Virtually Defenseless: America's Struggle to Defend Itself in Cyberspace and What Can be Done About It

Daniel B. Prieto

Nearly twenty-five years after the United States sounded the alarm regarding the risks to US national and economic security posed by the internet, we are struggling in our battle in and for cyberspace. Russia and China, other nation-states, and nation-state-aligned groups have come to regularly employ cyber-enabled espionage, information operations, and cyber effects operations against the United States and its allies to disrupt and degrade civil society and democratic political and institutional stability and to threaten or disrupt critical economic sectors and critical infrastructure. Making matters worse, adversaries have done so with little pushback or consequence. The United States, for all of its undeniable cyber capabilities, has for two decades misconstrued core elements of conflict and competition in cyberspace, focusing on the remote possibility of full-blown cyberwar instead of the ongoing pattern of adversary action below the threshold of war and seeking to address those attacks as individual incidents instead of essential elements of comprehensive political warfare campaigns waged by adversaries against the United States. As a result, US policy has been centered on flawed and incomplete defensive cyber strategies that relied almost exclusively on hardening targets via technical defenses, while neglecting defensive cyber effects operations to counter adversary cyber capabilities and failing to have a systematic answer for cyber-enabled influence operations and information warfare. This article examines the complex roots of America's challenges in cyberspace and sets forth a vision for a US cyber strategy that is essential to and inextricable from emerging US grand strategy for the post-post-9/11 world.

Introduction

In 1998, President Clinton issued Presidential Decision Directive 63 (PDD-63), marking the first White House effort to raise the alarm about the risks posed to the United States from its dependence on cyberspace. Over the ensuing two decades, national security leaders and major media outlets issued warnings about the threat to US national security from cyberspace. In 1999, *The New York Times* painted a vision of the "specter of simultaneous computer network

Daniel B. Prieto is an Adjunct Senior Research Scholar in the Arnold A. Saltzman Institute of War and Peace Studies at the Columbia University School of International and Public Affairs, as well as a cybersecurity strategy executive at a leading global technology firm. He is a member of the Council on Foreign Relations and the Homeland Security Experts Group, and he previously served in the White House as Director for Cybersecurity Policy on the staff of the National Security Council and as the Chief Technology Officer in the U.S. Department of Defense Office of the Chief Information Officer.

attacks against banking, transportation, commerce, and utility targets—as well as against the military—[that] conjures up the fear of an electronic Pearl Harbor in which the nation is paralyzed without a single bullet ever being fired."[1] In 2008, former counterterrorism czar Richard Clarke again warned of an electronic Pearl Harbor.[2] In 2012, Secretary of Defense Leon Panetta warned of a cyber 9/11.[3]

The warning of a "cyber Pearl Harbor" or a "cyber 9/11" type of attack established a high bar for what a cyberattack of national significance would look like, creating an expectation of catastrophic physical impacts emanating from a cyberattack. But, as cyberattacks against the United States became more numerous and more serious, they have failed to fit the profile. By October 2021, US National Cyber Director Chris Inglis acknowledged that "a cyber Pearl Harbor is already behind us. It happened cumulatively over time and we all experienced some part of it already."[4] Instead of major cyberattacks starkly manifesting themselves in physical destruction and body counts, they took the form of subtler operations—below the threshold of war—that compromised US secrets, threatened critical infrastructure, undermined democratic elections, and exacerbated fissures in civil society.

"A cyber Pearl Harbor is already behind us. It happened cumulatively over time and we all experienced some part of it already."

The admission that we have already experienced our cyber Pearl Harbor or cyber 9/11 is an admission that the United States has, in many respects, failed when it comes to national cyber defense. For years, the United States held a dominant position over its adversaries in cyberspace. But as adversaries evolved their capabilities and became more aggressive in their attacks, especially over the past decade after the United States' Stuxnet attacks on Iran, US cyber defense policy languished, and we failed to respond decisively and firmly in the face of ever-worsening cyber threats. US policymakers have been burdened by the flawed assumption that private sector investments to reduce technical vulnerabilities at the point of attack would be sufficient to thwart persistent nation-state attackers. Furthermore, by largely viewing each attack as an isolated incident, rather than as a component of an adversary's concerted political warfare campaign, policymakers missed the forest for the trees. Hence, when those network defenses failed, as they often did, the US government would respond with a predictable but ineffective mix of tough talk, limited diplomatic retaliation, economic sanctions, and criminal indictments. Particularly lacking from the US defensive cyber playbook has been the mechanisms to proactively hunt and evict adversaries from US critical infrastructure, to engage in defensive cyber effects operations to counter adversary cyber capabilities closer to their source, and a strategy for how to deal with foreign manipulation of the US information environment to sow discord and disinformation. Year after year, the Office of the Director of National Intelligence (ODNI) Worldwide Threat Assessments document the continued and unchecked advance of adversary

cyber threats, which metastasized from "emerging" in 2011 to "acute" in 2021. The cyber threat facing the United States today is acute, because flawed US cyber policy allowed it to become acute.

Despite years of warnings from national security leaders, and scores of billions of dollars in cybersecurity investments over more than twenty years, the United States lacks the strategy, doctrine, and national unity of effort—among government agencies and in coordination with the private sector and allies—to prosecute effective cyber defense against adversary cyber encroachments. Furthermore, the United States lacks doctrine on how to use the full range of cyber capabilities in comprehensive support of US grand strategy.[5] To be sure, a new US grand strategy is itself just starting to coalesce after a two-decade focus on counterterrorism as the linchpin of US foreign policy.[6] However US grand strategy might eventually evolve, it should be uncontroversial to believe that US cyber policy should comprehensively support, at minimum, a defense of US national and economic security and the integrity of US democratic institutions and democratic political processes. In support of this goal, this article seeks to analyze the following: the roots, evolution, and limitations of US defensive cyber policy; the rise and evolution of adversary cyber capabilities; the lack of effective US response to nation-state cyber aggression; and the way forward for US cyber policy to both counter adversary cyber aggression and to comprehensively advance US foreign policy objectives.

The cyber threat facing the United States today is acute, because flawed US cyber policy allowed it to become acute.

Definitions

In common parlance, the term "cyberattack" is used as a general term to describe a wide variety of malicious cyber activity that affects the confidentiality, integrity, or availability of computer networks, systems, and data. It includes denial-of-service (DoS) attacks; the penetration of systems; the theft of data for intelligence purposes or for the benefit of commercial or military interests; the manipulation of data for financial gain; the leaking of stolen data to influence public opinion; and the compromising of systems to extract ransom, establish a foothold in preparation for a future attack, or simply inflict damage outright. Adversaries' manipulation of social media to sow disinformation do not constitute cyberattacks *per se*, since the confidentiality, integrity, and availability of individual computers are not threatened, but rather are operations in which cyber-enabled means are used to conduct influence campaigns and information warfare. For the purposes of this article, it is important to define a number of core concepts that are essential to understanding the range of adversary and US activity in cyberspace. It is worth noting that there is little consistency or definitive consensus on either the proper terms of art or the definitions of such terms.

As such, the terms below were chosen to communicate and describe essential concepts, and their definitions often reflect hybrid combinations of definitions of multiple different terms which nonetheless describe largely similar concepts.

"*Cyber espionage*": activities conducted in or through cyberspace that access computers, information systems, or networks without authorization from their owners or operators for the primary purpose of collecting information and intelligence and with the intent to remain undetected.

"*Cyber effects*": "the manipulation, disruption, denial, degradation, or destruction of computers, information or communications systems, networks, physical or virtual infrastructure controlled by computers or information systems, or information resident thereon."[7]

"*Offensive cyber effects operations* (*OCEO*)": operations and related programs or activities conducted in or through cyberspace that are intended to enable or produce cyber effects for the purposes of projecting power.[8]

"*Defensive cyber effects operations* (*DCEO*)": operations and related programs or activities conducted in or through cyberspace that are intended to enable or produce cyber effects for the purposes of defending or protecting against ongoing or imminent threats, attacks, or other malicious cyber activity.[9]

"*Cyber operational preparation of the environment* (*C-OPE*)": "non-intelligence enabling functions within cyberspace conducted to plan and prepare for potential follow-on military operations. C-OPE includes but is not limited to identifying data, system/network configurations, or physical structures connected to or associated with the network or system (including software, ports, and assigned network address ranges or other identifiers) for the purpose of determining system vulnerabilities."[10]

"*Cyber-enabled influence operations*": a state's use of tools and methods in cyberspace to affect or manipulate the opinion, attitudes, behaviors, motivations, or decisions of foreign target audiences.[11]

"*Network defense*": "activities conducted and tools implemented on a computer, network, or information or communications system by the owner or with the consent of the owner and, as appropriate, the users for the primary purpose of protecting (1) that computer, network, or system; (2) data stored on, processed on, or transiting that computer, network, or system; or (3) physical and virtual infrastructure controlled by that computer, network, or system."[12]

Political Warfare 2.0: Cyber as a Core Element of Adversary Statecraft

In the early days of the Cold War, George Kennan in 1948 set forth the concept of political warfare. In its broadest definition, political warfare is "the employment of all the means at a nation's command, short of war, to achieve its national objectives. Such operations are both overt and covert. They range from such overt actions as political alliances, economic measures, and 'white' propaganda, to such covert operations as clandestine support of 'friendly'

foreign elements, 'black' psychological warfare, and even encouragement of underground resistance in hostile states."[13] The concept provides a strategic frame within which to locate adversary cyber efforts, both today and when examining their historical evolution.

In 2021, China and Russia are engaged in global political warfare against the United States on myriad fronts. They pose the most significant nation-state cyber threats to the United States and its interests, leveraging cyberattacks and cyber-enabled information operations as fully integrated components of their foreign policy and statecraft. Iran and North Korea are engaged in comparable political warfare as well, with a more regional and less global focus. Cyberattacks and cyber-enabled information warfare play an essential role in adversary efforts to advance their foreign policy objectives and to support domestic political and economic objectives. Their cyber capabilities advanced significantly over the past decade, with the years 2011–2016 reflecting a period of emergent adversary capability, and 2017–2021 reflecting a period in which a wide range of espionage, attack, and influence operations first became much more common, and then more acute.

Annual ODNI Worldwide Threat Assessments provide useful insight into the goals and capabilities of these four adversaries, analyzing each state's goals and cyber capabilities in the three strategic fronts of influence, espionage, and disruptive attacks. These assessments portray Russian, Chinese, Iranian, and North Korean cyberspace goals as strikingly similar, though proportional in scope to their capabilities (both cyber and conventional). Looking globally, Russia and China seek to use cyber tools to spread their influence, undercut the influence of the United States, and reshape international norms of statecraft to better favor their authoritarian systems of government. However, their strategies differ. China prioritizes efforts to stifle criticism and dissent online globally. Russia prioritizes disinformation and hack-and-leak operations to undermine US global standing, divide Western alliances, sow discord inside the United States, influence US voters and decision-makers, aggravate social and racial tensions, and undermine US public trust in authorities. On the espionage front, China is pursuing a broad strategy of targeting US government and private sector networks, especially those tied to key technology sectors like microchips or weapons systems, while Russia is more focused on gaining access to US, NATO, and other allied partners' technical information, military plans, and policy deliberations. Finally, these states have developed and still seek to improve their ability to disrupt US critical infrastructure by "preparing the environment" in ways that will facilitate cyberattacks against these infrastructures in the event of a future conflict.[14] According to reports, Iran and North Korea essentially pursue these same goals, only with much more modest means; however, North Korea presents the additional threat of outright theft of financial assets, having stolen hundreds of millions of dollars in cryptocurrency to fund government priorities, likely including nuclear and missile programs.

