Stanford | Center for International Security and Cooperation
Freeman Spogli Institute

Emerging Technology & The Future of The National Security Council

STANFORD UNIVERSITY

Brendan McCord[1] and Zoe A. Y. Weinberg[2]

Center for International Security and Cooperation,
Freeman Spogli Institute for International Studies, Stanford University

ABSTRACT

Rapid and profound advances in hardware and software, paired with the global shift to digitally-networked communications and transactions, have transformed the economic and security landscape. They have introduced new risks to personal safety and national security, fueled a strategic competition between the United States and China, and increased collective vulnerability to malicious states and non-state actors armed with cheaper, more effective, and difficult-to-attribute tools. The nature of the challenges posed by novel technologies has rendered our legacy tools for understanding and addressing national security risks outmoded and misaligned with the changing geopolitical landscape.

The National Security Council (NSC)—the most influential foreign policy decision-making body in the executive branch—is still playing catch-up. While the last two administrations have made commendable efforts to modernize the NSC, its structure and skillset continue to reflect an anachronistic picture of the critical threats facing the United States, failing to capture or address the mounting vulnerabilities posed by emerging technology.

As the Trump administration draws to a close, the new national security establishment has an opportunity to reexamine existing paradigms and approaches in light of the evolving threat landscape. Drawing from over 25 interviews with current and former NSC staffers, interagency personnel, national security professionals, policymakers, and academics, this report offers several policy options for restructuring the NSC to better respond to technological developments that impact national security.

---

[1] Former HQE/SGE and technology entrepreneur. Author of the Department of Defense Artificial Intelligence Strategy, founder of the Joint Artificial Intelligence Center, head of Machine Learning at Defense Innovation Unit, and Adjunct Senior Fellow at the Center for a New American Security.

[2] Fellow, Schmidt Futures. J.D., Yale Law School (2020), M.B.A., Stanford Graduate School of Business (2020), National Security Commission on Artificial Intelligence, Google AI.

CONTENTS

INTRODUCTION

The Changing Face of Security

Accelerating change across diverse forms of technology is fundamentally altering the security landscape. Rapid and profound advances in hardware and software, paired with the global shift to digitally-networked communications and transactions, have transformed the economic and security landscape, along with the fabric and rhythm of daily life. They have also introduced new risks to personal safety and national security, fueled a strategic competition between the United States and China, and increased collective vulnerability to malicious states and non-state actors armed with cheaper, more effective, and difficult-to-attribute tools.

Technology has long played a part in defining the security landscape, and leadership in technological innovation historically has been a crucial national security asset of the United States. The development and introduction of weapons such as modern small arms, nuclear weapons, stealth technology, and guided missiles altered the security equation and in some instances, transformed international relations.[3] Other, more prosaic civilian technologies have also had significant consequences for national security, including electricity, the combustion engine, the airplane, the global positioning system (GPS), and the internet. In each instance, national security policymakers had to take stock of their approach, reexamine existing theories and practices of warfare, and determine how organizations and strategies ought to adapt in light of new tools.

Examples of profound technological change include recent breakthroughs in artificial intelligence (AI)—specifically in the subfield of AI known as machine learning (ML)—which are enabling computers to interpret and understand the visual world, process and synthesize language, control autonomous vehicles, beat elite human players in sophisticated games, or automate tasks from the mundane to the creative, while exacerbating concerns of ubiquitous surveillance, technological unemployment, and

[3] For a robust history of technology and war, see, e.g., Barton C. Hacker & Margaret Vining, *American Military Technology* (2007); Timothy Moy, *War Machines: Transforming Technology in the U.S. Military 1920-1940* (2001); Alex Roland, *War and Technology* (2016); Alex Roland, *Strategic Computing: DARPA and the Quest for Machine Intelligence 1983-1993* (2002); Barton C. Hacker, *The Machines of War: Western Military Technology 1850-2000*, 21 History and Technology 3 (Sept. 2005); Warren Chin, *Technology, War and the State: Past, Present and Future*, 95 International Affairs 4 (July 2019).

geopolitical conflict. Beyond AI, there has been an explosion of activity in space and satellite technology, hypersonics, synthetic biology, cryptocurrencies, blockchain, quantitative social science, quantum computing, 3D printing, and telecommunications technology such as fifth generation (5G) broadband cellular networks. These breakthroughs undoubtedly have consequences for U.S. economic competitiveness, but also threaten to dissolve the mortar in the bricks of the current U.S. national security apparatus.

We are witnessing early consequences in real time. In 2014, groups such as al-Qaeda and the Islamic State of Iraq and Syria (ISIS) used online communication on Facebook, Twitter, YouTube, and other platforms to increase their prominence, recruit collaborators, and maximize the emotional impact of their efforts. The same year, an attack allegedly sponsored by the government of North Korea bombarded Sony Pictures by leaking thousands of personal emails and intellectual property, and erasing computer infrastructure. In 2016, Russia used coordinated campaigns of propaganda and disinformation along with cyber-attacks to meddle in the U.S. presidential election. And today, the United States finds itself in the midst of a stand-off with China on numerous fronts, from threats to ban technology exports such as the wildly popular social media app TikTok, to competition over who will build the backbone of the internet, to control over COVID-19 pandemic narratives that have been corrupted by disinformation and misinformation.

The impact of technology on national security is wide-ranging, spanning the military and intelligence revolution, economic competitiveness, and the future of democracy. In particular, the complex relationship between economic and security issues arising from new technology has also introduced difficult tradeoffs that the NSC structure was never designed to undertake. The buildout of 5G infrastructure, for example, has important consequences for both national competitiveness and economic power, which is both part of and orthogonal to the security equation. Decisions about trade and export controls are now more intimately connected to security decision-making than ever before.

