trust will need to be affirmed repeatedly. **If the partnership leads to value, it will result in a natural development of options and creative avenues for cooperation that the two communities may not presently foresee.**

Conclusion

Today the United States exists in a gray space below the level of outright hostilities in cyberspace. In the future, a potential adversary will seek to use whatever digital tools they have available during a conflict to gain an advantage. The national security community and the technology community can get ahead of that threat through prudent planning. Leaders and line officers in the public and private sector can invest in building relationships of trust, establish formal planning and coordination mechanisms to deal with escalating hostilities, conduct table-top exercises, and develop tactical options to use their own authorities and platforms to blunt cyberattacks in a combined manner analogous to the response to the 2018 U.S. Congressional Election. Cooperation should extend from the chief executive and cabinet secretary level to that of the deputy assistant secretary level and below to facilitate regular contact and options development. It should bring together the best strategists and operational planners in each organization to discover the best approach. The effort will need to be sustained for years to build trust.

Cooperation will come with risks to companies. When one company executive said, "We want to be patriotic but we are global operators," he reflected a sentiment shared by every company leader interviewed for this study. Before beginning to plan with the federal government, companies will need to carefully assess the cost and benefit of any counter-offense operation from the standpoint of their global customers and markets. They may need to amend their terms of service agreements to declare that they will block any hostile actor that tries to use their infrastructure for malicious purposes. Such a strategy will help improve their defense posture and inoculate a company against accusations of national preference.

What might success look like at the end of five years?

Under the leadership of the Enduring Security Framework or another national security forum, the U.S. government and the U.S. technology sector will have worked together to plan and exercise for a range of potential conflict scenarios impacting the United States including scenarios involving cyberspace operations conducted by China, Russia, North Korea, or Iran. Scenarios will have examined how a conflict could impact the American people, the American government, and American corporations. Participants will have used the planning process to develop viable defensive options and deepen bonds of trust.

At the end of five years, the two communities will have a deeper understanding of each other's cultures, personnel, and operating environments. Today, the two communities misperceive each other and lack situational awareness of each other's capabilities. At the end of five years, government operators will be more familiar with the policies, worldviews, and technological capabilities of their private-sector counterparts. Private-sector actors will likewise have a deeper understanding of the cultures, operating environments, and technological capabilities of the U.S. military, intelligence community, and law enforcement community. Mutual respect and trust will have increased through good-faith engagements.

At the end of five years, companies should be able to identity areas where cooperation has helped them to understand potential risks and stay ahead of threats. In a scenario involving a dangerous cyberspace operation, public opinion could quickly and significantly shift against a company, as happened to Facebook following Russia's actions in 2015–2016. If companies have worked with the government in advance of a contingency, however, they will be in a stronger position when an incident occurs. After five years, companies should be able to look back and identify measurable benefits in this regard.

Over the last decade, the public and private sectors made significant progress in building the structures and teams for cybersecurity. It was not enough. The Russian cyberattack on American democracy in 2015–2016 marked the end of Act I in our cybersecurity story. In the future, it is likely that hostile powers will try to impact American interests in new and more dangerous ways. This could include manipulating political narratives, altering demographic data, attacking the electoral process, or targeting aspects of public safety and security in ways yet unseen. As digital access expands and attack surfaces grow, attackers will seek alternative methods to subvert the United States and its interests. The two communities should begin now to conduct regular, deliberate planning exercises for combined, voluntary operations.

Endnotes

1 2018 U.S. Department of Defense Cyber Strategy, Summary, available at https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF (accessed on November 14, 2019).

2 See The Intel Brief, "Protection for the Election," *The Cipher Brief*, available at https://www.thecipherbrief.com/column_article/protection-for-the-election; accessed on August 19, 2019.

3 See Microsoft's statements about its approach to countering malicious actors. Jon Brodkin, "Microsoft shuts down phishing sites, accuses Russia of new election meddling," *Ars Technica*, August 21, 2018, available at https://arstechnica.com/tech-policy/2018/08/microsoft-shuts-down-phishing-sites-accuses-russia-of-new-election-meddling/; accessed on August 19, 2019. For Facebook's statements, see Nathaniel Gleicher, "More Information About Last Week's Takedowns," Facebook Newsroom, November 13, 2018, available at https://newsroom.fb.com/news/2018/11/last-weeks-takedowns/ ; accessed on August 19, 2019.

4 Tom Gjelten, "Cyber Briefings 'Scare the Bejeezus' Out of CEOs," *National Public Radio*, May 9, 2012, available at https://www.npr.org/2012/05/09/152296621/cyber-briefings-scare-the-bejeezus-out-of-ceos; accessed on August 19, 2019.

5 Author conversations during a Defense Department trip to Silicon Valley in May of 2015.

6 Google, "Artificial Intelligence at Google: Our Principles," Google AI, available at https://ai.google/principles/; accessed on August 8, 2019.