Background for US Policy

PDD-63, issued in 1998, marked the genesis of cybersecurity as an issue of national importance. It focused on vulnerabilities in computer networks, systems, and data and viewed market forces as sufficient to address those vulnerabilities. Information sharing about vulnerabilities between the public and private sectors would allow the market to efficiently address vulnerabilities. However, individual organizations were responsible for protecting their own technology assets. Government intervention and action to address cybersecurity vulnerabilities were to be explored only as a last resort. The focus on a market approach to cybersecurity made sense at the time. US policy was focused on enabling innovation, and there was broad bipartisan consensus that a policy of non-interference and non-regulation would be most conducive to the internet's growth. Given its exclusive focus on vulnerabilities, PDD-63 was silent on and provided no guidance regarding cyber threat actors and how to deal with them.

The laissez-faire approach to cybersecurity was further reinforced by the belief that an unfettered internet was inherently a force for economic growth, political liberalization, and democratization. That belief was based on a view that authoritarian states relied on strict control of information for their survival. The internet's proliferation would inherently undermine authoritarian regimes by increasing the availability of information and speeding its flow. As such, an unencumbered internet was viewed as a significant source of US influence and soft power, a reliable arrow in its quiver to promote democratic liberalization globally.

Those three elements—a focus on technical vulnerabilities, a laissez-faire market-driven approach to defense, and an abiding belief in an unfettered internet as a constructive source of American power—comprised the intellectual cornerstones of US cyber policy and doctrine. The persistence of these unquestioned assumptions in US cyber policy over the past two decades, however, has hampered the United States' ability to effectively confront cyber threats. While there have been some modifications to the general strategy, such as the Bush administration's 2003 National Strategy to Secure Cyberspace, which envisioned federal intervention as necessary in only limited circumstances of heightened cyber threats to economic and national security networks, the centrality of private sector investment and action as the most effective means of cyber defense has remained a constant in policymakers' thinking.[15] Ultimately, PDD-63 cast a long shadow, conditioning and constraining US cyber policy to this day.

The persistence of these unquestioned assumptions in US cyber policy over the past two decades has hampered the United States' ability to effectively confront cyber threats.

While US defensive cyber strategy was conditioned by the market-oriented approach to cybersecurity built into PDD-63, US thinking regarding the use of cyber effects operations was conditioned by concern and caution. Five assumptions were critical: 1) cyber tools were novel elements of statecraft; 2)

cyber effects operations and their associated cyber tools and mechanisms (e.g., malware and DoS attacks) should be thought of as akin to weapons of war, with the potential to generate physical effects equivalent to a traditional use of force; 3) that the use of cyber "weapons" could lead to conflict escalation;[16] 4) that the impacts generated by the use of cyber effects operations were unpredictable; and 5) that the use of cyber effects operations by the United States would likely serve as a precedent for other countries as they developed and contemplated their own use of cyber capabilities.

In light of these perceptions and concerns, there was an abiding fear—across multiple administrations—of the risks posed by the United States' own use of cyber effects operations. In 2003, for example, President Bush rejected the use by the Department of Defense (DOD) and the US intelligence community to engage in cyber operations to cripple the financial assets and systems of Saddam Hussein and the Iraqi government, with officials worrying about the possibility that the effects would spread and cause worldwide financial havoc.[17] Given his concerns, President Bush ordered the Pentagon to develop rules of engagement for the use of cyber "warfare."[18] Similarly, President Obama expressed concern that the use by the United States of offensive cyber effects operations could set a precedent that would enable other actors to justify similar cyberattacks and that the administration lacked and would eventually need to develop a conceptual framework and clear set of rules for evaluating the use of offensive cyber effects operations as "cyber weapons."[19] With the view that cyber effects operations had the potential to generate a Pandora's Box of unpredictable collateral damage and escalatory effects, and with the risk of giving license to US adversaries, the rules of engagement for US cyber operations under Presidents Bush and Obama became highly restrictive.[20]

Any framework and set of rules governing cyber effects operations would need to address a range of questions around the use of force under international law.[21] First, under what circumstances do cyber effects operations qualify as a use of force under the laws of war?[22] Second, if a use of force, would a cyber effects operation be considered justified, and if it was defensive, would it be considered proportional under the laws of war? Third, what is the likelihood of collateral damage, and how much is acceptable?[23] Fourth, under what circumstances would cyber effects operations be escalatory? Fifth and finally, how would US operations set precedents for other states' cyber operations, and how could this disadvantage the United States in the future?

In addition, it is important to ask what role US cyber strategy will play in support of US grand strategy, which is itself at a crossroads after focusing for twenty years on combatting terrorism, in light of concerted efforts since the end of the Cold War to cultivate China and Russia as productive partners on a range of global issues, and in hopes of incentivizing their political liberalization. Since 2018, however, conflict and competition with Russia and China have moved to the forefront of US national security strategy. And since 2021, the focus on global counterterrorism is no longer at the center of US foreign policy priorities. With US grand strategy at such a crossroads, what is the proper role of US cybersecurity strategy and doctrine within our overall foreign policy?

Should US cyber strategy focus on more than just the defense of the United States, and how far should US cyber capabilities be used to defend allies? Should the US leverage cyber means to not just defend democracies, but to promote democracy as well—which could include using US cybersecurity means and measures to protect, defend, enable, or otherwise support fledgling democratic movements, dissidents, or political opposition groups? To explore these questions, it is important to review and assess the evolution of US cyber policy and capabilities over time, the evolution of adversary capabilities, and whether and how US behavior in cyberspace shaped adversary behavior.

Timeline of Capabilities, Policy, and Thinking

1998–2010: The United States Ascendant

The first dozen years after PDD-63 was issued constituted a period of relatively low cyber threat from nation-state adversaries. From 1998 to 2003, cyber threats to US interests were largely theoretical. Cyber vulnerabilities increased—in line with the steady adoption of the web, online media and communications tools, and social media—as more and more systems became interconnected. Despite growing vulnerabilities, threats were minimal as few nation-states possessed the requisite technical capabilities to pose cyber threats. From 2004 to 2010, adversary capabilities were nascent, with a small handful of adversaries exhibiting limited offensive cyber capabilities. There was a low to moderate level of adversary targeting of US government and commercial interests, ranging from traditional espionage to targeted intellectual property (IP) theft. To the extent that more aggressive actions occurred, they were limited to regional conflicts (e.g., Russia's use of DoS and website defacement attacks in its military campaigns against Georgia in 2008). Those attacks marked the first known use of cyberattacks synchronized with conventional military operations.[24]

From 1998 to 2010, the US exercised unparalleled cyber prowess when it came to intelligence and espionage operations to gain insight into the actions and motivations of other countries. While official details of US cyber activity are understandably not publicly disclosed, reporting by private sector cybersecurity firms on nation-state "advanced persistent threat" actors provides insight into US capabilities. For example, in 2015, Kaspersky Labs published a report on the Equation group, widely presumed to be the US National Security Agency.[25,26] The report characterized the Equation group as "probably the most sophisticated computer attack group in the world. . . a powerful threat actor with an absolute dominance in terms of cyber-tools and techniques."[27] According to the report, "since 2001, the Equation group has been busy infecting thousands, or perhaps even tens of thousands of victims throughout the world in the following sectors: government and diplomatic institutions; telecoms; aerospace; energy; nuclear research; oil and gas; military; nanotechnology; Islamic activists and scholars; mass media; transportation; financial institutions; companies developing encryption technologies."[28]

US effectiveness and dominance in its cyber espionage capabilities were reflected in other ways as well. It maintained leadership at the forefront of the development and use of hacking tools.[29] And US global intelligence collection efforts had accelerated rapidly with both the Global War on Terror and the contemporaneous global rise in the use of social and mobile technologies. In 2012, the US policy document governing US cyber operations, Presidential Policy Directive 20 (PPD-20), made clear that rules for cyber espionage and intelligence collection were mature and well-practiced, and that espionage was to be treated separately from policy frameworks and rules for cyber effects operations.[30]

Beyond espionage, starting during the Bush administration, the United States began targeting Iranian nuclear facilities with offensive cyber effects operations.[31] President Bush deemed the operation necessary to slow Iranian uranium enrichment efforts and to forestall an Israeli conventional strike against Iran.[32] The Obama administration inherited and accelerated the operation—known as "Olympic Games"—deeming the risk of collateral damage acceptable and given a lack of other viable options for slowing Iran. The joint US-Israeli cyber operation successfully penetrated Iranian nuclear reactors with bespoke malware, known as Stuxnet, that specifically targeted Siemens industrial controllers in order to disrupt centrifuges at Iran's Natanz nuclear facility.[33]

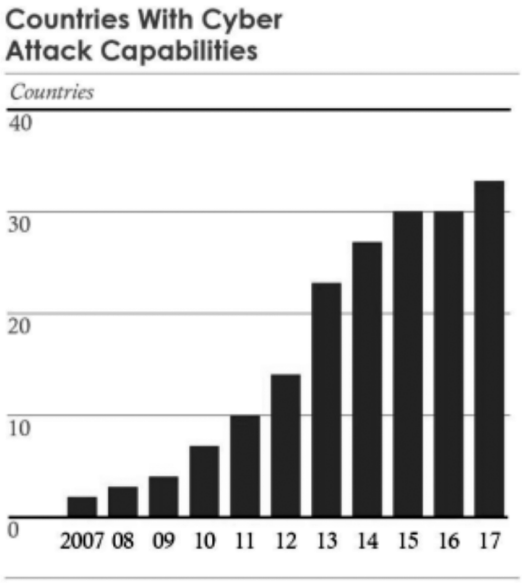
2011–2016: The United States Self-Deters While Adversaries Strengthen

While the Stuxnet attack was a success insofar as it achieved its intended effect of slowing Iranian nuclear development, it also produced negative unintended consequences. President Obama had worried about collateral damage as well as the risk of creating precedent that could be used by other countries to justify their own offensive cyber effects operations.[34] The exploit was intended to affect only the targeted Iranian nuclear facilities. But by 2010, the Stuxnet malware escaped beyond Natanz's air-gapped network and began spreading globally, infecting scores of thousands of computers in over one hundred countries.[35]

The Stuxnet attacks and their fallout marked a pivot both for the direction of US cyber policy and the trajectory of adversary cyber capabilities. In response to the Stuxnet attacks, Iran built up its cyberattack capabilities, and, more broadly, other US adversaries also developed greater capability and displayed greater aggressiveness.[36] Notably, the number of countries with cyberattack capabilities tripled from 2011–2015, from ten countries to thirty.