While technological developments have always shaped the nature of global threats and the evolution of the security landscape, the scale, velocity, and potential impact of emerging technology is unprecedented. Many of the challenges we face today are not only *facilitated by* advances in technology—such as developments in weapons capabilities or shifts in the underlying geopolitical balance of power—but present new

risks *in and of themselves*, as in the case of information operations, cyber-attacks, or genetically-engineered biological threats.

Furthermore, the pace of evolution today is faster than ever before.[4] As a result, technological innovations represent a constantly moving target. In the past, a technological breakthrough was often followed by a period of relative stability, giving policymakers and regulators a chance to play catch-up in developing new rules of the road. Today, techniques and methods associated with certain technologies—for example, natural language processing—are rapidly and constantly evolving, making it particularly difficult for policymakers to master an area of expertise.

In addition, many present-day innovations are "born open" rather than "born secret."[5] In the past, major advancements in military technology were generated in government labs or under government direction, required access to tightly-controlled physical resources or advanced manufacturing capabilities, and were classified in nature (hence the "born secret" designation). These attributes defined where and how the technological breakthroughs could be introduced and applied.

By contrast, recent innovations in areas such as machine learning are available on open-source platforms from day one. These innovations frequently occur in software rather than hardware, and therefore do not require sophisticated manufacturing to replicate and distribute. Their development increasingly takes place outside government, with civilians at the helm in developing new tools, often absent context on their potential security implications. Their access has become largely democratized, with potent technologies available to anyone with a computer and internet connection (with compute availability being a limiting factor for activities such as the development of large machine learning models). While some emerging technologies require specialized expertise and/or significant resources—such as quantum computing, hypersonics, 5G hardware, and synthetic biology—many of the innovations that pose the biggest risks (e.g., automated fake identities that spread disinformation, facial recognition that supports ubiquitous surveillance technologies, or malware that facilitates cyberattack) have diminishing barriers to entry and are inexpensive to proliferate. As a result, the threats enabled by technology developments in this new

[4] Paul Scharre, *Making Sense of Rapid Technological Change*, Center for a New American Security (July 19, 2018), https://www.cnas.org/publications/commentary/making-sense-of-rapid-technological-change.
[5] Amy Zegart, interview by author, Sept. 10, 2019.

paradigm seem poised to become cheaper, more effective, and more difficult to attribute.[6]

Geopolitical competition is evolving in response. The character of military and economic rivalry is shifting so profoundly that our old tools for understanding and fighting appear increasingly misaligned with the new reality of global competition. While kinetic combat will always remain a component of warfare, the next generation of weapons has expanded to include technological control, human rights-abusing technological surveillance, and information access. Increasingly, hostilities will take the shape of information operations, stolen intellectual property, cyber-attacks, and the undermining of democratic institutions. The new security landscape is particularly expedient to adversaries who benefit from certain asymmetric advantages—such as quantities of data, demographic trends, and autocratic control over information flow—creating an environment ever more hospitable to authoritarian ideology and regimes.

The world is also experiencing a period of renewed great power competition and, simultaneously, devolution of power away from state actors toward powerful non-state groups, corporations, and super-empowered individuals. Escalating friction with China and Russia has come to define this moment in foreign policy, with scholars heralding a new era of geostrategic rivalry that may permanently transform the global world order.[7] Yet, in other regards, the centers of power within the international system are becoming increasingly distributed, privatized, and transnational. These crosscurrents form a complex backdrop to the innovation race.

An Opportunity for Upgrade

Since the end of the Cold War, U.S. national security policy and, in turn, the approach of the NSC has rested on a series of assumptions about how conflicts unfold, from the

[6] The more fundamental question of whether new technology will endanger or reinforce strategic stability is an area of emerging scholarship. In some instances, it appears that the introduction of new technology might escalate conflict by creating new vulnerabilities or power asymmetries in the global system, but in other cases enhanced technological ability appears to lead to greater deterrence and stability. While this question of international relations is an area ripe for research and scholarship, it is outside the scope of this inquiry. See, e.g., Todd S. Sechser, Neil Narang, and Caitlin Talmadge, *Emerging Technologies and Strategic Stability in Peacetime, Crisis, and War*, Journal of Strategic Studies (Aug. 22, 2019); Jacquelyn Schneider, *The Capability/Vulnerability Paradox and Military Revolutions: Implications for Computing, Cyber, and the Onset of War*, Journal of Strategic Studies (Aug. 22, 2019).

[7] Elbridge A. Colby & A. Wess Mitchell, *The Age of Great-Power Competition*, Foreign Affairs (Jan./Feb. 2020), https://www.foreignaffairs.com/articles/2019-12-10/age-great-power-competition.

relevance of geographic clustering, to an emphasis on great power politics and defense spending as an indicator of military might, to common definitions of victory, to a lack of emphasis on low-intensity conflict and measures short of war, to a limited role for commercial or open-source innovation. The NSC's structure reflects those assumptions, with an enduring reliance on regional specialization and a functional separation of security from most domestic and economic policymaking.

The changes brought about by new technology challenge decades-old assumptions about how the national security enterprise ought to function and how it might be most effective. America's ability to respond to these challenges will depend on the integrity of our organizational structures. The institutions, processes, and sources of expertise on which the White House currently relies were designed for an earlier era, and are not well-suited for the cross-sectoral, transnational nature of new threats. The complexity and unique character of these new challenges warrant a rigorous re-evaluation of existing structures that comprise our security apparatus, and in particular, the National Security Council (NSC).[8] Neglect of these issues in its own structural design is leaving the United States at danger of falling behind; the countries that embrace this change and adapt their institutions to harness these new technologies will ultimately dominate those that do not.