7 Zachary Fyer-Biggs, "Inside the Pentagon's Plan to Win Over Silicon Valley AI Experts," *Wired*, December 12, 2018, available at https://www.wired.com/story/inside-the-pentagons-plan-to-win-over-silicon-valleys-ai-experts/; accessed on August 19, 2019.

8 Brad Smith, "Growing consensus on the need for an international treaty on nation state attacks," The Official Microsoft Blog, available at https://blogs.microsoft.com/on-the-issues/2017/04/13/growing-consensus-need-international-treaty-nation-state-attacks/; accessed on August 19, 2019. Beyond defensive operations, Brad Smith also argued correctly that the world's governments should gain international support for legal norms and agreements for preventing attacks on infrastructure. These agreements have developed, including an agreement in 2015 by the U.S. and China to refrain from stealing intellectual property, and members of the United Nations Group of Governmental Experts have worked to gain agreement for states to refrain from conducting cyberspace operations against civil infrastructure. Absent countries supporting and following international agreements, however, the next step is for companies to work with governments to plan and identify when and how a hostile nation might break their policies and terms of service. For more background on these issues, see https://fas.org/sgp/crs/row/IN10376.pdf, accessed August 19, 2019, and also https://www.cfr.org/blog/united-nations-doubles-its-workload-cyber-norms-and-not-everyone-pleased; accessed on August 19, 2019.

9 Sam Brannen, "Five Risks to Watch in 2019," December 13, 2019, Center for Strategic and International Studies, available at https://www.csis.org/analysis/five-risks-watch-2019; accessed on August 19, 2019.

10 Brendan Koerner, "Inside the cyberattack that shocked the U.S. Government," *Wired Magazine,* October 23, 2016, available at https://www.wired.com/2016/10/inside-cyberattack-shocked-us-government/; accessed on August 19, 2019.

11 Matt Burgess, "When a tanker vanishes, all the evidence points to Russia," *Wired UK,* September 21, 2017, available at https://www.wired.co.uk/article/black-sea-ship-hacking-russia; accessed on August 19, 2019.

12 For a detailed breakdown of the Stuxnet attack, see Ralph Langner, "To kill a centrifuge," The Langner Group, November, 2013, available at https://www.langner.com/wp-content/uploads/2017/03/to-kill-a-centrifuge.pdf; accessed on August 19, 2019.

13 Robert Mueller, *The Report On The Investigation Into Russian Interference In The 2016 Presidential Election,* March, 2019, available at https://en.wikipedia.org/wiki/File:Report_On_The_Investigation_Into_Russian_Interference_In_The_2016_Presidential_Election.pdf; accessed on August 19, 2019.

14 See the U.S. Department of Homeland Security, Cybersecurity Strategy, May 15, 2018, available at https://www.dhs.gov/sites/default/files/publications/DHS-Cybersecurity-Strategy_1.pdf; accessed on July 18, 2019.

15 See the Summary of the Department of Defense Cyber Strategy, 2018, available at https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF; accessed on July 20, 2019.

16 See The U.S. Department of Justice, "U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage," Press Release, May 19, 2014, available at https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor; accessed on August 19, 2019.

17 The U.S. Department of the Treasury, "Treasury Sanctions Iranian Organizations and Individuals Supporting Intelligence and Cyber Targeting of U.S. Persons," Press Release, February 13, 2019, available at https://home.treasury.gov/news/press-releases/sm611; access on August 19, 2019.

18 Julian Barnes, "Cyber Command Operation Took Down Russian Troll Farm for Midterm Elections," *The New York Times*, February 26, 2019, available at https://www.nytimes.com/2019/02/26/us/politics/us-cyber-command-russia.html; accessed on August 19, 2019.

19 For example, Microsoft has developed a threat operations center that leverages the company's large global software platform to monitor behavior across large parts of the internet. Capabilities include Microsoft's cloud capability and the omnipresent Windows platform. For background on Microsoft's Threat Intelligence Center and the platform, see Patrick Howell O'Neil, "Inside the Microsoft team tracking the world's most dangerous hackers," *MIT Technology Review,* November 6, 2019. Google has one of the largest data sets about nation-state and non-state actors' behavior on the internet, and the Google Threat Analysis Center has "tracked Iranian hackers as they spread disinformation in the U.S., unmasked North Korea's responsibility for a crippling global computer virus, and probed Russians linked to the 2016 hack of the Democratic National Committee." See Robert McMillan, "Inside Google's Team Fighting to Keep Your Data Safe From Hackers," *Wall Street Journal*, January 23, 2019, available at https://www.wsj.com/articles/inside-googles-team-battling-hackers-11548264655?fbclid=IwAR2WuzxlOpLrc9p7QwXRvfWi94HJsWGeSnY2lJbqnedfgbbgiSo0D6zuwBY; accessed on October 20, 2019.