US adversaries also developed greater capability and displayed greater aggressiveness.

Just as the cyber threat environment was about to worsen, the United States reaffirmed and extended core elements of its approach and assumptions regarding cyber defense, while also implementing a range of limitations on its use of cyber effects operations, ostensibly to reduce the risk of unintended consequences, like those wrought by Stuxnet. In 2011, the Obama administration's International Strategy for Cyberspace reasserted that the internet was a core element of US soft power, warranting a laissez-faire approach.[37] The strategy acknowledged threats, and



Source: DNI World Threat Assessment (2018)

it promoted diplomacy, law enforcement, self-defense, and deterrence to deal with those threats. It also focused heavily on norms as an essential element to shape and govern acceptable state behavior in cyberspace. Consistent with prior policy, it focused on reducing technical vulnerabilities to attacks and response and recovery after attacks occur. It acknowledged hostile acts in cyberspace, the inherent right to self-defense, and US willingness to use "all necessary means—diplomatic, informational, military, and economic" to defend the United States, though it did not clarify the United States' willingness to employ cyber effects operations as means of defense and deterrence.

The 2011 DOD Strategy for Operating in Cyberspace acknowledged the rising level of cyber threat and again focused significantly on reducing technical vulnerabilities to address the threat.[38] It focused on better indication and warning, defense of DOD networks, support of civilian agencies in defense of .gov networks and systems, collaboration with the private sector, and the potential need for regulation and incentives to boost protective activities. It pledged to work with the Department of Homeland Security (DHS) to establish a holistic government approach. To address nation-state cyber aggression, it asserted broad optionality on how to defend and deter, "reserv[ing] the right to defend these vital national assets as necessary and appropriate" and envisioning allied coalition efforts to deter malicious activities in cyberspace. It invoked "active cyber defense" for protecting DOD networks—which it defined as the real-time capability to discover, detect, analyze, and mitigate threats and vulnerabilities. Of note, its "active" measures were all reactive, focused on better detection and response.

Notably the strategy itself was silent on cyber effects operations. That same year, though, in a report to Congress, the DOD acknowledged its capacity

to conduct offensive cyber operations in cyberspace if directed by the president and under the laws of war, "consistent with the policy principles and legal regimes that the Department follows for kinetic capabilities, including the law of armed conflict."[39]

In 2012, the Obama White House issued PPD-20, which comprehensively laid out the governance procedures for the use of cyber effects operations, both offensive and defensive.[40] PPD-20 became public as part of the unauthorized Edward Snowden disclosures of sensitive US Intelligence in 2013. PPD-20 reaffirmed law enforcement as well as technical defenses by IT owners as the preferred methods of defense while also implementing layers of procedural gates for the use of CEOs.[41] PPD-20 embodied the concerns regarding the use of cyber operations that had animated both Republican and Democratic administrations to that point. It directed that DCEOs be contemplated only "in circumstances when network defense or law enforcement measures are insufficient. . . and when other previously approved measures would not be more appropriate."[42] It created a high bar for defensive activity within US territory, barring operations "that are intended or likely to produce cyber effects within the United States unless approved by the President," despite the fact that most effective adversary actions against US commercial interests, government organizations, and critical infrastructure have occurred on US networks on US soil. Furthermore, any DCEO that might be pursued should be proportionate and rely on the inherent right of self-defense under international law, including anticipatory self-defense actions.

Consideration for the use of DCEOs was governed by a need to conduct an onerous and comprehensive evaluation of competing criteria, including the threat of adversary action and retaliation, the pros and cons of DCEOs versus other alternative measures, an assessment of intelligence gain or loss, political impacts, and the risk of creating "unwelcome norms of international behavior."[43] Consequently, DCEOs against nation-state adversaries were often ruled out based on the concern that cyber operations risked exposing US intelligence presence on adversary systems, which could lead to that access, and therefore that source of intelligence, being shut off.[44]

In sum, PPD-20 prohibited most possible uses of DCEOs without presidential approval while also failing to provide presidential government-wide strategic leadership and guidance regarding when and how DCEOs should be deployed and for what purposes. Instead, it was left up to individual departments and agencies to "establish criteria and procedures to be approved by the president for responding to persistent malicious cyber activity against US national interests."[45] Therefore, despite acknowledging that it may be necessary and beneficial to resort to DCEOs, at its core the directive was highly restrictive in its use of DCEOs from an approvals, threshold, and geographic perspective.[46] PPD-20 enshrined DCEOs as measures of last resort, effectively excluding them as a viable response option to mounting adversary cyber aggression.[47]

The cautious approach to cyber effects operations built into PPD-20 was consistent with concerns raised by the ODNI in 2013 that the "growing use of cyber capabilities to achieve strategic goals is also outpacing the develop-

ment of a shared understanding of norms of behavior, increasing the chances for miscalculations and misunderstandings that could lead to unintended escalation."[48] Along those lines, much of the same cautious thinking built into PPD-20 was also evident in the DOD's 2015 cyber strategy.[49] It focused largely on how to improve the integration of cyber operations into US military planning. As regards critical infrastructure, it limited itself solely to the defense of government networks and defense critical infrastructure, deferring to the DHS as the government lead for cyberattacks against civilian infrastructure targets. The 2015 strategy also tended to treat cyberattacks and the response to them as isolated and discrete incidents, rather than as part of ongoing adversary nation-state strategy and behavior. And, likely colored by the unintended consequences of the Stuxnet attacks, it also focused on the risks of collateral damage and escalation that might result from DOD's use of cyber operations. As such, the strategy sought to "control escalation" and "mitigate risk".

The 2015 strategy also tended to treat cyberattacks and the response to them as isolated and discrete incidents, rather than as part of ongoing adversary nation-state strategy and behavior.

So, while US cyber policy continued to focus on technical defenses to counter cyber threats and implemented highly restrictive frameworks around the use of DCEOs, adversary cyber capabilities advanced. The 2011–2015 phase was a period of emerging cyber threat to the United States, during which an expanded set of malicious actors (e.g., Iran and North Korea) developed and tested out new capabilities, while more advanced adversaries increased their level of activity (e.g., China and Russia). Iran launched cyberattacks that compromised US Navy networks (2013), disrupted US financial institutions (2012–2013), targeted US dams, and disrupted the oil and gas operations of Saudi Aramco (2012). North Korea launched ransomware attacks and engaged in destructive cyberattacks against Sony Pictures (2014). China hacked into the Office of Personnel Management (OPM) in 2014, stealing sensitive background investigation information on millions of US citizens and current and former US federal employees while also conducting wide-scale IP theft. Russia was increasingly active and overt in its exploitation of critical infrastructure in Ukraine (2015, 2016) as well as in US military networks. Russia also increasingly targeted critical infrastructures, and targeted US elections with both cyberattacks against election infrastructure and information operations to influence the electorate and amplify discord and distrust.[50]

As adversary cyber operations against the United States rose in severity, the US response was largely muted and piecemeal. In many cases, the United States did respond in kind, typically with a menu of responses that included some combination of economic sanctions, criminal charges, and strongly worded demarches.

In the case of Iranian attacks against US financial institutions in 2012–2013, the United States did not provide material assistance to the affected banks.[51] The State Department sought other countries' assistance to take down compromised computers engaged in the attacks. And the United States indicted

seven individuals linked to the Iranian Revolutionary Guard involved in the attacks.[52] In the case of Sony, while the United States called out North Korea for the attack and imposed sanctions, NSA Director Michael Rogers made it clear that he had argued for a more aggressive response.[53]

Following Chinese theft of commercial and military IP in May 2014, the United States indicted five officers from China's Peoples' Liberation Army on charges of hacking US companies. In the case of the massive hack of sensitive data on government personnel and background investigation data, the United States initially determined that retaliation for the OPM breach was necessary.[54] But it later backed down, declining to impose sanctions so as not to disrupt an upcoming Chinese state visit and for fear of counter sanctions.[55] In exchange, the Chinese government agreed to reduce its cyber theft of IP for purely commercial gain.

In the case of Russia, in response to its 2016 election hacking, the United States responded with a combination of tough talk, diplomatic expulsions, and narrowly targeted sanctions. Criminal indictments eventually were issued in 2018 against twelve members of the Russian intelligence service for hacks against election infrastructure.[56] There was significant debate, within the administration and publicly, about whether the response should have been more forceful and if it should have included a stronger cyber operations component.[57] And it eventually became known that the United States did engage in covert retaliatory cyber operations to threaten Russian infrastructure and signal US capabilities and a warning to the Kremlin.[58]

In each case, the United States stuck to a familiar but self-limited response playbook. However, indictments and sanctions did not prove effective in deterring adversary cyber operations. Proponents of criminal indictments as an effective means of response to cyberattacks argue that they serve as a form of public attribution, a means of disrupting hacking groups, a mechanism to pressure states to refrain from further attacks, and a form of signaling in support of the development of international cyber norms.[59] Proponents of sanctions argue that they help by serving a signaling function, "cutting off financial flows, galvanizing global support for further actions against malicious cyber actors, and enforcing norms of responsible behavior in cyberspace."[60] However, the record of both tools actually imposing sufficient costs to deter malicious behavior is poor.[61] Furthermore, while the United States has also hoped to lead the development and acceptance of international norms in cyberspace, it is a slow process, and the development of adversary cyber capabilities has outpaced the development of these norms.

However, indictments and sanctions did not prove effective in deterring adversary cyber operations.

The message to US adversaries has therefore been that they could use cyberattacks and cyber-enabled information operations—below the threshold of war—against the United States with relative impunity. They can damage and disrupt US companies, steal IP, attack the US government, threaten and disrupt the integrity of critical infrastructure, and threaten and undermine US elections with limited pushback or reprisal.

The dire implications of the United States' weak response to adversary cyber aggression were acknowledged by the ODNI in 2015 and 2016, when it noted that the absence of accepted and enforceable norms, muted responses from victims, low entry costs, and expected payoffs had left malicious nation-state cyber actors undeterred, resulting in "a cyber environment in which multiple actors continue to test their adversaries' technical capabilities, political resolve, and thresholds."[62] Furthermore, the ODNI had come to the conclusion that while the likelihood of a "cyber Pearl Harbor" or "cyber 9/11" remained remote, what was more likely was that the ongoing low and moderate severity cyberattacks would "impose cumulative costs on US economic competitiveness and national security," as well as warning for the first time that data, information, and media manipulation, especially by China and Russia, could be used to distort public discourse and sentiment, reduce trust in systems, create confusion, and undermine decision making.[63] Additionally, by 2017, numerous then-current and former national security officials had begun to increasingly question the efficacy of and thinking behind US defensive cybersecurity policy and actions, including: James Clapper (then Director of National Intelligence), Richard Clarke (former Special Advisor to the President for Cyberspace), Leon Panetta (former Defense Secretary), Jack Goldsmith (former DOD General Counsel), Clint Watts (former FBI Special Agent and counterterrorism expert), Victoria Nuland (former Assistant Secretary of State for European Affairs), and former National Security Council cybersecurity officials, including this author.[64]

Faced with multiple opportunities to display our "technical capabilities, political resolve, and thresholds" to our adversaries, the United States backed down.