As the most powerful decision-making body in our executive branch's security establishment, the NSC's institutional structure and priorities sets the stage for the rest of government. As we head into the Biden administration, a high-level review of our nation's security and presidential priorities is squarely on the table, presenting a unique opportunity to reexamine the NSC. Taking stock now better facilitates any required re-engineering with the inauguration of a new administration in January 2021.[9]

In addition, the COVID-19 outbreak has prompted a broader reassessment of the scope and meaning of national security. Just as the Cuban Missile Crisis prompted a fixation on arms control and September 11 gave rise to a counterterrorism-centric strategy, COVID-19 may bring about a new era of national security, with biological and other

[8] Of course, institutional structure is not dispositive; mishandling of tech-related national security threats can be attributed to a wide variety of factors, including reluctance to interfere in markets, Congressional dysfunction, opposition from allies or private sector players, and so on.
[9] Historically new presidents issue a National Security Policy Memorandum to organize the NSC.

transnational threats such as climate change at the center.[10] While this report focuses primarily on the dilemmas posed by new technological developments, some of its lessons and conclusions similarly apply to other threats that frequently are marginalized in national security conversations, including global health concerns. Like new technological threats, a pandemic represents an unconventional and unprecedented peril that requires a broader reconceptualizing of the contours of defense.

Past examinations of the NSC have focused on enduring organizational challenges: the constant deluge of information and the "tyranny of the inbox"[11]; the growth of the size of the staff[12]; the consolidation and centralization of power[13]; and the difficulty of dedicating resources to long-term strategic planning.[14] This report does not weigh in substantively on these long-standing debates, but instead focuses more narrowly on the question of how the NSC might be better-designed to address threats posed by emerging technology, broadly defined.[15]

Drawing from more than 25 interviews with current and former NSC staffers, interagency personnel, national security professionals, policymakers, and academics,[16] this report offers several policy options for restructuring the NSC to better respond to

[10] In many ways, such a shift would be a return to the agenda of the Obama NSC, which had actively bolstered its global health focus and climate focus over time. See also, David E. Sanger, *Analysis: Will Pandemic Make Trump Rethink National Security?*, N.Y. Times (April 15, 2020).

[11] *See, e.g.*, Shawn Brimley, Dr. Dafna H. Rand, Julianne Smith, and Jacob Stokes, *Enabling Decision: Shaping the National Security Council for the Next President*, Center for a New American Security (June 2015).

[12] Mark Cancian, *Limiting Size of NSC Staff*, Assessing Defense Reform (July 1, 2016); I. M. Destler & Ivo H. Daalder, *A New NSC for a New Administration*, Brookings (Nov. 2000); Kim R. Holmes, *Memo to a New President: How Best to Organize the National Security Council*, Heritage Foundation (Apr. 14, 2016).

[13] *See, e.g.,* Derek Chollet, *The National Security Council: Is it Effective, or Is It Broken?*, Oxford Handbook of U.S. National Security (July 2018).

[14] *Id.*

[15] Of course, the reforms considered as part of this analysis do intersect with the issues of staff size and the balance between daily operational work versus long-term strategic planning. However, this examination focuses more directly on the implications of structure for tackling emerging technology-related threats, rather than on the implications for the NSC's workflow or effectiveness as a whole.

[16] The authors would like to thank the following individuals for offering their insight and perspectives to this report: David Agronovitch, Salman Ahmed, Tess Bridgeman, Tarun Chhabra, David Cohen, Ivo Daalder, R. David Edelman, John Gans, Andrew Grotto, Avril Haines, William Happer, Colin Kahl, Thomas Kalil, Christopher Kirchhoff, Amb. Michael McFaul, Gen. H. R. McMaster, Chris Meserole, Jeffrey Prescott, Nadia Schadlow, Paul Scharre, Michael Sekora, Matthew Spence, Anthony Vinci, Sec. Robert Work, and Amy Zegart.

developments in conflict. Interviewees represented a diverse array of perspectives, with strong and differing opinions on every issue. Our research sought to surface the best ideas and to probe key concerns, while recognizing that not all trade-offs will be satisfyingly balanced, nor disagreements resolved. Our intention is for this report to initiate discussion by serving as both snapshot of the current challenges faced by our national security enterprise and a blueprint for thinking through how to solve them.

I. THE ROLE OF THE NATIONAL SECURITY COUNCIL

The National Security Council represents the single most important foreign policy decision-making body in our government. Charged with advising the President on matters of military strategy, statecraft, and diplomacy, the NSC serves as the primary coordinating hub for the executive branch. It is responsible for collating inputs from the government's vast array of intelligence and defense bodies; crafting short- and long-term strategy; and coordinating implementation among agencies. Given its oversight role and the broad scope of its duties, it is imperative that the NSC itself be thoughtfully designed to identify and tackle novel challenges as they emerge and develop over the horizon. Any structural weaknesses or flaws at the NSC may have far-reaching consequences, as lapses at the top reverberate down the executive branch hierarchy and across government.