20 For more on DNS blocking, see https://www.webtitan.com/what-is-dns-blocking/.

21 For information on IP blocking, see https://www.domain.com/blog/2019/05/23/how-to-block-an-ip-address/.

22 A "CIDR" block is a table of IP addresses. CISCO and other companies have blocked Russian, China, and Iranian access to their platforms in the past. https://community.cisco.com/t5/firewalls/block-all-russia-public-ip-addresses/td-p/2094303.

23 Exercises happen all the time for different sectors and objectives; there have been few coordinated scenarios between the public and private sector to prepare for hostilities and discover options. The Department of Treasury-led Hamilton series of exercises, for example, "explored the risk of a banking system collapse resulting from a cyberattack." Its purpose was to evaluate the "impact of a cyber incident on financial stability." See Shaun Waterman, "Bank regulators briefed on Treasury-led cyber drill," *CyberScoop,* July 20, 2016, available at https://www.fedscoop.com/us-treasury-cybersecurity-drill-july-2016/ (accessed on November 13, 2019).

24 The U.S. Senate Committee on Armed Services, "Inquiry into Cyber Intrusions Affecting US Transportation Command Contractors," U.S. Government Printing Office, 2014, available at https://www.armed-services.senate.gov/imo/media/doc/SASC_Cyberreport_091714.pdf; accessed on August 19, 2019.

25 See Microsoft's statements about its approach to countering malicious actors. Jon Brodkin, "Microsoft shuts down phishing sites, accuses Russia of new election meddling," *Ars Technica*, August 21, 2018, available at https://arstechnica.com/tech-policy/2018/08/microsoft-shuts-down-phishing-sites-accuses-russia-of-new-election-meddling/; accessed on August 19, 2019. For Facebook's statements, see Nathaniel Gleicher, "More Information About Last Week's Takedowns," Facebook Newsroom, November 13, 2018, available at https://newsroom.fb.com/news/2018/11/last-weeks-takedowns/; accessed on August 19, 2019.

26 See The Intel Brief, "Protection for the Election," *The Cipher Brief*, available at https://www.thecipherbrief.com/column_article/protection-for-the-election; accessed on August 19, 2019.

27 Edelman, Edelman Trust Barometer, January 20, 2019, available at https://www.edelman.com/trust-barometer; accessed on August 27, 2019.

28 Author conversation with a senior security leader at a major information technology company in California in April and May of 2018.

29 The U.S. Director of National Intelligence, "Background to 'Assessing Russian Activities and Intentions in Recent US Elections': The Analytic Process and Cyber Incident Attribution," January 6, 2017, available at https://www.dni.gov/files/documents/ICA_2017_01.pdf; accessed on August 19, 2019.

30 To borrow a phrase from the military strategist Carl von Clausewitz, a country's "center of gravity" is the source from which a country draws its strength. It could include the political leadership, the economy, or the population. In United States' history, al-Qaeda struck at America's center of gravity when it flew airplanes into the World Trade Center (finance) and the Pentagon (military), and aimed for the White House or the Capitol Building (political). Each building symbolized a part of the country's "center of gravity."

31 Some of this writing about the Russian attack has appeared in other sources by the author, including *Secure Beyond Breach: Building a Defense in Depth Strategy Through Security Segmentation*, Illumio, available at https://www.illumio.com/resource-center/guide-secure-beyond-breach; accessed on August 27, 2019.

32 See Evan Osnos and David Remnick, and Joshua Yaffa, "Trump, Putin, and the New Cold War," *The New Yorker*, February 24, 2017, available at https://www.newyorker.com/magazine/2017/03/06/trump-putin-and-the-new-cold-war; accessed on August 19, 2019.

33 Of all of the organizations that did work in advance of the 2018 election, Harvard's Belfer Center did the most comprehensive work, under the leadership of Eric Rosenbach, Robby Mook, and Matt Rhoades. See the "Defending Digital Democracy" initiative webpage, https://www.belfercenter.org/publication/defending-digital-democracy-project-aims-protect-election-integrity.

34 For the rise of Asia and the risks posed by the expanding Internet, see Jonathan Reiber and Arun Mohan Sukumar, *Asian Cybersecurity Futures: Opportunity and Risk in the Rising Digital World*, Berkeley's Center for Long-Term Cybersecurity, December, 2017, available at https://cltc.berkeley.edu/2017/12/18/asian-cybersecurity-futures/; accessed on August 19, 2019.

35 See Alex Hollings, "Counterfeit Air Power: Meet China's Copycat Air Force," *Popular Mechanics*, September 19, 2018, available at https://www.popularmechanics.com/military/aviation/g23303922/china-copycat-air-force/; accessed August 19, 2019.

36 Jose Pagliery, "The Inside story of the biggest hack in history," *CNN,* August 5, 2015, available at https://money.cnn.com/2015/08/05/technology/aramco-hack/index.html; accessed on August 19, 2019.