In short, the 2011–2017 period should be understood as one of proliferating adversary cyber capabilities and uses, and a failure to respond on the part of the United States. Faced with multiple opportunities to display our "technical capabilities, political resolve, and thresholds" to our adversaries, the United States backed down. The lack of strong US response to growing cyber aggression over this period created a permissive global environment for US adversaries to increase the scale and aggressiveness of their cyber activities to spy on the United States, compromise its critical infrastructures, and degrade its politics and civil society with disinformation and influence operations.

2017 - Present: US Cyber Strategy at Crossroads

By 2017, the mismatch between US cyber strategy and the threat environment was increasingly evident. The ODNI characterized adversaries' strategic success in using cyber means to effectively threaten and damage US interests as essentially a status-quo condition.[65] Its report that year noted that cyber threats from adversaries will put "nearly all [US] information, communication networks, and systems. . . at risk for years," challenge public trust in institutions and norms, impose economic costs, and pose risks to public health and

safety, noting that adversaries remain undeterred from using cyber capabilities to project their influence. In 2018, the ODNI warned of the growing risk of data deletion, localized and temporary disruptions of critical infrastructure, and the global spread of ransomware and malware. The ODNI assessed that while threats of US retaliation had had some deterrent effect on major attacks intended to disrupt critical US infrastructure, it remained worried by the "increasingly damaging effects of cyber operations and the apparent acceptance by adversaries of collateral damage." In 2019, the DNI assessed that "China, Russia, Iran, and North Korea increasingly use cyber operations to threaten both minds and machines," stealing information, influencing citizens, and disrupting infrastructure.[66] Importantly, the ODNI acknowledged the growing ability of adversaries to manipulate social media to influence Americans as a means of altering US policy and decision-making. By 2021, the DNI assessed that "cyber threats from nation-states and their surrogates will remain acute," with the increasing prevalence of states using cyber operations as a tool of national power.[67]

Despite the wide range of warning and frustration over the shortcomings of US cyber policy, the United States "went from occasional wake up calls to one continuous blaring alarm—and got better and better at ignoring it all."[68] Over the decade preceding 2021, cyber threats to US national and economic security metastasized from "emerging" to "acute." From 2016 onward, the steady drumbeat of diverse nation-state cyber operations seeking political, economic, and military advantage against the United States had come to pose a strategic threat to US interests. Critical infrastructure had been significantly compromised, mapped, and put at risk in what amounted to adversary preparation of the environment for future conflict. Theft of sensitive scientific, technical, and business IP from commercial, academic, and government targets helped China undermine US military, technological, and commercial advantage, advance key industrial sectors, and rapidly leap ahead in weapons development. The penetration of government and contractor systems allowed China and Russia to gain unprecedented visibility into US policy deliberations. And a combination of attacks and influence operations, allowed adversaries to weaken democratic institutions, to undermine US alliances and partnerships, to erode confidence and trust in US democratic political processes, and to amplify discord and fragmentation in civil society, making the United States both less governable at home and less effective abroad as an aspirational economic and political model. Adversaries' effective use of a full spectrum of cyberattacks and influence operations has therefore allowed them to threaten or successfully generate physical, economic, security, and psychological consequences.

It supported a more aggressive use of cyber operations to counter nation-state cyber actors, preemptively and overseas if necessary.

Faced with an acute cyber threat and lagging cyber strategy, US cyber policy shifted significantly in 2018. The 2018 DOD cyber strategy reflected a marked departure from prior cyber strategies across both Republican and Dem-

ocratic administrations. It supported a more aggressive use of cyber operations to counter nation-state cyber actors, preemptively and overseas if necessary. At the same time, the Trump administration rescinded PPD-20, replacing it with National Security Presidential Memorandum 13 (NSPM-13).[69]

The evolution regarding the use of cyber effects operations was catalyzed by several factors. First was the worsening threat environment, with US adversaries pursuing increasingly bold and expansive attacks and influence operations, largely unimpeded and undeterred. Also playing a role was the elevation of US Cyber Command to a combatant command, which was proposed under the Obama administration and finalized in 2018. Part of Cyber Command's increasing capability was the evolution of its Cyber Mission Force (CMF), founded in 2012 and comprising 133 cyber mission teams.[70] Cyber Command carried out cyber effects operations against ISIL starting in 2016 and continuing in 2018.[71] In 2019, the United States employed limited cyber operations against Iran in response to their downing of a US drone and a series of attacks on ships in international waters near Iran.[72] Also in 2019, the United States revealed that it had implanted malware on Russian electrical grids as part of an effort to deter malicious Russian cyber activity against the United States.[73]

But the most important contributing factors to the evolution in cyber policy were significant intellectual shifts. First among these was the Trump administration's willingness to put US confrontation with China at the front of its foreign policy agenda. It was also willing to take a more adversarial approach towards Russia within the cyber realm, notwithstanding a vexingly more dovish approach by President Trump towards Russia in other areas.[74]

Second was a reversal on longstanding prior concerns that the use of cyber effects operations created a high level of risk to the United States, including the risk of collateral damage and conflict escalation with US adversaries. Those in favor of extreme caution in the use of cyber effects operations could point to Stuxnet, which inflicted widespread collateral damage and catalyzed a rapid expansion in adversary cyber capabilities. The counterargument is that the United States' overcaution in the use of DCEOs signaled its acquiescence in the face of mounting attacks and that adversaries could increase the scope and scale of cyberattacks against US interests with relative impunity.

Traditional concepts of both deterrence and norms lack viable mechanisms for altering adversary cyber behavior.

The third major intellectual shift in the 2018 DOD cyber strategy is the idea that traditional concepts of both deterrence and norms lack viable mechanisms for altering adversary cyber behavior.[75] The ubiquity of IT vulnerabilities and the inability to eliminate them make cyberattacks too appealing of a tool for adversaries to forego. Adversaries who are generally less powerful than the United States find cyberattacks calibrated below the threshold of war a straightforward, low cost, and low barrier-to-entry tool of political warfare that has the ability to generate outsized, asymmetric benefits.[76] Acknowledging these dynamics, and the failure of deterrence and norms to combat them, the 2018 strategy

dramatically re-oriented the longstanding policy away from target hardening and reactive incident-response damage control, sanctions, and indictments to the use of cyber operations to thwart attacks, calling on the United States to "defend forward" with a level of "persistent engagement."[77]

"Defend forward" signifies the ability and desirability of engaging adversaries on overseas cyber terrain, a sharp departure from prior strategies that limited DOD's defensive cyber activity to DOD networks. NSPM-13's vision for "defend forward" was further enabled by the granting of additional authorities to DOD by Congress in the 2019 National Defense Authorization Act, in which Congress determined that "clandestine" cyber operations qualified as "traditional military activity," exempting them from the presidential approvals required by the covert action statute.[78] "Persistent engagement" requires the United States to contest adversary malicious cyber activity continually in a day-to-day competition. It provides a means of "tacit bargaining" with adversaries through the use of maneuver and action to shape adversary behavior, degrade their capabilities, and signal to them what is and is not acceptable.[79] The rationale for persistent engagement stems from the fact that adversaries are engaged in cyber espionage, cyber operations, and cyber-enabled information operations against the United States in a routine, if not pervasive, manner. Under the new policies, the United States would engage in cyber operations to confront China and Russia on their own turf and on a regular basis, thereby exposing their vulnerabilities, proactively degrading their ability to engage in cyber and influence operations against the United States and its allies and engaging in responsive actions for attacks against us.

In line with the new policies, the United States executed more than twenty-four "hunt forward" operations in fourteen countries from 2018 to 2020, including US Cyber Command's use of DCEOs to protect the 2020 election against Russian and Iranian malicious cyber activity.[80] The long-term impact and efficacy of the policy shift to more robust counter-threat defensive measures still remains to be seen, however. As the policy shift occurred under the Trump administration, it is unclear how and whether the policy changes will be embraced fully by the Biden administration, and whether the shift has sustainable bipartisan support.

In spite of the strategic shift, the US response to a spike in cyberattacks in 2020 and 2021 shows signs of regression to the policies and playbooks that hamstrung effective cyber defense in the past. In 2020 and 2021, there was a surge in attacks fueled by vulnerabilities in COVID-related remote work, by Chinese nation-state actors against widely used identity and email systems,[81] against a range of critical infrastructure sectors that led to shutdowns and shortages in fuel supplies and food processing, and a rash of increasingly automated ransomware attacks. In addition, the Russian intelligence agency, SVR, engaged in a novel compromise of the global software supply chain.[82] By inserting malicious code into an update for a widely used enterprise monitoring software, SolarWinds, Russian state actors were able to compromise 18,000 organizations. Analysts characterized the attacks as espionage, while others argued that such wide ranging intrusions were indiscriminate and, therefore, unacceptable as a

form of espionage.[83] Instead of targeted intrusions to conduct espionage, the attackers were seeking systemic access and "willing to undermine the trust and reliability of the world's critical infrastructure in order to advance the interests of one nation's intelligence agency."[84]

In response to the SolarWinds attack, National Security Advisor Jake Sullivan vowed that the United States would respond with more than just sanctions.[85] Staking out that position was consistent with prior arguments by Sullivan that traditional sanctions alone are insufficient to impose the kinds of costs that might compel malicious nation-state actors like Russia or China to consider modifying their behavior.[86]

In spite of initial signaling that the United States would engage in a tougher than typical response, the United States again reverted to the standard response playbook, levying sanctions and expelling diplomats.[87] At around the same time, the United States pursued criminal indictments against REvil, a Russian-language and Russia-based hacking and ransomware group that disrupted meat processing infrastructure in the United States, in addition to fomenting a wide range of additional ransomware attacks. President Biden argued that the restrained nature of the response that was ultimately taken was necessary in order to avoid conflict escalation with Russia.[88] Notwithstanding the significant 2018 changes to DOD cyber strategy, the United States was again engaging in self-imposed restraint when addressing nation-state cyber threats. A few months later, after US sanctions and repeated warnings from President Biden, Russian intelligence services were back on the offensive, targeting thousands of US government, think tank, and corporate computers.[89]

The predictable effect has been that Russia continues its far reaching malicious cyber activities largely unchanged, unimpeded, and undeterred.[90] The dynamic of US decision-making around the response—whether the attacks were simply espionage; what response measures to pursue; whether a stronger response (including cyber effects operations) would be escalatory; whether escalation would end up being more harmful to the United States—was predictable in light of the prior two decades of policy development and evolution. To address the Chinese attacks, the United States coordinated with allies to issue detailed attribution as a way to name and shame China but did not pursue cyber effects operations as part of a defensive response.[91]

In addition to reverting to the familiar menu of response options in the interest of avoiding escalation, other key aspects of the cyber debate reverted to familiar territory as well. In line with longstanding policy approaches, the Biden administration and Congress are focusing their cyber policy initiatives on hardening targets (e.g., better technical defenses at the point of attack and faster detection after an intrusion, mandatory reporting of ransomware payments, and bans on the use of digital currency to pay off ransomware attackers).[92]

US cyber strategy is at a crossroads. At the start of 2022, bipartisan consensus on the use of cyber effects operations is unclear. US cyber strategy suffers from additional gaps, especially as regards reducing nation-state threats to critical infrastructure and countering the threat of influence

US cyber strategy is at a crossroads.

operations and information warfare. Going forward, US cybersecurity policy should cease existing simply as a technical discipline geared primarily to countering adversaries on an incident-by-incident basis. Instead, US policymakers should strive for cyber strategy to serve a larger purpose and to advance broader US national security priorities in an emerging US grand strategy.