The NSC has evolved over time from an informal group of personal presidential advisors and clerical support staff to a collection of key foreign principals and in-house experts. When it was established by the National Security Act of 1947, the NSC was charged with three primary activities:

> (1) to advise the President with respect to the integration of domestic, foreign, and military policies relating to the national security so as to enable the Armed Forces and the other departments and agencies of the United States Government to cooperate more effectively in matters involving the national security;
>
> (2) to assess and appraise the objectives, commitments, and risks of the United States in relation to our actual and potential military power, in the interest of national security, for the purpose of making recommendations to the President in connection therewith;

(3) to consider policies on matters of common interest to the departments and agencies of the Government concerned with the national security, and to make recommendations to the President in connection therewith.[17]

The size and structure of the NSC has varied tremendously since its establishment. In 1991, the size of the staff totaled only about 40, but toward the end of the Obama administration the number approached 400, in part due to the merging of the Homeland Security Council and NSC in 2009 and an increase in support staff roles.[18] (The ballooning of the staff has been a preoccupation for many scholars, with both left- and right-wing commentators advocating for limitations on the size of the staff.[19]) Over time, the NSC has also taken on responsibilities that are arguably beyond the gamut of its originally intended function, becoming increasingly execution-focused rather than limiting itself to a coordination role.[20]

---

[17] The National Security Act of 1947 also created the Department of Defense (merging the War Department and Navy Department), the U.S. Air Force, the Joint Chiefs of Staff, and the Central Intelligence Agency. National Security Act of 1947, Pub.L. 80-253 (July 26, 1947), 80th. Cong. 1st Sess. Chs. 343, Sec. 101. The National Security Act was later amended to create a fourth responsibility: "[to] coordinate, without assuming operational authority, the United States Government response to malign foreign influence operations and campaigns." 50. U.S.C. § 3021(b)(4).

[18] Mark Cancian, *Limiting Size of NSC Staff*, Center for Strategic and International Studies (July 2016). Some have estimated that core policy staff always remained well below 100, suggesting that the increase in staff may not be as steep as other counts would suggest.

[19] Cancian helpfully documents a range of recommendations by policy groups. In 2000, Brookings recommended that the NSC limits its staff size to 45 (half of its size at the time). The Center for a New American Security published a report in 2015 advocating that the staff size be limited, but did not specify a headcount. RAND published a report examining potential NSC reforms and included a blueprint for a staff of 120. The Heritage Foundation released a policy memo in 2016 recommending a limit of 150 staff. These recommendations can be difficult to compare as they often define staff differently, including or excluding administrative personnel, for example. See Mark Cancian, *Limiting Size of NSC Staff*, Center for Strategic and International Studies (July 2016); I. M. Destler and Ivo H. Daalder, *A New NSC for a New Administration* (Washington, DC: Brookings, November 2000), http://www.brookings.edu/research/papers/2000/11/governance-daalder; Shawn Brimley, Dafna H. Rand, Julianne Smith, and Jacob Stokes, *Enabling Decision: Shaping the National Security Council for the New President* (Washington, DC: Center for a New American Security, June 2015), http://www.cnas.org/sites/default/files/publications- pdf/CNAS%20Report_NSC%20Reform_Final.pdf; Charles P. Ries, Improving Decisionmaking in a Turbulent World (Arlington, VA: RAND Corporation, 2016), http://www.rand.org/pubs/perspectives/PE192.html; Kim R. Holmes, *Memo to a New President: How Best to Organize the National Security Council* (Washington, DC: The Heritage Foundation, April 14, 2016), http://www.heritage.org/research/reports/2016/04/memo-to-a-new-president-how-best-to- organize-the-national-security-council.

[20] Secretary of Defense Robert Gates famously remarked that "[i]t was the operational micromanagement that drove me nuts," referring to the NSC's involvement in field activity. Robert Gates, *Interview with Bret*

Brent Scowcroft, who served as National Security Advisor under Presidents Ford and H. W. Bush, is widely credited with building the model for the modern-day NSC.[21] His "winning formula" included positioning the National Security Advisor as an honest broker and establishing a cooperative process for escalating issues to the President and generating policy recommendations.[22] The general approach has remained largely the same, though each administration has instated its own changes, including modifying the non-statutory membership of the council,[23] altering the names of decision-making documents,[24] and creating new standing committees or councils.[25]

II. Previous Efforts to Address Emerging Technologies

Obama Administration

The Obama administration was the first to make changes to the NSC structure with the explicit intent to tackle technological challenges. Those updates were concurrent with a larger undertaking across the executive branch to better account for new technology in defensive strategy. For example, in 2015, the administration unveiled its Third Offset Strategy, architected by U.S. Deputy Secretary of Defense Robert Work, which sought to improve the United States' geopolitical position by exploiting advantages associated

Baier, Fox News (Apr. 7, 2015), http://www.washingtonexaminer.com/watch-3-former-defense-secretaries-slam-white-house-micromanagement/article/2587908.

[21] See, e.g., Bartholomew Sparrow, *Brent Scowcroft and the Call of National Security* (2015); John Gans, *White House Warriors: How the National Security Council Transformed the American Way of War* (2019).

[22] Ivo Daalder and I. M. Destler, *In the Shadow of the Oval Office: Profiles of the National Security Advisers and the Presidents They Served—From JFK to George W. Bush* (2009).

[23] For example, the Clinton administration added the Secretary of the Treasury, the U.S. Representative to the United Nations, the Assistant to the President for National Security Affairs, the Assistant to the President for Economic Policy, and the Chief of Staff to the President. Office of the Historian, *History of the National Security Council 1947-1997*, Bureau of Public Affairs, United States Department of State (Aug. 1997).

[24] For example, President Carter replaced National Security Study Memorandums with Presidential Review Memorandums, and National Security Decision Memorandums with Presidential Directives. Office of the Historian, *History of the National Security Council 1947-1997*, Bureau of Public Affairs, United States Department of State (Aug. 1997).