37 See Eric Chabrow, "7 Iranians Indicted for DDoS Attacks Against U.S. Banks," Bank Info Security, March 24, 2016, available at https://www.bankinfosecurity.com/7-iranians-indicted-for-ddos-attacks-against-us-banks-a-8989; accessed on August 19, 2019.

38 Agence-France Presse, "U.S. charges North Korean in Bangladesh central bank, Sony hacks," *ABS-CBN News*, September 7, 2018, available at https://news.abs-cbn.com/business/09/07/18/us-charges-north-korean-in-bangladesh-central-bank-sony-hacks; accessed on August 19, 2019.

39 See Brendan Koerner, "Inside the cyberattack that shocked the U.S. Government," *Wired Magazine,* October 23, 2016, available at https://www.wired.com/2016/10/inside-cyberattack-shocked-us-government/; accessed on August 19, 2019.

40 Andy Greenberg, "How an entire nation became Russia's test bed for cyberwar," *Wired Magazine,* June 20, 2017, available at https://www.wired.com/story/russian-hackers-attack-ukraine/; accessed on August 19, 2019.

41 David Sanger, "Russian Hackers Appear to Shift Focus to U.S. Power Grid," *The New York Times*, July 27, 2018, available at https://www.nytimes. com/2018/07/27/us/politics/russian-hackers-electric-grid-elections-.html; accessed on August 19, 2019.

42 This example has been cited in other sources including *Defend Forward and Assume Breach: Preparing Canada for a Cyber Resilient Future,* Testimony Before the Canadian Parliament, Subcommittee on Public Safety and National Security, February 6, 2019, available at https://openparliament.ca/committees/public-safety/42-1/148/jonathan-reiber-1/only/; accessed on August 27, 2019. For data on China's penetrating Cambodia's electoral infrastructure, please see Gerry Shih, "US firm: Chinese hackers infiltrate Cambodia ahead of polls," *Associated Press*, July 11, 2018, available at https://www.apnews.com/0b52e20517a74b678cf5eae5d0e177ab; accessed on August 19, 2019.

43 See, *inter alia*, Nathaniel Persily, "Can Democracy Survive the Internet?" *Journal of Democracy*, 28 (July 2017), available at https://www.journalofdemocracy.org/article/can-democracy-survive-the-internet; accessed on August 20, 2019. See also Cass Sunstein, *Republic.com 2.0*, Princeton University Press, 2011.

44 See the U.S. Constitution, available at https://constitutionus.com/; accessed on August 19, 2019.

45 See UpGuard's post on Verizon and AT&T, "Cyber Resilience Showdown: AT&T vs. Verizon," *UpGuard,* November 8, 2019, available at https://www.upguard.com/blog/cyber-resilience-showdown-att-vs-verizon; accessed on November 13, 2019.

46 For the process of identifying critical assets and infrastructure that required additional cybersecurity, see the Department of Homeland Security's Presidential Executive Order (EO) 13800 Strengthening the Cybersecurity of

Federal Networks and Critical Infrastructure Support to Critical Infrastructure at Greatest Risk ("Section 9 Report") Summary.

47 See S. Iswaran, Minister-in-Charge of Cybersecurity, "Statement on the cyber-attack on SingHealth's IT system, during Parliamentary Sitting on 6 August 2018," available at https://www.mci.gov.sg/pressroom/news-and-stories/pressroom/2018/8/statement-by-mr-s-iswaran-on--cyber-attack-on-singhealth-it-system-during-parl-sitting-on-6-aug-2018; accessed on November 13, 2019.

48 Brendan Koerner, "Inside the cyberattack that shocked the U.S. Government," *Wired Magazine,* October 23, 2016, available at https://www.wired.com/2016/10/inside-cyberattack-shocked-us-government/ accessed on August 19, 2019.

49 Supra 18.

50 The U.S. Department of Homeland Security, Cyber Incident Response, available at https://www.dhs.gov/cisa/cyber-incident-response; accessed on August 19, 2019. See also the National Cybersecurity Incident Response Plan, available at https://www.dhs.gov/cisa/cyber-incident-response; accessed on August 19, 2019

51 See David Sanger, Nicole Perlroth, and Michael Schmidt, "Obama Vows a Response to Cyberattack on Sony," *The New York Times*, December 19, 2014, available at https://www.nytimes.com/2014/12/20/world/fbi-accuses-north-korean-government-in-cyberattack-on-sony-pictures.html; accessed on November 13, 2019.

52 See the United States of America vs. Wang Dong, Sun Kailiang, Wen Xinyu, Huang Zhenyu, Go Chunhui, Criminal Number 14-118, U.S. District Court, Western District of Pennsylvania, May 1, 2014, available at https://www.justice.gov/iso/opa/resources/5122014519132358461949.pdf (accessed on November 13, 2019).