Policy Recommendations: Address Critical Gaps in Cyber Strategy and Align Cyber Doctrine with Emerging US Grand Strategy

A revised US cyber strategy should continue efforts to harden targets and make them more resilient. US cyber policy must also affirm the commitment to use DCEOs to degrade adversary cyber capabilities closer to their point of origin. In addition, US cyber policy must address a number of important areas where US defensive efforts have historically been insufficient.

Recommendation 1: Explicitly align US cyber effects operations and cyber doctrine to the priorities of emerging US grand strategy.

The 2018–2019 NDAA opened the door for increased US cyber operations below the threshold of war. The release of the 2018 DOD strategy a few months later made it US policy to focus those efforts overseas to "defend forward" and "persistently engage" in order to disrupt and degrade adversary cyber capabilities at their point of origin in order to limit or prevent their capacity to operate in the United States. On the one hand, that suggests a level of activity that could completely consume existing US capacity for conducting cyber operations. On the other hand, there may be a natural upper limit to the volume of operations the United States conducts against China and Russia for the simple fact that, at some point, intelligence gain and loss considerations will likely weigh in favor of foregoing certain defensive operations in order to maintain access for surveillance purposes or for future cyber operations. There is always an essential decision-making calculus between collection equities and disruption equities. What is certain though is that while the US Cyber Mission Force has grown and matured, it is not an unlimited resource. It will need to be selectively deployed, which raises the question of when and where it should be deployed and based on what criteria and objectives.

Overseas, the United States will need to answer a range of critical questions as it figures out how to deploy finite cyber resources. Is the need to compete effectively against China and Russia simply *ad hoc* and transactional, or does it imply a broader mandate to defend democracies? And if the goal is to defend democracies, should the United States use cyber operations to defend only a finite set of allied mature democracies (e.g., NATO allies or Japan)? Or might the United States use cyber means seeking to *promote* democracy as well (e.g., in support of Ukraine or Hong Kong, or even political opposition groups, dissidents, and journalists)? Answers to questions like these are unclear, and it is not yet clear where the Biden administration will land as it develops its own

foreign policy doctrine. Contemplating these questions should serve as an opportunity to more clearly define how US cyber resources will be deployed in support of emerging US grand strategy.

Recommendation 2: Develop a national strategy to de-risk US critical infrastructures by proactively hunting for and evicting foreign nation-state adversaries.

According to the ODNI, multiple adversaries currently have the ability to disrupt US critical infrastructures for up to multiple weeks. Their ability to hold US critical infrastructures at risk has been widely speculated as a primary reason for US restraint in responding more firmly to Russian and Chinese cyberattacks generally; there was a fear that more aggressive US responses to cyberattacks could incite even more severe reprisals against US critical infrastructures. Adversaries' ability to so effectively threaten US critical infrastructure is the result of years of preparatory activities that have allowed them to implant malicious code or to install backdoors that would facilitate future access. It should be a goal of US policy to change that status quo and definitively roll back and reduce the current cyber risk posed to critical infrastructure.

It should be a goal of US policy to change that status quo and definitively roll back and reduce the current cyber risk posed to critical infrastructure.

Current US policy is not well positioned to de-risk critical systems within the United States. Vulnerability reduction efforts by critical infrastructure owners have always been unlikely to result in the level of investment needed to thwart advanced persistent threats. DHS guidance for evicting adversaries still puts the onus on the owners of targeted systems.[93] Current cyber bills before Congress focus on requiring critical infrastructure owners to report compromises and on limiting their ability to pay off attackers after ransomware attacks.[94] The 2018 DOD push for increased cyber operations is focused on the use of cyber operations to counter adversaries overseas, not in the United States.

In light of these limits, a new strategy should ensure that the US government works with the approval of and in concert with private sector actors to engage in proactive cyber hunt activities that comprehensively identify and evict nation-state threats from within critical infrastructures here at home. Doing this will require adjusting US cyber defensive strategy to increase government counter-threat operations within the United States. For that to occur, it will require the US federal government to engage more directly with and provide material and resource assistance to private-sector, state, and local owners of critical infrastructure. As recently as 2018, 63 percent of organizations did not engage in proactive threat hunting activities, owing to a lack of adequate resources and technical skills.[95] Federal guidance exhorting owners of targeted systems to conduct hunt operations will not succeed if they don't have the wherewithal to do it.

Efforts to de-risk US critical infrastructures would benefit from the continued growth in the capabilities of DHS's Cybersecurity and Infrastructure Security Agency (CISA). They would also benefit from close coordination between homeland security and law enforcement with DOD cyber mission teams so that the most numerous and skilled cyber operators in the US government can act legally and appropriately under proper civilian authorities within US borders, notably DHS and the FBI.[96] A concerted national initiative of this nature to de-risk critical infrastructures would be a high-profile demonstration of national unity-of-effort when it comes to cyber defense. Pursuing this as a national project will build essential relationships and muscle memory for future cyber conflicts that we are likely to face. Right now, our adversaries are far too able to exploit seams between government and the private sector and between defense and civilian authorities. A national project—across industries, sectors, and disciplines—to de-risk critical infrastructure would make it less likely that adversaries could exploit these seams going forward.

Recommendation 3: Develop a national strategy to counter cyber-enabled influence operations and information warfare.

Cyber-enabled information operations comprise a significant portion of Chinese, and especially Russian, malicious cyber activity. These activities do not constitute cyberattacks, but rather manipulations of the US political and social fabric via social media. Obviously, US issues and concerns over the effect of social media on US politics and society extend beyond foreign interference and manipulation. Social media reforms and regulation are already high on the congressional agenda. Despite that, the United States urgently needs a strategy to limit foreign manipulation of the US information environment. Reforms that could help in this regard include restricting foreign spending related to political campaigns, requiring the labeling and reporting of foreign originated or sourced content, increasing social media data access by researchers, and implementing "know your customer" requirements on social media companies akin to those in the banking industry.[97] Even if such ideas get traction, piecemeal reforms to social media platforms will likely not be sufficient. The private sector cannot be relied upon to solve a complicated national security problem on their own. For its part, the US government should continue to employ DCEOs to degrade adversary capabilities around cyber-enabled influence campaigns and information warfare.[98] The president should make it a national priority to address the manipulation of the US information environment by foreign adversaries since no organization exists in either the private or public sector that has the capacity to comprehensively and continually track and assess dynamic and massive-scale foreign influence campaigns, or the wherewithal to develop and implement countermeasures.[99] Success will require skills and expertise from across society, academia, government, and the private sector. What the nation learns by

The private sector cannot be relied upon to solve a complicated national security problem on their own.

reining in foreign disinformation may even have the added benefit of helping to ameliorate some of the ills posed to society by social media generally, even where foreign adversaries are not involved.

Conclusion

The shortcomings of US cybersecurity policy for the better part of two decades left the United States acutely at risk from mounting adversary cyber aggression. Unless firmly checked, cyberattacks and cyber-enabled influence operations will continue to pose an unacceptable threat to US intellectual property, both commercial and military; the confidentiality of US government policymaking and deliberations; US critical infrastructure as a cornerstone of US economic and national security; trust in the integrity of the US elections; and the cohesion of civil society within the United States and its allies.

US cyber strategy must address the full spectrum of adversary cyber activity: espionage, operational preparation of the environment, cyber effects operations, and cyber-enabled influence operations. Technical defenses, sanctions, criminal indictments, and tough talk have proven to be an incomplete and inadequate cyber strategy. Cyber threats will continue to evolve, and we should expect to see attacks make increasing use of automation, artificial intelligence, machine learning, quantum computing, cloud, and the growing proliferation of Internet of Things (IoT) devices. The 2018 shift to a firmer defensive cyber posture through the increased use of DCEOs to disrupt or degrade adversary cyber capability marked an important evolution in US cyber strategy. It discarded a number of longstanding assumptions that had previously handcuffed US defensive cyber efforts. Notwithstanding signs that the Biden administration, in its response to Russian software supply chain attacks in 2021, might be reverting to problematic prior cybersecurity policy preferences, it will be critical to cement bipartisan consensus regarding the value of defensive cyber effects operations as an indispensable tool in the US playbook for cyber defense.[100]

Beyond the beneficial changes of the 2018 DOD cyber strategy, critically important challenges and gaps remain. First, the United States needs to urgently reduce the level of cyber risk to US critical infrastructures that adversaries have achieved as a result of years engaging in operational preparation of the environment. The government cannot expect the private sector to do this on their own. Within the United States, the role of the government cannot just be to provide technical advice, indications, and warning to the private sector. The US government needs to take a more engaged and direct role in protecting targeted systems within the United States against cyberattacks. Accomplishing this will require the government to provide direct material support and technical expertise to owners of critical infrastructure in order to hunt and

The US government needs to take a more engaged and direct role in protecting targeted systems within the United States against cyberattacks.

evict adversaries from critical US systems. Second, the United States needs to develop a comprehensive strategy to counter nation-state cyber-enabled influence operations. Piecemeal reforms to social media will not be adequate, and there must be a whole-of-nation effort to track, assess, and thwart foreign influence campaigns. Third, the United States needs to marshal its cyber strategy in support of emerging US grand strategy, whether it is outright competition with China and Russia, the defense of democracies, or the promotion of democracy.

As the United States works to fill critical gaps in its cybersecurity strategy and doctrine, we need to make tough decisions about how and where the government should lead, how it should harness and coordinate the deep technical skills and patriotism of the private sector, and how best to collaborate with friends and allies. We cannot wait for five or ten years or more for US cyber policy and doctrine to catch up to the threats that the United States and its allies face now and will certainly face as technology continues to rapidly evolve. The United States needs to ensure that it has the necessary cybersecurity strategy and doctrine in place to support emerging US grand strategy for the coming decades of heightened nation-state competition during the information age and in an increasingly multipolar world.

Notes

[1] John Markoff, "Ideas and Trends: Blown to Bits; Cyberwarfare Breaks the Rules of Military Engagement," *The New York Times*, October 17, 1999, https://www.nytimes.com/1999/10/17/weekinreview/ideas-trends-blown-to-bits- cyberwarfare-breaks-the-rules-of-military-engagement.html.

[2] "Seven Questions: Richard Clarke on the Next Cyber Pearl Harbor," *Foreign Policy*, April 2, 2008, https://foreignpolicy.com/2008/04/02/seven-questions-richard-clarke-on-the-next-cyber-pearl-harbor/. For the evolution of rhetoric regarding cybersecurity, see: Sean Lawson and Michael K. Middleton, "Cyber Pearl Harbor: Analogy, Fear, and the Framing of Cyber Security Threats in the United States 1991–2016," *First Monday* 24, no. 3 (2019), http://dx.doi.org/10.5210/fm.v24i3.9623.