[25] The Trump administration, for example, re-established the Homeland Security Council as a co-equal council with the NSC, rather than embedded within the NSC, as had been the case during the Obama administration. National Security Presidential Memorandum – 2 (Jan. 28, 2017).

with new digital technologies in an effort to reverse a decline in America's technological edge.[26]

While the Third Offset Strategy was primarily designed and implemented at the Department of Defense, technology policy also attracted new energy and enthusiasm across the White House. The National Economic Council began to look at technology more closely, though usually in the context of domestic policy formulation, including workforce development (e.g., the TechHire Initiative), regulation of new financial technologies (e.g., the White House FinTech Summit), and high-skilled immigration to support American tech competitiveness. The role of the White House Office of Science and Technology Policy (OSTP) under Obama also expanded significantly, with a focus on improving STEM education, spurring innovation in government, and advancing scientific research.

The NSC began to turn its attention to issues of technology and security as well, and soon the Cyber Directorate was born. Though the primary mission of the directorate was defensive and offensive cyber capabilities, it soon became the catch-all group for a wide range of technology issues, from AI to quantum information science to encryption.

Other directorates also picked up the slack, occasionally covering technology or technology-adjacent issues. Following the Ebola crisis, the administration also established a Directorate for Global Health Security & Biodefense, spun out of the Resilience Directorate. The Strategic Planning Directorate undertook a Big Data report and supported a Deputies' Strategic Trends series.

The Obama administration also amplified OSTP's role in national security. Less than a month after his inauguration, President Obama issued a Presidential Policy Directive giving the OSTP director the ability to attend NSC meetings when science and technology-related issues were on the agenda.[27] (However some former staffers indicated that in practice, OSTP was not always included in relevant conversations, or was brought in too late in the policymaking process to meaningfully shape the outcome.) President Obama later established four new OSTP Associate Director positions, including one focused on national security and international affairs, and

[26] Bob Work, *The Third U.S. Offset Strategy and Its Implications for Partners and Allies*, Jan 28, 2015.

[27] The directive stated that "when science and technology related issues are on the agenda, the NSC's regular attendees will include the Director of the Office of Science and Technology Policy." Organization of the National Security Council System, Presidential Policy Directive – 1 (PPD-1), Feb. 13, 2009.

another focused specifically on technology.[28] John Holdren, Director of OSTP at the time, indicated that the Associate Director for National Security would be dual-hatted with the NSC,[29] though the formal appointment never occurred. OSTP General Counsel later clarified that the director "necessarily works in close collaboration with the National Security Staff on a wide variety of issues, though the position has not been officially 'dual-hatted' during the Obama Administration."[30]

Toward the close of the administration, the White House began to lay the groundwork for larger structural changes at the NSC. A commission chaired by former National Security Advisor Tom Donilon recommended that the next administration consider the elevation of the Cybersecurity Coordinator to the level of Assistant to the President, reporting directly to the National Security Advisor.[31] The Strategic Planning Directorate was charged with undertaking a 60-Day Review in 2015-2016 in conjunction with OSTP that culminated in a set of recommendations concerning the ways in which the White House, NSC, and OSTP could better tackle technology-related issues. The memo was included in transition documents for the incoming administration.

Trump Administration

President Trump's NSC built on certain initiatives from the previous administration, while dismantling others. At the start of the administration, responsibility for emerging technology largely resided with a Director in the Transnational Issues Directorate.[32] As National Security Advisor, Gen. H. R. McMaster sought to limit the proliferation of new directorates, addressing new risks posed by technology by focusing the principals and deputies on critical issues as they arose through existing processes.[33] By March 2017,

[28] John F. Sargent Jr. & Dana A. Shea, *The President's Office of Science and Technology Policy (OSTP): Issues for Congress*, Congressional Research Service (Jan. 13, 2014).
[29] Jeffrey Mervis, "John Holdren Brings More than Energy to His Role as Science Adviser," Science, vol. 324 (April 17, 2009), pp. 324-325.
[30] E-mail communication from OSTP General Counsel Rachael Leonard to CRS, January 24, 2012; cited in John F. Sargent Jr. & Dana A. Shea, *The President's Office of Science and Technology Policy (OSTP): Issues for Congress*, Congressional Research Service (Jan. 13, 2014).
[31] Commission on Enhancing National Cybersecurity, *Report on Securing and Growing the Digital Economy* (Dec. 1, 2016), https://www.nist.gov/system/files/documents/2016/12/02/cybersecurity-commission-report-final-post.pdf.
[32] The Clinton administration had a version of this directorate called the Office of Transnational Threats, staffed by a Special Assistant. National Security Council, Transnational Threats, https://clintonwhitehouse4.archives.gov/WH/EOP/NSC/html/global.html.
[33] Gen. H.R. McMaster, Interview with Author, Feb. 21, 2020.

the Deputy Assistant position overseeing Transnational Issues was eliminated,[34] and in the spring of 2018, the directorate was shuttered in an effort to streamline operations.

While the Cyber Directorate has continued its operations, the White House eliminated the position of cybersecurity coordinator in 2018 in a memo circulated by an aide to then-National Security Advisor John R. Bolton, about a month after his appointment.[35] The memo emphasized that the post was no longer considered necessary because lower-level officials had already accomplished making cybersecurity a "core function" of the NSC.