53 U.S. Department of Justice Press Release, "Seven Iranians Working for Islamic Revolutionary Guard Corps-Affiliated Entities Charged for Conducting Coordinated Campaign of Cyber Attacks Against U.S. Financial Sector," March 24, 2016, available at https://www.justice.gov/opa/pr/seven-iranians-working-islamic-revolutionary-guard-corps-affiliated-entities-charged (accessed on November 13, 2019).

54 See Jonathan Reiber, "States Must Explain When a Cyber Attack Might Draw a Violent Reprisal," *DefenseOne,* June 6, 2019, available at https://www.defenseone.com/ideas/2019/06/states-must-explain-when-cyber-attack-might-draw-violent-reprisal/157533/ (accessed on November 13, 2019).

55 Financial Services Information Sharing and Analysis Center, Mission Statement, available at https://www.fsisac.com/; accessed on August 19, 2019, May 8, 2018, available at https://www.dhs.gov/sites/default/files/publications/EO-13800-Section-9-Report-Summary-20180508-508.pdf; accessed on October 29, 2019.

56 The White House, Vulnerabilities Equities Policy and Process for the United States Government, November 15, 2017, available at https://www.whitehouse.gov/sites/whitehouse.gov/files/images/External%20-%20Unclassified%20VEP%20Charter%20FINAL.PDF; accessed on August 19, 2019. As the VEP policy states, "the primary focus of this policy is to prioritize the public's interest in cybersecurity and to protect core Internet infrastructure, information systems, critical infrastructure systems, and the U.S. economy through the disclosure of vulnerabilities discovered by the USG, absent a demonstrable, overriding interest in the use of the vulnerability for lawful intelligence, law enforcement, or national security purposes." Importantly, the policy states that "It is also important to recognize that the USG has not created these vulnerabilities. Information systems will continue to have vulnerabilities and efforts to discover and disclose these flaws is an ongoing need."

57 Michael Daniel, The White House Blog, "Heartbleed: Understanding When We Disclose Cyber Vulnerabilities," April 28, 2014, available at https://obamawhitehouse.archives.gov/blog/2014/04/28/heartbleed-understanding-when-we-disclose-cyber-vulnerabilities; accessed on October 29, 2019.

58 National Institute for Standards and Technology, NIST Framework, updated regularly; available at https://www.nist.gov/cyberframework; accessed on August 19, 2019.

59 The U.S. Cybersecurity Information Act of 2014, available at https://www.congress.gov/bill/113th-congress/senate-bill/2588/text; accessed on August 19, 2019.

60 Gartner, "Gartner Forecasts Worldwide Information Security Spending to Exceed $124 Billion in 2019," Press Release, August 15, 2018, available at https://www.gartner.com/en/newsroom/press-releases/2018-08-15-gartner-forecasts-worldwide-information-security-spending-to-exceed-124-billion-in-2019.

61 See the statement of Admiral Cecil Haney, Hearing on the National Defense Authorization Act for Fiscal Year 2016, Committee on Armed Services, U.S. House of Representatives, Subcommittee on Strategic Forces, February 26, 2015, available at https://fas.org/irp/congress/2015_hr/stratfor.pdf; accessed on October 29, 2019.

62 Author conversation with a senior official working in government and regulatory affairs for a major American telecommunications provider in May 2018.

63 Stanford Encyclopedia of Philosophy, "Trust," first published February 20, 2006, substantive revision, August 3, 2015, available at https://plato.stanford.edu/entries/trust/; accessed on August 19, 2019.

64 Noticeably absent from this analysis is the narrative about the encryption debate. This debate focused on two polar views, one held by the law enforcement community and one held by the technology and privacy communities. For the law enforcement, they sought company assistance in breaking encryption or opening up personal devices for counter-terrorism or other purposes. Technology and privacy advocates argued that to do so would forfeit privacy and security for millions once the encrypted door was left open. The encryption debate followed the Snowden disclosures and revealed differences of opinion, but has been treated extensively elsewhere, so I am choosing to omit it. For more on the encryption debate or other related issues of trust between these two communities, see Adam Segal's excellent report on the breakdown between Silicon Valley and Washington following the Snowden disclosures and encryption debate of 2014–2016: Adam Segal, "Rebuilding Trust Between Washington and Silicon Valley," *Council on Foreign Relations*, January 2017, available at https://www.cfr.org/report/rebuilding-trust-between-silicon-valley-and-washington; accessed on October 30, 2019.

65 Conor Friedersdorf, "A Question for 60 Minutes: Why Would China Want to Destroy the Global Economy?" *The Atlantic,* December 16, 2013, available at https://www.theatlantic.com/international/archive/2013/12/a-question-for-em-60-minutes-em-why-would-china-want-to-destroy-the-global-economy/282376/; accessed on August 19, 2019.