[3] Elisabeth Bumiller and Thom Shanker, "Panetta Warns of Dire Threat of Cyberattack on US," *The New York Times*, October 11, 2012, https://www.nytimes.com/2012/10/12/world/panetta-warns-of-dire-threat-of- cyberattack.html.

[4] Homeland Security Enterprise Forum 2021, "Plenary Session 2: Fireside Chat," live streamed on September 13, 2021, Vimeo video, https://vimeo.com/604590964.

[5] Rebeca Friedman Lissner, "What Is Grand Strategy? Sweeping a Conceptual Minefield," *Texas National Security Review* 2, no. 1 (November 2018), http://dx.doi.org/10.26153/tsw/868. In Lissner: "Grand strategy represents an integrated scheme of interests, threats, resources, and policies. It is the conceptual framework that helps nations determine where they want to go and how they ought to get there; it is the theory, or logic, that guides leaders seeking security in a complex and insecure world . . . grand strategy is. . . long term in its vision, holistic in its treatment of all instruments of national power, and important in its focus on the most consequential interests."

[6] Norman Eisen, Andrew Kenealy, and Mario Picon, "The Biden Democracy Summit: Will It Actually Work?" *Brookings*, December 21, 2021, https://www.brookings.edu/blog/fixgov/2021/12/21/the-biden-democracy- summit-will-it-actually-work/. The Biden Administration's Summit for Democracy in 2021 marks early efforts to shape US foreign policy doctrine after the ostensible end of the War on Terror era.

[7] "PPD-20: US Cyber Operations Policy," Presidential Policy Directive, https://irp.fas.org/offdocs/ppd/ppd-20.pdf.

[8] Computer Security Resource Center, "Offensive Cyberspace Operations (OCO)," *National Institute of Standards and Technology*, https://csrc.nist.gov/glossary/term/offensive_cyberspace_operations; Computer Security Resource Center, "Computer Network Attack (CNA)," *National Institute of Standards and Technology*, https://csrc.nist.gov/glossary/term/computer_network_attack.
[9] "PPD-20: US Cyber Operations Policy."
[10] United States Department of Defense, "2010–2011 Joint Terminology for Cyberspace Operations," memorandum from the Vice Chairman of the Joint Chiefs of Staff, http://www.nsci-va.org/cyberreferencelib/ 2010–11-joint%20terminology%20for%20cyberspace%20operations.pdf.
[11] David Tayouri, "The Secret War of Cyber Influence Operations and How to Identify Them," *Institute for National Security Studies Cyber, Intelligence, and Security Publication* 4, no. 1 (March 2020), https://www.inss. org.il/publication/the-secret-war-of-cyber-influence-operations-and-how-to-identify-them/; Pascal Brangetto and Matthijs A. Veenendaal, "Influence Cyber Operations: The Use of Cyberattacks in Support of Influence Operations," *NATO Cooperative Cyber Defence Centre of Excellence*, 2016, https://ccdcoe.org/uploads/2018/ 10/Art-08-Influence-Cyber-Operations-The-Use-of-Cyberattacks-in-Support-of-Influence- Operations.pdf; Sean Cordey, "Cyber Influence Operations: An Overview and Comparative Analysis," *Center for Security Studies at ETH Zurich*, October 2019, https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities- studies/pdfs/Cyber-Reports-2019-10-CyberInfluence.pdf.
[12] Computer Security Resource Center, "Offensive Cyberspace Operations."
[13] Linda Robinson et al., "The Growing Need to Focus on Modern Political Warfare," *RAND*, 2019, https://www. rand.org/pubs/research_briefs/RB10071.html.
[14] Office of the Director of National Intelligence, "Annual Threat Assessment of the Intelligence Community," April 9, 2021, https://www.dni.gov/files/ODNI/documents/assessments/ATA-2021-Unclassified-Report.pdf; Office of the Director of National Intelligence, "Annual Threat Assessment of the Intelligence Community," 5–6, January 29, 2019, https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf.
In DNI, "Threat Assessment," 2021, 15: North Korea "probably possesses the expertise to cause temporary, limited disruptions of some critical infrastructure networks and disrupt business networks in the United States." In DNI, "Threat Assessment," 2019, 5–6: "China has the ability to launch cyber attacks that cause localized, temporary disruptive effects on critical infrastructure—such as disruption of a natural gas pipeline for days to weeks;" "Russia has the ability to execute cyber attacks in the United States that generate localized, temporary disruptive effects on critical infrastructure—such as electrical distribution network for at least a few hours. . . . Russian intelligence and security services will continue to probe . . . [and map] critical infrastructure with the long-term goal of being able to cause substantial damage;" and Iran is "capable of causing localized, temporary disruptive effects—such as disrupting a large company's corporate networks for days to weeks—similar to its data deletion attacks against dozens of Saudi governmental and private-sector networks in late 2016 and early 2017."
[15] Executive Office of the President of the United States, "The National Strategy to Secure Cyberspace," February 2003, https://www.energy.gov/sites/prod/files/National%20Strategy%20to%20Secure%20Cyberspace. pdf; "The National Strategy," 2003. "In general, the private sector is best equipped and structured to respond to an evolving cyber threat. There are specific instances, however, where federal government response is most appropriate and justified;" "The National Strategy," 2003. Among the threats considered addressable by private action were: "the threat of organized cyber attacks capable of causing debilitating disruption to our Nation's critical infrastructures, economy, or national security" and "[preparation] for cyber strikes during a confrontation by mapping US information systems, identifying key targets, and lacing our infrastructure with back doors and other means of access." In regards to government action, it explained that "externally, a government role in cybersecurity is warranted in cases where high transaction costs or legal barriers lead to significant coordination problems; cases in which governments operate in the absence of private sector forces; resolution of incentive problems that lead to under provisioning of critical shared resources; and raising awareness [. . .] A federal role in these and other cases is only justified when the benefits of intervention outweigh the associated costs. This standard is especially important in cases where there are viable private

sector solutions for addressing any potential threat or vulnerability. For each case, consideration should be given to the broad-based costs and impacts of a given government action, versus other alternative actions, versus non-action, taking into account any existing or future private solutions. Federal actions to secure cyberspace are warranted for purposes including: forensics and attack attribution, protection of networks and systems critical to national security, indications and warnings, and protection against organized attacks capable of inflicting debilitating damage to the economy. Federal activities should also support research and technology development that will enable the private sector to better secure privately-owned portions of the Nation's critical infrastructure."

[16] For a good primer on escalation risks related to cyber, see: Andrew A. Szarejko and John Arquilla, "Accidents and Escalation in a Cyber Age," *War on the Rocks*, December 22, 2021, https://warontherocks.com/2021/12/ accidents-and-escalation-in-a-cyber-age/. For a specific discussion regarding the risks of nuclear escalation in a conventional conflict as a result of cyber attacks, see: James M. Acton, "Cyber Warfare and Inadvertent Escalation," *Dædalus Journal of the American Academy of Arts and Sciences* (Spring 2020), https://www. amacad.org/publication/cyber-warfare-inadvertent-escalation.

[17] John Markoff and Thom Shanker, "Halted '03 Iraq Plan Illustrates US Fear of Cyberwar Risk," *The New York Times*, August 1, 2009, https://www.nytimes.com/2009/08/02/us/politics/02cyber.html.

[18] Bradley Graham, "Bush Orders Guidelines for Cyber-Warfare," *The Washington Post*, February 7, 2003, https://www.washingtonpost.com/archive/politics/2003/02/07/bush-orders-guidelines-for-cyber-warfare/dd8b4a18-140c-4690-88a5-0041d4ce1b1c/; Jarrett Murphy, "Bush Wants Cyber Warfare Rules," *CBS*, February 7, 2003, https://www.cbsnews.com/ news/bush-wants-cyber-warfare-rules.

[19] Vincent Manzo, "Stuxnet and the Dangers of Cyberwar," *The National Interest*, January 29, 2013, https://nationalinterest.org/commentary/stuxnet-the-dangers-cyberwar-8030.

[20] Markoff and Shanker, "Halted": "The cyberwarriors are held back by extremely restrictive rules of engagement."

[21] Michael V. Hayden, "The Future of Things Cyber," *Strategic Studies Quarterly* 5, no. 1 (Spring 2011): 3; In Hayden: "Rarely has something been so important and so talked about with less clarity and less apparent understanding [than cyber security]. . . I have sat in very small group meetings in Washington . . . unable (along with my colleagues) to decide on a course of action because we lacked a clear picture of the long-term legal and policy implications of any decision we might make."

[22] Markoff and Shanker, "Halted": "But what kinds of cyberattacks count as force is a hard question, because force is not clearly defined."

[23] Markoff and Shanker, "Two traditional military limits now are being applied to cyberwar: proportionality, which is a rule that, in layman's terms, argues that if you slap me, I cannot blow up your house; and collateral damage, which requires militaries to limit civilian deaths and injuries." "Defense Department officials and military officers directly involved in planning for the Pentagon's new 'cybercommand' acknowledge that the risk of collateral damage is one of their chief concerns." "'We are deeply concerned about the second- and third-order effects of certain types of computer network operations, as well as about laws of war that require attacks be proportional to the threat,' said one senior officer."

[24] John Markoff, "Before the Gunfire, Cyberattacks," *The New York Times*, August 12, 2008, https://www.nytimes. com/2008/08/13/technology/13cyber.html.

[25] "Equation Group: The Crown Creator of Cyber-Espionage," *Kaspersky Lab*, February 16, 2015, https://www. kaspersky.com/about/press-releases/2015_equation-group-the-crown-creator-of-cyber-espionage; See also: "Equation Group," *Council on Foreign Relations*, https://www.cfr.org/cyber-operations/equation-group.

[26] Dan Goodin, "How 'Omnipotent' Hackers Tied to NSA Hid for 14 Years—and Were Found at Last," *ARS Technica*, February 16, 2015, https://arstechnica.com/information-technology/2015/02/how-omnipotent-hackers -tied-to-the-nsa-hid-for-14-years-and-were-found-at-last/.

[27] Dan Goodin, "'Omnipotent' Hackers."