Five months later, Bolton authorized the creation of an Office of Emerging Technologies within the NSC, to be led by Princeton physicist Dr. William Happer (better-known for his public skepticism of climate change science). The office survived for about a year, from September 2018 to September 2019, folding when Happer left the White House (Happer's decision to leave was independent of Bolton's departure around the same time).[36] During the office's short life, Happer made the rounds of all relevant government agencies, met several times a week with the Cyber Directorate, and "tried to avoid stepping on OSTP's toes," but struggled to break through the noise amidst "all the other chaos going on."[37] In his role as a Senior Director on the NSC, Happer reportedly also helped to drive an executive order on the dangers of electromagnetic pulses on the electrical grid, and blocked congressional testimony on the security risks posed by climate change.[38] At the time of its disbanding, the office had three Directors and one Senior Director position, occupied by Happer.[39]

Even with the creation of the new office, many of the key emerging technology issues—including export controls, biosecurity, and 5G—continued to be owned by other groups within the NSC and the White House, as well as departments and agencies. For example, within the NSC, many issues related to technology and export controls were overseen by a Director for Strategic Trade and Nonproliferation. During the same period, OSTP

[34] Eliana Johnson et al., *McMaster Rolls Back Flynn's Changes at NSC*, Politico (Mar. 1, 2017), https://www.politico.com/story/2017/03/mcmaster-national-security-council-staff-changes-235579.
[35] Nicole Perlroth & David E. Sanger, *White House Eliminates Cybersecurity Coordinator Role*, N.Y. Times (May 15, 2018).
[36] Dr. William Happer, Interview with Author, May 29, 2020.
[37] *Id.*
[38] Scott Waldman, *Why a High-Profile Climate Science Opponent Quit Trump's White House*, Science Magazine (Sept. 12, 2019), https://www.sciencemag.org/news/2019/09/why-high-profile-climate-science-opponent-quit-trump-s-white-house.
[39] Dr. William Happer, Interview with Author, May 29, 2020.

took on some of the policymaking responsibilities for emerging technology and national security, playing an important role in crafting the White House strategies on AI, for example.[40]

National Security Advisor Robert C. O'Brien's NSC has been marked by shift away from functional directorates back toward a traditional focus on regional directorates. As of May 2020, the Strategic Planning Directorate was collapsed and its senior director was made a counselor to O'Brien. The International Economic Affairs Directorate was also removed, and the personnel report up through the National Economic Council (NEC). Shortly after O'Brien assumed the role of National Security Advisor in the fall of 2019, he published an op-ed on his plan to restructure the NSC, emphasizing the need to limit the staff of the NSC, and committed to reducing 174 policy positions to under 120 by early 2020.[41] His op-ed did not mention technology.

III. PROPOSALS FOR REFORM

Former staffers and NSC observers on both side of the aisle agree that the time has come to overhaul the NSC to adapt to new circumstances and better handle threats posed by emerging technology. They recognize that the relevant changes implemented by both the Obama and Trump administrations amounted to piecemeal improvements, rather than comprehensive realignment. But consensus ends there—perspectives on how best to cover emerging technology issues vary widely, with no unanimity concerning structure or approach. Some are in favor the creation of a "czar" position (who might sit outside the NSC), while others believe such a role would only ever amount to a stopgap solution; some think "dual-hatting" ensures synchronized operations, while others believe it creates bureaucratic redundancy; some support building up in-house technical expertise within the NSC, while others believe that subject-matter expertise ought to reside at the agency level or outside government.

The recommended reforms outlined in this report are informed by the insights of individuals who have focused on emerging technology issues from inside and outside government, as well as collected wisdom from past reform attempts or proposals from

[40] Executive Order 13859, Maintaining American Leadership in Artificial Intelligence, Feb. 11, 2019.
[41] Robert C. O'Brien, *Here's How I Will Streamline Trump's National Security Council*, Washington Post (Oct. 16, 2019), https://www.washingtonpost.com/opinions/robert-c-obrien-heres-how-i-will-streamline-trumps-national-security-council/2019/10/16/2b306360-f028-11e9-89eb-ec56cd414732_story.html.

different administrations. They are based on the assumption that structure influences substance—the priorities of an administration—but also recognize the limits of institutional design in determining outcomes.

Rather than attempting to design a future organizational chart in fine-grained detail, this analysis focuses on two broad-strokes options for incorporating emerging technology into security coordination: 1) an NSC-based strategy in which the Council's structure is adapted to take on emerging technology issues; or 2) an agency-centered approach that requires across-the-board changes throughout the executive branch. The two are not mutually exclusive, though in the first formulation, the NSC serves as the nucleus for emerging technology security issues, whereas in the latter formulation, that responsibility is spread across multiple agencies.

An ideal reform option would satisfy the following criteria, discussed in greater detail below:

(1) Recognizes the urgency and priority of grappling with emerging technology in the security context

(2) Enables relevant expertise at the technology-security nexus to be brought to bear on these issues

(3) Ensures various White House components can coordinate effectively with one another regarding emerging technology issues

(4) Promotes interagency coordination that produces outcomes reflective of broad security, diplomatic, economic, commercial, legal, and ethical considerations

(5) Creates iterated contact, consultation, and problem solving with the private sector and academia, reflecting the shift in the locus of innovation outside of government

(6) Avoids negative externalities associated with over-securitizing technology by preventing security risks from dominating the policy-making discourse to the detriment of greater human flourishing

The two overarching options discussed below are graded based on these criteria in the appendix, along with three other proposed reform structures that are not discussed in detail.

Reform Option 1: NSC-Based Approach

By making targeted structural changes to the NSC's organization, this approach would reorient the Council toward emerging technology through the establishment of a new directorate and dedicated Deputy National Security Advisor.