66 Paul Szoldra, "This is everything Edward Snowden revealed in one year of unprecedented top-secret leaks," *Business Insider,* September 16, 2016, available at https://www.businessinsider.com/snowden-leaks-timeline-2016-9; accessed on August 19, 2019.

67 The White House, Presidential Policy Directive – Signals Intelligence, January 17, 2014, available at https://obamawhitehouse.archives.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities; accessed on August 19, 2019.

68 Nitasha Tiku, "Three Years of Misery Inside Google, the Happiest Company in Tech," *Wired*, August 13, 2019, available at https://www.wired.com/story/inside-google-three-years-misery-happiest-company-tech/; accessed on August 19, 2019.

69 Google, "Artificial Intelligence at Google: Our Principles," Google AI, available at https://ai.google/principles/; accessed on August 8, 2019.

70 Ryan Browne, "Top US general says Google 'is indirectly benefiting the Chinese military," *CNN*, March 14, 2019, available at https://www.cnn.com/2019/03/14/politics/dunford-china-google/index.html, accessed on December 11, 2019.

71 Zachary Fyer-Biggs, "Inside the Pentagon's Plan to Win Over Silicon Valley AI Experts," *Wired*, December 12, 2018, available at https://www.wired.com/story/inside-the-pentagons-plan-to-win-over-silicon-valleys-ai-experts/; accessed on August 19, 2019.

72 Klint Finley, "Microsoft CEO Defends Army Contract for Augmented Reality," *Wired*, February 2, 2019, available at https://www.wired.com/story/microsoft-ceo-defends-army-contract-augmented-reality/; accessed on August 19, 2019.

73 Brad Smith, "Technology and the U.S. military," Official Microsoft Blog, October 26, 2018, available at https://blogs.microsoft.com/on-the-issues/2018/10/26/technology-and-the-us-military/; accessed on August 19, 2019.

74 Nicholas Thompson and Fred Vogelstein, "15 months of fresh hell inside Facebook," *Wired*, April 16, 2019, available at https://www.wired.com/story/facebook-mark-zuckerberg-15-months-of-fresh-hell/; accessed on August 19, 2019.

75 There is a tremendous amount of research available for when and how the U.S. government can build support for war with the American population. Factors of American support include the population's perception of the adversary threat (including the behavior of the regime and its military power), the opinions of the elites, and an individual's own perceptions about his or her life. See *inter alia* Dukhong Kim, "Affect and Public Support for Military Action," SAGE Open, October-December 2014: 1–13, available at https://journals.sagepub.com/doi/pdf/10.1177/2158244014560530; accessed on October 31, 2019. See also Stephen M. Walt, "How do you sustain public support for wars of choice?" *Foreign Policy,* October 31, 2019, available at https://foreignpolicy.com/2012/10/11/how-do-you-sustain-public-support-for-wars-of-choice/ (accessed on October 31, 2019).

76 Author conversation with former senior White House cybersecurity official in Silicon Valley in April 2018.

77 See John Miller, "NSA speaks out on Snowden, spying," *CBS News*, December 15, 2013, available at https://www.cbsnews.com/news/nsa-speaks-out-on-snowden-spying/ (accessed on November 13, 2019).

78 Michael Steen and Richard McGregor, "Merkel's phone tapped by US since 2002, leaked documents claim," *The Financial Times*, October 27, 2013, available at https://www.ft.com/content/65044af4-3f15-11e3-b665-00144feabdc0 (accessed on November 1, 2019).

79 There is a wealth of reporting on the impact of the Snowden disclosures on the government and the technology sector. See Robyn Greene, Danielle Kehl, Robert Morgus, and Kevin Bankston, "Surveillance Costs: The NSA's Impact on the Economy, Internet Freedom & Cybersecurity," New America Foundation Policy Paper, available at https://www.newamerica.org/oti/policy-papers/surveillance-costs-the-nsas-impact-on-the-economy-internet-freedom-cybersecurity/ (accessed on November 13, 2019). See also Claire Cain Miller, "Revelations of N.S.A. Spying Cost U.S. Tech Companies," *New York Times*, March 21, 2014, available at https://www.nytimes.com/2014/03/22/business/fallout-from-snowden-hurting-bottom-line-of-tech-companies.html (accessed on November 13, 2019).

80 The intelligence community operates in the shadows to collect intelligence and operate on behalf of the nation's interests when called upon to do so by the president. At times, like other parts of U.S. policy, the actions of the intelligence community have failed to live up to the nation's ideals. Edward Snowden did not follow protocol by speaking to his superiors about the issues that concerned him when he learned about the NSA's bulk metadata collection program. He never became a "whistleblower," he simply stole and disclosed the information.