[28] "Equation: The Death Star of Malware Galaxy," *Kaspersky Lab*, February 16, 2015, https://securelist.com/ equation-the-death-star-of-malware-galaxy/68750/.
[29] See: Nicole Perlroth, *This is How They Tell Me the World Ends: The Cyberweapons Arms Race* (Bloomsbury Publishing, 2021).
[30] "PPD-20: US Cyber Operations Policy."
[31] Manzo, "Stuxnet;" David E. Sanger, "Obama Order Sped Up Wave of Cyberattacks Against Iran," *The New York Times*, June 1, 2012, https://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of- cyberattacks-against-iran.html.
[32] Sanger, "Obama Order."
[33] Manzo, "Stuxnet."
[34] Manzo, "Stuxnet."
[35] Vivian Yeo, "Stuxnet Infections Spread to 115 Countries," *ZDNet*, August 9, 2010, https://www.zdnet.com/ article/stuxnet-infections-spread-to-115-countries/.
[36] Andrea Shalal-Esa, "Iran Strengthened Cyber Capabilities After Stuxnet: US General," *Reuters*, January 17, 2013, https://www.reuters.com/article/us-iran-usa-cyber/iran-strengthened-cyber-capabilities-after-stuxnet-u-s- general-idUSBRE90G1C420130118.
[37] Executive Office of the President of the United States, "International Strategy for Cyberspace," May 2011, https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.
[38] United States Department of Defense, "Department of Defense Strategy for Operating in Cyberspace," July 2011, https://csrc.nist.gov/CSRC/media/Projects/ISPAB/documents/DOD-Strategy-for-Operating-in-Cyberspace .pdf.
[39] United States Department of Defense, "Department of Defense Cyberspace Policy Report," November 2011, https://www.hsdl.org/?view&did=692701; Ellen Nakashima, "Pentagon: Cyber Offense Part of US Strategy," *The Washington Post*, November 15, 2011, https://web.archive.org/web/20131005000741/http:/articles.washington post.com/2011-11-15/news/35284321_1_cyberspace-new-report-cyberwarfare.
[40] "PPD-20: US Cyber Operations Policy."
[41] "PPD-20: US Cyber Operations Policy."
[42] "PPD-20: US Cyber Operations Policy," 10.
[43] "PPD-20: US Cyber Operations Policy."
[44] David E. Sanger, "US Cyberattacks Target ISIS in a New Line of Combat," *The New York Times*, April 25, 2016, https://www.nytimes.com/2016/04/25/us/politics/us-directs-cyberweapons-at-isis-for-first-time.html. In Sanger, "US Cyberattacks": "The NSA has spent years penetrating foreign networks . . . placing thousands of implants in those networks to allow it to listen in. But those implants can be used to manipulate data or to shut down a network. That frequently leads to a battle between the NSA civilians—who know that to make use of an implant is to blow its cover—and the military operators who want to strike back. NSA officials complained that once the implants were used to attack, the Islamic State militants would stop the use of a communications channel and perhaps start one that was harder to find, penetrate or de-encrypt."
[45] "PPD-20: US Cyber Operations Policy," 9–10.
[46] "PPD-20: US Cyber Operations Policy."
[47] The restrictiveness of PPD-20 bore out in practice. According to a senior DoD official speaking on the condition of anonymity in 2019, ". . . in 8, 9, 10 years under the old decision process, I can count on less than two fingers the number of operations conducted." Mark Pomerleau, "New Authorities Mean Lots of New Missions at Cyber Command," *Fifth Domain*, May 8, 2019, https://www.fifthdomain.com/dod/cybercom/2019/05/ 08/new-authorities-mean-lots-of-new-missions-at-cyber-command/.
[48] James R. Clapper, "Statement for the Record: Worldwide Threat Assessment of the US Intelligence Community," statement to Senate Armed Services Committee, March 12, 2013, https://www.dni.gov/files/documents/Intelligence%20Reports/2013%20ATA%20SFR%20for%20SSCI%2012%20Mar%202013.pdf
[49] United States Department of Defense, "The Department of Defense Cyber Strategy 2015," April 2015, https://www.hsdl.org/?view&did=764848.

[50] Office of the Director of National Intelligence, "Joint Statement From DoJ, DoD, DHS, DNI, FBI, NSA, and CISA on Ensuring Security of 2020 Elections," press release, November 5, 2019, https://www.dni.gov/index.php /newsroom/press-releases/press-releases-2019/item/2063-joint-statement-from-doj-dod-dhs-dni-fbi-nsa-and-cisa-on-ensuring-security-of-2020-elections.
[51] Homeland Security Enterprise Forum 2021, "Plenary Session 2."
[52] "Denial of Service Attacks Against US Banks in 2012–2013," *Council on Foreign Relations*, September 2012, https://www.cfr.org/cyber-operations/denial-service-attacks-against-us-banks-2012–2013.
[53] Ellen Nakashima, "Why the Sony Hack Drew an Unprecedented US Response Against North Korea," *The Washington Post*, January 15, 2015, https://www.washingtonpost.com/world/national-security/why-the-sony- hack-drew-an-unprecedented-us-response-against-north-korea/2015/01/14/679185d4-9a63-11e4-96cc-e858eba91ced_story.html; David E. Sanger, "US Decides to Retaliate Against Chinese Hacking," *The New York Times*, July 31, 2015, https://www.nytimes.com/2015/08/01/world/asia/us-decides-to-retaliate-against-chinas-hacking.html.
[54] Sanger, "US Decides to Retaliate."
[55] Ellen Nakashima, "US Won't Impose Sanctions on Chinese Companies Before Xi Visit," *The Washington Post*, September 14, 2015, https://www.washingtonpost.com/world/national-security/the-us-will-not-impose-sanctions- on-chinese-companies-before-state-visit-by-president-xi-jinping/2015/09/14/98a447e6-5b25-11e5-b38e-06883aacba64_story.html.
[56] United States Department of Justice, "Grand Jury Indicts 12 Russian Intelligence Officers for Hacking Offense Related to the 2016 Election," news release, July 13, 2019, https://www.justice.gov/opa/pr/grand-jury- indicts-12-russian-intelligence-officers-hacking-offenses-related-2016-election.
[57] David Corn and Michael Isikoff, "'Why the Hell Are We Standing Down,'" *Mother Jones*, March 9, 2018, https://www.motherjones.com/politics/2018/03/why-the-hell-are-we-standing-down/.
[58] "Obama also approved a previously undisclosed covert measure that authorized planting cyberweapons in Russia's infrastructure, the digital equivalent of bombs that could be detonated if the United States found itself in an escalating exchange with Moscow. The project, which Obama approved in a covert-action finding, was still in its planning stages when Obama left office. It would be up to President Trump to decide whether to use the capability," in Greg Miller, et al., "Obama's Secret Struggle to Retaliate Against Putin's Election Interference," *The Washington Post*, June 23, 2017, https://www.washingtonpost.com/graphics/2017/world/national-security/obama-putin-election-hacking/?utm_term=.beefe1bc6df2&itid=lk_inline_manual_2; see also: Austin Carson, "Obama Used Covert Retaliation in Response to Russian Election Meddling. Here's Why," *The Washington Post*, June 29, 2017, https://www.washingtonpost.com/news/monkey-cage/wp/2017/06/29/obama-used-covert- retaliation-in-response-to-russian-election-meddling-heres-why/.
[59] Garrett Hinck and Tim Mauer, "What's the Point of Charging Foreign State-Linked Hackers?," *Lawfare*, May 24, 2019, https://www.lawfareblog.com/whats-point-charging-foreign-state-linked-hackers.
[60] Allison Peters and Pierce MacConaghy, "Unpacking US Cyber Sanctions," *Third Way*, January 29, 2021. https://www.thirdway.org/memo/unpacking-us-cyber-sanctions.
[61] Hinck and Mauer, "What's the Point;" Peters and MacConaghy, "Unpacking US Cyber Sanctions."
[62] James R. Clapper, "Statement for the Record: Worldwide Threat Assessment of the US Intelligence Community," statement to Senate Armed Services Committee, February 26, 2015, https://www.dni.gov/files/ documents/Unclassified_2015_ATA_SFR_-_SASC_FINAL.pdf; James R. Clapper, "Statement for the Record: Worldwide Threat Assessment of the US Intelligence Community," statement to Senate Armed Services Committee, February 9, 2016, https://www.dni.gov/files/documents/SASC_Unclassified_2016_ATA_SFR_ FINAL.pdf.
[63] Clapper, 2016. Also noted the risk of software/ICT supply chain manipulation, risks to operational technologies (for example, IOT devices and industrial control systems where technologies are used to control physical systems), and artificial intelligence.
[64] David Sanger, "U.S. Decides to Retaliate Against China's Hacking," *The New York Times*, July 31, 2015, https://www.nytimes.com/2015/08/01/world/asia/us-decides-to-retaliate-against-chinas-

hacking.html; In Sanger, "U.S. Decides to Retaliate": "Mr. Clapper predicted that the number and sophistication of hacking aimed at the United States would worsen 'until such time as we create both the substance and psychology of deterrence.'"
Ron Rosenbaum, "Richard Clarke on Who Was Behind the Stuxnet Attack," *Smithsonian Magazine*, April 2012, https://www.smithsonianmag.com/history/richard-clarke-on-who-was-behind-the-stuxnet- attack-160630516/; In Rosenbaum, "Richard Clarke": "We are being failed again, being left defenseless against a cyberattack that could bring down our nation's entire electronic infrastructure, including the power grid, banking and telecommunications, and even our military command system. . . 'I think we're living in the world of non-response. . . Where you know that there's a problem, but you don't do anything about it. If that's denial, then that's denial.'"
Nicole Perlroth, "Are We Waiting for Everyone to Get Hacked?," *The New York Times*, June 5, 2021, https://www.nytimes.com/2021/06/05/business/leon-panetta-cyber-attacks.html?action=click&module=Related Links&pgtype=Article; Leon Panetta in Perlroth, "Are We Waiting": "It's like there's a fire and you're ringing a bell, but the fire department doesn't show."
Jack Goldsmith, "Disconcerting US Cyber Deterrence Troubles Continue," *Lawfare*, September 15, 2015, https://www.lawfareblog.com/disconcerting-us-cyber-deterrence-troubles-continue/; in Goldsmith, "Disconcerting": "Why is the US government not treating the . . . digital threat as a core national security interest? Why has it not yet chosen to make this (in the President's words) 'an area of competition' with [our adversaries]? And why can't it come up with a credible deterrence strategy."
Clint Watts, "Russia is Hammering the U.S. in Cyberspace, Why is Biden Meeting with Putin at All?," Foreign Policy Research Institute, June 14, 2021, https://www.fpri.org/article/2021/06/russia-is-hammering-the-u-s-in-cyberspace-why-is-biden-meeting-with-putin-at-all/; in Watts, "Russia is Hammering the U.S.": "Why don't we fight back? Why don't we do a counterattack?. . . America's decade of conventional wisdom on cyberspace has led to a crisis. Not a cyber "Pearl Harbor," but an untreated cyber "cancer" that slowly cripples American society."
Susan B. Glasser, "How Top US Diplomat Pushed Back Against Russian Hacking," *Politico*, February 5, 2018, https://www.politico.eu/article/ russia-hacking-victoria-nuland-the-hairs-really-went-up-on-the-back-of-our-necks/.
See my own pushback against the US response to Russian election meddling in Corn and Isikoff, "Standing Down."
[65] Daniel R. Coats, "Statement for the Record: Worldwide Threat Assessment of the US Intelligence Community," statement to Senate Select Committee on Intelligence, May 11, 2017, https://www.dni.gov/files/ documents/Newsroom/Testimonies/SSCI%20Unclassified%20SFR%20-%20Final.pdf.
[66] Daniel R. Coats, "Statement for the Record: Worldwide Threat Assessment of the US Intelligence Community," statement to Senate Select Committee on Intelligence, January 29, 2019, https://www.dni.gov/ files/ODNI/documents/2019-ATA-SFR---SSCI.pdf.
[67] Office of the Director of National Intelligence, "Annual Threat Assessment of the Intelligence Community," April 9, 2021, https://www.dni.gov/files/ODNI/documents/assessments/ATA-2021-Unclassified-Report.pdf;
[68] Perlroth, "How the US Lost."
[69] Pomerleau, "New Authorities."
[70] "DOD Fact Sheet: Cyber Mission Force," *US Army Cyber Command*, February 10, 2020, https://www.arcyber. army.mil/Info/Fact-Sheets/Fact-Sheet-View-Page/Article/2079594/dod-fact-sheet-cyber-mission-force/.
[71] Sean Lawson, et al., "Dropping the Cyber Bomb? Spectacular Claims and Unremarkable Effects," *Council on Foreign Relations*, May 24, 2016, https://www.cfr.org/blog/dropping-cyber-bomb-spectacular-claims-and- unremarkable-effects; "Joint Task Force ARES and Operation GLOWING SYMPHONY: Cyber Command's Internet War Against ISIL," *National Security Archive*, August 13, 2018, https://nsarchive.gwu.edu/briefing-book/ cyber-vault/2018-08-13/joint-task-force-ares-operation-glowing-symphony-cyber-commands-internet-war-against-isil.
[72] Julian E. Barnes and Thomas Gibbons-Neff, "US Carried Out Cyberattacks on Iran," *The New York Times*, June 22, 2019, https://www.nytimes.com/2019/06/22/us/politics/us-iran-cyber-attacks.html.