Directorate on Emerging Technology

The ad hoc divvying up of emerging technology issues among the Cyber Directorate and other directorates (often Defense Policy or StratPlan), has historically resulted in inconsistent coverage and a lack of coherent strategy. Because many technology issues are not core to the mission of the existing directorates, the directorates often lack the relevant expertise (with some notable exceptions), resulting in technology being routinely disregarded or marginalized in the policy conversation. While the Cyber Directorate often served as the default home for many technology issues during the Obama administration, placing a diverse array of issues within the Cyber Directorate on an ongoing basis risks the possibility that all challenges will be viewed through a "cyber lens" or framework, where the risk-reward calculus or economic implications may be different.

A new Directorate of Emerging Technology would house several directors covering a range of threats arising due to innovation. By creating a dedicated headcount devoted to emerging technology, the NSC can prevent tech-related threats from falling between the cracks. The directorate would be structured to ensure consistency in mission and scope, while undertaking regular reviews to adjust coverage and expertise to respond to a constantly-evolving landscape. For example, while today the directorate might include coverage of artificial intelligence, biological threats, and information operations, it may be comprised of a substantially different issue-set in 18 months. The directorate would engage in constant horizon-scanning for new risks (in coordination with agencies and StratPlan), and would also take on miscellaneous, ad hoc topics as necessary.

The directorate would be charged with leading Interagency Policy Committees (IPCs)/Policy Coordinating Committees (PCCs) below the Deputies level to ensure

agency coordination on various topics. In addition, it would be charged with coordinating all activities with OSTP's Technology Policy Task Force and other relevant White House offices. Over time, expertise in specific technologies ought to be cultivated within regional portfolios as relevant, but directors in the emerging technology directorate would serve as a backup reserve of deeper knowledge, as well as a coordinator to ensure policy consistency across global issues.

Several staff members within this directorate ought to be "dual-hatted" between the NSC and the NEC and others dual-hatted between the NSC and OSTP, with reporting lines to principals in both entities. Dual-hatting staff would ensure synchronization between the three so that security policy would be informed by both science policy and economic concerns (a similar structure has worked successfully for the Directorate of International Economic Affairs, known as "Intecon"). Dual-hatting with the NEC is especially useful for technology issues that have significant economic considerations, such as export controls and supply chains. It would also prevent emerging technology issues from being "over-securitized," with an outsize emphasis on national security concerns rather than implications for consumers, workforce, or trading partners. While dual-hatting can create bureaucratic convolution and at times impede the ability of teams to move quickly, it also helps to eliminate the possibility of redundancies between councils, which may be meaningful in limiting the growth of staff.

Of course, creating an emerging technology directorate introduces complications, including the challenge of cleanly defining the scope and proper coverage of the group. Grouping threats under the broad title "emerging technology" is in many ways a clumsy designation and belies the reality that these issues are deeply intertwined with other domain-specific or regional threats. For example, the threat of information operations cannot be tackled in a vacuum—rather, specific disinformation campaigns stem from regional dynamics that may already be well-covered by NSC directorates. In addition, some security issues that may rightly fall into this directorate's scope are perhaps more properly understood as "emerging threats" arising from the use of technology that itself may not be particularly novel.[42]

[42] While "emerging technology directorate" was the title favored by most interviewees, others have suggested alternatives, including the "technology and security" directorate, the "technological threats" directorate, and the "techno-security directorate," among others. We have chosen to use "emerging technology" for simplicity, while recognizing that the title may be both over- and under-inclusive in its designation.

On the other hand, it is also possible that creating a separate functional directorate may inadvertently silo or marginalize emerging technology issues, preventing those issues from getting the attention of the National Security Advisor on a regular basis. For these reasons, some have argued that it is preferable for these threats to bubble up organically from the agencies and the departments most affected. But in practice, waiting for issues to bubble up organically has resulted in inconsistent coverage, disorganization, and redundancy. While emerging technology may comprise an ill-defined issue set, the consequences of neglect are greater than the nuisance of coordination challenges or misclassification.

New Deputy National Security Advisor for Technology

The creation of a new position of Deputy Assistant to the President and Deputy National Security Advisor (DAP) for Technology would help to elevate the new threats within the White House and in the national security establishment. It would also signal to the rest of government and industry partners that emerging technology security issues are a key priority with commensurate resources and talent dedicated to addressing them.

A new Deputy National Security Advisor could oversee at least two directorates: 1) the existing Cyber Directorate; and 2) the new Emerging Technology Directorate (though others have suggested additional oversight of a Space Directorate, and a Telecommunications and Supply Chain Directorate). The DAP-level position could also have a formal appointment within OSTP, to help facilitate seamless coordination between the two.[43] Grouping two directorates under the Deputy would give the combined entity more muscle and influence in the White House. A new Deputy would enable the White House to recruit a senior hire from government or industry who is capable of convening officials at the deputy and undersecretary level across the interagency, DAP levels in OSTP, and CIOs and CTOs (usually at the IPC/PCC level) throughout various agencies.[44] A candidate for this role would have to be polymathic, with substantive technical expertise to secure credibility among technologists, but the ability to cover a wide range of security issues and balance numerous competing priorities.

---

[43] Another approach to ensuring connectivity between the NSC and OSTP would be to name the Science Advisor a permanent member of the NSC and its Principals Committee. Christopher Chyba & Ethan Magistro, *The President's Science Advisor Should be a Full Member of the National Security Council and Its Principals Committee*, War on the Rocks (Dec. 11, 2020).

[44] Christopher Kirchhoff, Director for Strategic Planning, "Transition Considerations for Tech Policy at the NSC," July 2016.