As a writer in *The Guardian* commented, "Very few people think the NSA is staffed by mustache-twirling villains who view the law as an obstacle to be overcome. . . . Malice isn't the real issue. Overbroad tools are." See Spencer Ackerman, "NSA goes on 60 Minutes: the definitive facts behind CBS's flawed report," *The Guardian*, December 16, 2013, available at https://www.theguardian.com/world/2013/dec/16/nsa-surveillance-60-minutes-cbs-facts; accessed on August 19, 2019.

81 Author conversations with two cybersecurity leaders at a major Silicon Valley company and a major U.S. government agency responsible for cybersecurity.

82 Brad Smith, Microsoft Blog Post, "We are taking new steps against broadening threats to democracy," August 20, 2018, available at https://blogs.microsoft.com/on-the-issues/2018/08/20/we-are-taking-new-steps-against-broadening-threats-to-democracy/; accessed on August 19, 2019.

83 Nathaniel Gleicher, "More Information About Last Week's Takedowns," Facebook Newsroom, November 13, 2018, available at https://newsroom.fb.com/news/2018/11/last-weeks-takedowns/; accessed on August 19, 2019.

84 See The Intel Brief, "Protection for the Election," *The Cipher Brief*, available at https://www.thecipherbrief.com/column_article/protection-for-the-election; accessed on August 19, 2019.

85 For background, see Richard Rhodes, *The Making of the Atomic Bomb* (Simon and Schuster, New York, NY, 1986).

86 "Don't be evil" was removed from the company's code of conduct in 2018. See Kate Conger, "Google Removes 'Don't Be Evil' Clause From Its Code of Conduct," *Gizmodo*, May 18, 2018, available at https://gizmodo.com/google-removes-nearly-all-mentions-of-dont-be-evil-from-1826153393 (accessed on October 30, 2019).

87 Supra 58.

88 See Philip Gourevitch, *We Wish To Inform You That Tomorrow We Will Be Killed With Our Families* (Farrar, Straus and Giroux, New York, NY: 1998).

89 See Gourevitch. See also Allison Des Forges, *Leave None to Tell the Story: Genocide in Rwanda* (Human Rights Watch, New York, NY: 1999). Her chapter "Propaganda and the Media" is available online at https://www.hrw.org/legacy/reports/1999/rwanda/Geno1-3-10.htm (accessed on October 31, 2019).

90 Author conversation with a senior official working in government and regulatory affairs for a major American telecommunications provider in May of 2018.

91 Author conversation with a senior technology leader in New York City in December 2018.

92 Multiple author conversations in 2018 and 2019 with policy staff in Washington, D.C.

93 They may also have hoped that this project would yield results that could help them achieve the same objective.

94 Author phone conversation with a senior chief information security officer at a U.S. Internet infrastructure provider in April 2018.

95 Author phone conversation with a senior chief information security officer at a U.S. internet infrastructure provider in April 2018.

96 On the use of scenarios for cybersecurity, please see, *inter alia*, UC Berkeley's work on scenarios; this book covers the history and practice of scenario planning and provides tools for business and governments to use as they think about the future of cybersecurity risk. UC Berkeley Center for Long-Term Cybersecurity, Scenarios 2025, available at https://cltc.berkeley.edu/scenarios2025/; accessed on August 19, 2019.

97 For an Asia-specific set of scenarios, please see Reiber and Sukumar's *Asian Cybersecurity Futures*, at https://cltc.berkeley.edu/2017/12/18/asian-cybersecurity-futures/.

98 Author conversation with a senior official working in government and regulatory affairs for a major American telecommunications provider in May 2018.

99 Ibid..

100 Author conversation with a senior technology company cybersecurity strategist in France in December 2017.

101 Supra 82.

102 Matthew Rosenberg, Nicholas Confessore, and Carole Cadwalladr, "How Trump Consultants Exploited the Facebook Data of Millions," *The New York Times,* March 17, 2018, available at https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html; accessed on August 19, 2019.

103 Views about China's importance to the global economy are broadly accepted and compared to the other potential cyberspace adversaries of Russia, Iran, and North Korea, it is the only emerging market of significant interest to American information technology companies. See the Director of National Intelligence report on China from 2012 as just one example. In the World Bank's baseline modeling of future economic multipolarity, China—despite a likely slowing of its economic growth—will contribute about one-third of global growth by 2025, far more than any other economy. See U.S. National Intelligence Council, *Global Trends 2030: Alternative Worlds* (Washington, D.C.: Office of the Director of National Intelligence, 2012), iv, https://globaltrends2030.files.wordpress.com/2012/11/global-trends-2030-november2012.pdf. This data was ratified in author conversations with a former senior White House official responsible for cybersecurity planning in April 2018.

104 See the Department of Defense, "Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2019," Office of the Secretary of Defense, available at https://media.defense.gov/2019/May/02/2002127082/-1/-1/1/2019_CHINA_MILITARY_POWER_REPORT.pdf (accessed on November 13, 2019).