[73] David E. Sanger and Nicole Perlroth, "US Escalates Online Attacks on Russia's Power Grid," *The New York Times*, June 15, 2019, https://www.nytimes.com/2019/06/15/us/politics/trump-cyber-russia-grid.html.
[74] Marshall Cohen, "37 Times Trump Was Soft on Russia," *CNN*, August 4, 2020, https://www.cnn.com/2019/ 11/17/politics/trump-soft-on-russia/index.html.
[75] Brad D. Williams, "Nakasone: Cold War-Style Deterrence 'Does Not Comport to Cyberspace,'" *Breaking Defense*, November 4, 2021, https://breakingdefense.com/2021/11/nakasone-cold-war-style-deterrence-does- not-comport-to-cyberspace/; Brad D. Williams, "Meet the Scholar Challenging the Cyber Deterrence Paradigm," *Fifth Domain*, July 19, 2017, https://www.fifthdomain.com/home/2017/07/19/meet-the-scholar-challenging-the- cyber-deterrence-paradigm/.
[76] Garrett M. Graff, "China's Hacking Spree Will Have a Decades-Long Fallout," *Wired*, February 11, 2020, https://www.wired.com/story/china-equifax-anthem-marriott-opm-hacks-data/.
[77] United States Department of Defense, "Summary: Department of Defense Cyber Strategy," September 18, 2018, https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF; United States Cyber Command, "Achieve and Maintain Cyberspace Superiority: Command Vision for US Cyber Command," April 2018, https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf
[78] Robert Chesney, "The Law of Military Cyber Operations and the New NDAA," *Lawfare*, July 26, 2018, https://www.lawfareblog.com/law-military-cyber-operations-and-new-ndaa. See also: Pomerleau, "New Authorities."
[79] Michael P. Fischerkeller and Richard J. Harknett, "Persistent Engagement and Tacit Bargaining: A Path Toward Constructing Norms in Cyberspace," *Lawfare*, November 9, 2018, https://www.lawfareblog.com/ persistent-engagement-and-tacit-bargaining-path-toward-constructing-norms-cyberspace.
[80] Brad D. Williams, "CYBERCOM Has Conducted 'Hunt-Forward' Ops in 14 Countries, Deputy Says," *Breaking Defense*, November 10, 2021, https://breakingdefense.com/2021/11/cybercoms-no-2-discusses-hunt-forward- space-cybersecurity-china/; Ellen Nakashima and Craig Timberb, "US Agencies Mount Major Effort to Prevent Russian Interference in the Election Even Though Trump Downplays Threat," *The Washington Post*, October 21, 2021, https://www.washingtonpost.com/national-security/us-defends-russian-election-interference/2020/10/21/ 533b508a-130a-11eb-bc10-40b25382f1be_story.html; Joseph Marks, "Four Takeaways from the Iranian Election Interference Indictments," *The Washington Post*, November 19, 2021, https://www.washingtonpost.com/ politics/2021/11/19/four-takeaways-iranian-election-interference-indictments/.
[81] Patrick O'Neill, "How China's Attack on Microsoft Escalated into a 'Reckless' Hacking Spree," *MIT Technology Review*, March 10, 2021, https://www.technologyreview.com/2021/03/10/1020596/how-chinas-attack-on-microsoft-escalated-into-a-reckless-hacking-spree/
[82] Dina Temple-Raston, "A 'Worst Nightmare' Cyberattack: The Untold Story of the SolarWinds Hack," *NPR*, April 16, 2021, https://www.npr.org/2021/04/16/985439655/a-worst-nightmare-cyberattack-the-untold-story-of-the-solarwinds-hack
[83] Tarah Wheeler, "The Danger in Calling the SolarWinds Breach an 'Act of War,'" *Brookings*, March 4, 2021, https://www.brookings.edu/techstream/the-danger-in-calling-the-solarwinds-breach-an-act-of-war/.
[84] Joe Warminsky, "SolarWinds Attack Is Not 'Espionage as Usual,' Microsoft President Says," *CyberScoop*, December 18, 2020, https://www.cyberscoop.com/microsoft-brad-smith-solarwinds/.
[85] David E. Sanger, "After Russian Cyberattack, Looking for Answers and Debating Retaliation," *The New York Times*, February 23, 2021, https://www.nytimes.com/2021/02/23/us/politics/solarwinds-hack-senate-intelligence -russia.html?action=click&module=RelatedLinks&pgtype=Article.
[86] David E. Sanger, et al., "Preparing for Retaliation Against Russia, US Confronts Hacking by China," *The New York Times*, March 7, 2021, https://www.nytimes.com/2021/03/07/us/politics/microsoft-solarwinds-hack-russia-china. html.
[87] Tracy Wilkinson and Chris Megerian, "Biden Sanctions Russia for SolarWinds Hack and Election Attack," *Los Angeles Times*, April 14, 2021, https://www.latimes.com/world-nation/story/2021-04-14/months-after-hack-us- poised-to-announce-sanctions-on-russia.

[88] David E. Sanger and Andrew E. Kramer, "US Imposes Stiff Sanctions on Russia, Blaming It for Major Hacking Operation," *The New York Times*, April 15, 2021, https://www.nytimes.com/2021/04/15/world/europe/ us-russia-sanctions.html?action=click&module=RelatedLinks&pgtype=Article; see also: Bret Stephens, "America's Crumbling Global Position, *The New York Times*, October 26, 2021, https://www.nytimes.com/2021/ 10/26/opinion/us-military-russia-china-iran.html.

[89] David E. Sanger, "Ignoring Sanctions, Russia Renews Broad Cybersurveillance Operation," *The New York Times*, October 25, 2021, https://www.nytimes.com/2021/10/25/us/politics/russia-cybersurveillance-biden.html.

[90] Sanger, "Ignoring Sanctions."

[91] Joseph Marks, "The Cybersecurity 202: The US and Allies Are Taking a Stand Against Chinese Hacking. Here Are Three Takeaways," *The Washington Post*, July 19, 2021, https://www.washingtonpost.com/politics/2021/ 07/19/cybersecurity-202-us-allies-are-taking-stand-against-chinese-hacking-here-are-three-takeaways/.

[92] "Executive Order 14028 of May 12, 2021, Improving the Nation's Cybersecurity," *Code of Federal Regulations*, title 3 (2021): 26633-26647, https://www.federalregister.gov/documents/2021/05/17/2021-10460 /improving-the-nations-cybersecurity. White House Executive Order 14028 requires all federal departments and agencies to implement "zero trust" protections or networks systems and data and to do better and faster technical analysis of log data from the organization's IT systems; Katie Bo Lillis, "Biden Administration Ramps Up Efforts to Secure American Infrastructure from Russian and Chinese Cyberattacks," *CNN*, October 10, 2021, https://www.cnn.com/2021/10/10/politics/biden-secure- infrastructure-cyberattacks/index.html.

[93] "CISA Issues Guidance on Evicting Adversaries from Networks Following SolarWinds Attack," *HIPAA Journal*, May 18, 2021, https://www.hipaajournal.com/cisa-issues-guidance-on-evicting-adversaries-from-networks-following-solarwinds-attacks/.

[94] Lillis, "Biden Administration Ramps Up Efforts."

[95] Sean Michael Kerner, "Most Organizations Not Engaging in Threat Hunting, Fidelis Finds," *eWeek*, October 26, 2018, https://www.eweek.com/security/most-organizations-not-engaging-in-threat-hunting-fidelis-reports/.

[96] While this might seem problematic on its face, NSA cyber experts have in the past supported a number of cyber response efforts after breaches of federal IT systems, acting domestically under the authority of DHS and the FBI.

[97] "Limiting Foreign Meddling in US Campaigns," *Brennan Center for Justice*, August 14, 2019, https://www.brennancenter.org/our-work/analysis-opinion/limiting-foreign-meddling-us-campaigns; Maggie Miller, "Lawmakers Introduce Bill Targeting Foreign Disinformation on Social Media," *The Hill*, October 1, 2020, https://thehill.com/policy/cybersecurity/519247-lawmakers-introduce-bill-targeting-foreign-disinformation-on- social; Nathaniel Persily and Joshua A. Tucker, "How to Fix Social Media? Start with Independent Research," *Brookings*, December 1, 2021, https://www.brookings.edu/research/how-to-fix-social-media-start-with-independent-research/.

[98] Andy Greenberg, "US Hackers' Strike on Russian Trolls Sends a Message—but What Kind," *Wired,* February 27, 2019*,* https://www.wired.com/story/cyber-command-ira-strike-sends-signal/.

[99] Karen Hao, "Troll Farms Reached 140 Million Americans a Month on Facebook Before 2020 Election, Internal Report Shows," *MIT Technology Review*, September 16, 2021, https://www.technologyreview.com/2021 /09/16/1035851/facebook-troll-farms-report-us-2020-election/; see: "10 Ideas to Fix Democracy," *Foreign Policy*, January 7, 2022, https://foreignpolicy.com/2022/01/07/10-ideas-fix-democracy/; see also: Elise Thomas, et al., "The Challenges of Countering Influence Operations," *Carnegie Endowment for International Peace*, https://carnegieendowment.org/2020/06/10/challenges-of-countering-influence-operations-pub-82031.

[100] Congressional votes on the 2019 NDAA (359–54 in the House and 87–10 in the Senate) do indicate strong bipartisan support for tougher cyber defense through an increased reliance on cyber effects operations. Congress.gov, "H.R.5515–115th Congress (2017–2018): John S. McCain National Defense Authorization Act for Fiscal Year 2019," August 13, 2018, https://www.congress.gov/bill/115th-congress/house-bill/5515/actions.