105 In economic terms, purchase power parity deals with the quantity of the currency needed to purchase a given unit of a good. See The World Bank, *The World Bank in China,* April 8, 2019, available at https://www.worldbank.org/en/country/china/overview; accessed on August 19, 2019.

106 Sean Keane, "Huawei ban: Full timeline on how and why its phones are under fire," CNET, August 19, 2019, available at https://www.cnet.com/news/huawei-ban-full-timeline-on-how-and-why-its-phones-are-under-fire/; accessed on August 19, 2019.

107 See the list of companies banned in China on WikiPedia, available at https://en.wikipedia.org/wiki/Websites_blocked_in_mainland_China; accessed on August 16, 2019.

108 Presentation to the author and other delegates at the East-West Institute US-China-India trilateral commission in 2018.

109 Brad Smith, "Growing consensus on the need for an international treaty on nation state attacks," The Official Microsoft Blog, available at https://blogs.microsoft.com/on-the-issues/2017/04/13/growing-consensus-need-international-treaty-nation-state-attacks/; accessed on August 19, 2019. Beyond defensive operations, Brad Smith also argued correctly that the world's governments should gain international support for legal norms and agreements for preventing attacks on infrastructure. These agreements have developed, including an agreement in 2015 by the U.S. and China to refrain from stealing intellectual property, and members of the United Nations Group of Governmental Experts have worked to gain agreement for states to refrain from conducting cyberspace operations against civil infrastructure. Absent countries supporting and following international agreements, however, the next step is for companies to work with governments to plan and identify when and how a hostile nation might break their policies and terms of service. For more background on these issues, see https://fas.org/sgp/crs/row/IN10376.pdf, accessed August 19, 2019, and also https://www.cfr.org/blog/united-nations-doubles-its-workload-cyber-norms-and-not-everyone-pleased; accessed on August 19, 2019.

110 For a definition of a Special Master in the United States, please see Wikipedia, https://en.wikipedia.org/wiki/Special_master; accessed on August 19, 2019.

111 See Brad Smith's statement in advance of the 2018 U.S. Congressional Election; https://blogs.microsoft.com/on-the-issues/2018/08/20/we-are-taking-new-steps-against-broadening-threats-to-democracy/.

112 Danielle Paquette, "Tech giants to Trump: we need Chinese workers," The Washington Post, May 4, 2018, available at https://www.washingtonpost.com/news/wonk/wp/2018/05/02/tech-giants-to-trump-we-need-chinese-workers/; accessed on August 19, 2019.

113 Supra 64.

114 Liz Ryan, "Ten ways to build trust on your team," *Forbes,* March 17, 2018, available at https://www.forbes.com/sites/lizryan/2018/03/17/ten-ways-to-build-trust-on-your-team/#157eeef12445; accessed on August 19, 2019.

About the Author

Jonathan Reiber is a writer and security strategist based in Oakland, California. From serving in senior positions in the Department of Defense in Barack Obama's administration to leading cybersecurity strategy for companies in Silicon Valley, he is focused on building resilience to technological and political disruptions in the digital age. Host of the *Beyond the Breach* podcast, he advises governments, companies, and organizations on the risks of digitization—from online extremism to influence operations to cybersecurity. A former Chief Strategy Officer for Cyber Policy and Speechwriter in the Office of the Secretary of Defense, his writing has appeared and been highlighted by *Foreign Policy, The Atlantic Monthly, DefenseOne, The Christian Science Monitor*, *The San Jose Mercury News, Mint*, *Today* and *Literary Hub*. He is the author of the scenario study, *Asian Cybersecurity Futures: Opportunity and Risk in the Rising Digital World* (with Arun Mohan Sukumar), and the principal author of *The Department of Defense Cyber Strategy* (2015). He has held research and writing fellowships at UC Berkeley's Center for Long-Term Cybersecurity, the Smith Richardson Foundation, and the Thomas J. Watson Foundation.

Prior to serving as CSO for Cyber Policy, Jonathan served as Special Assistant and Speechwriter to the United States' Deputy Secretary of Defense, Dr. Ashton B. Carter, and previously as Special Assistant to the United States' Principal Deputy Under Secretary of Defense for Policy, Dr. James N. Miller. In both positions he focused his work on foreign and defense policy, grand strategy, Middle East and Asia-Pacific affairs, and cybersecurity. He campaigned full-time for Barack Obama in 2007–2008. Prior to U.S. government service, he worked for the United Nations Peacekeeping Mission in Sudan, as a Research Manager at a geological intelligence firm, and as a political and communications advisor to the Episcopal Church. He is a graduate of Middlebury College, where he studied religion and creative writing, and The Fletcher School of Law and Diplomacy, where he served as Editor-in-Chief of *The Fletcher Forum of World Affairs*.

CLTC

Center for Long-Term Cybersecurity

UC Berkeley

Center for Long-Term Cybersecurity
cltc.berkeley.edu
@CLTCBerkeley