The disadvantages of creating a new Deputy includes the possibility that yet-another Deputy National Security Advisor will only increase bureaucratic processes, with more DAPs competing for the National Security Advisor's attention, more Deputies Committee meetings called on a regular basis, and so on. Some argue that the position is simply unwarranted, or that the Deputy National Security Advisor for Transnational Issues should be resurrected instead (as many emerging technology threats are indeed transnational in nature). It is worth noting that there may be good reason to do both—create a new Deputy position and resurrect Transnational Threats—as there are a number of transnational topics that fall into the bucket of the latter but not the former, including pandemics, climate change, and the refugee crisis. Others have advocated for a DAP for international economics or a DAP for strategy and reform instead, with a variety of functional directorates that report up to both the emerging technology and international economics deputies. Specific high-priority issues—including COVID-19 and climate change—could be supported by other designated bodies, such as a temporary czar or task force, or a dedicated council.

Reform Option 2: Agency-Centered Approach

Another strategy for incorporating emerging technology into security decision-making is a comprehensive restructuring that locates expertise across the executive branch, with the NSC occupying a supporting role, rather than taking the lead.

Under this decentralized approach, the National Security Advisor may choose to appoint a single advisor or coordinator on emerging technology issues, who then serves as a convener for all voices throughout government on emerging technology, but likely does not have extensive dedicated staff nor seek to drive policy from the NSC itself. The center of gravity on particular issues will reside in specific departments and agencies with relevant expertise; for example, the National Science Foundation might serve as the lead for new research and development efforts on security-related technology. It may also require strengthening and empowering existing tech policy offices to cover security-related subjects more effectively. For example, OSTP staff might need to be cleared in order to run point on certain sensitive policy areas.[45]

[45] The way that space-related security topics are handled by the White House may provide a useful model, with NASA overseeing research and exploratory efforts, and the Department of Defense overseeing the new U.S. space command.

An agency-centered approach would rely on bottom-up evolution at the department and agency level.[46] The Department of Defense is the furthest ahead in accounting for the role of emerging technology, with the establishment of the Defense Innovation Unit, the Defense Digital Service, and the Joint AI Center. But efforts to integrate DoD's contribution to the interagency process on policy remains underdeveloped, and the Office of Net Assessment (ONA) and Office of the Secretary of Defense policy operation (OSD-P) could be better utilized in this regard.

In the intelligence community, evolution may mean strengthening existing capacity by increasing the number of technologists in its analyst ranks. At the Departments of Commerce and Treasury, development of advanced market forecasting on the technology sector may be a worthwhile investment. The State Department will need to upgrade its diplomatic strategy to structure the types of global alliances and multilateral architectures are needed to successfully engineer technological statecraft for the next century (such as the proposed D-10 or T-12[47]).

There are several key benefits to the agency-centered approach. First, it takes advantage of the fact that most subject-matter expertise naturally resides within departments and agencies and enhances their ability to assume leadership roles on those policy areas. Limiting the NSC to a minimalist role may also help to prevent NSC-overreach and proliferation of staff. The agency-centered approach, while posing a more complex bureaucratic undertaking up front, may also bring about much-needed sweeping changes across departments and agencies that will ultimately be necessary in the long-term.

There are also disadvantages to removing the center of power from the NSC. In a memo evaluating tech policy issues at the NSC, former Senior Director for Strategic Planning Christopher Kirchhoff noted that "the U.S. cannot rely on any one department to lead the U.S. response to them, given their security, diplomatic, economic, commercial, legal, and ethical implications."[48] Only the NSC has the vantage point that enables it to holistically consider the myriad tradeoffs and competing interests across the executive branch. And without a dedicated NSC entity focused on emerging technology,

[46] The authors thanks Christopher Kirchhoff for his insightful contributions on this topic.
[47] An informal grouping of twelve "techno-democracies," modeled on the G7 or G20. Jared Cohen & Richard Fontaine, *Uniting the Techno-Democracies: How to Build Digital Cooperation*, Foreign Affairs (Nov./Dec. 2020).
[48] Christopher Kirchhoff, Director for Strategic Planning, "Transition Considerations for Tech Policy at the NSC," July 2016.

resources and attention may be diverted from adjacent NSC directorates, such as Cyber, Defense, or Strategic Planning. In order for the NSC to play an effective role as a convener and address all of these facets, "the NSC will need dedicated capacity to drive an integrated [U.S. government] approach."[49]

IV. OTHER CONSIDERATIONS

While thoughtful structural reforms may help to alleviate the challenges facing the NSC today, there are a number of perennial considerations that a future National Security Advisor must consider in staffing the Council and designing its processes to best address emerging technology threats.

Technical Expertise

The question of where technical expertise ought to reside within the security establishment is subject to much disagreement, with some arguing that all technical subject-matter expertise should sit at departments and agencies, and others advocating for a significant level of expertise within the NSC itself. The advantage of having technical expertise within the NSC staff is that it provides the president with an independent source of advice that is not motivated or influenced by agency-specific interests. It also ensures that all NSC policymaking is informed by technical considerations.

On the other hand, it may be impracticable to employ deep technical experts on the broad range of issues covered by the NSC. And generalists who are fluent on a range of issues may ultimately be more effective policymakers than narrow experts. Some have suggested that technical expertise ought to be housed within OSTP and utilized on an as-needed basis by the NSC. Others have recommended that the NSC have an improved mechanism for bringing in outside expertise from academia and the private sector (in Special Government Employee or Highly Qualified Expert positions or similar) for short periods of time to advise on technical issues.[50]

[49] *Id.*

[50] Paul Scharre, Interview with Author, Oct. 17, 2019. The Defense Advanced Research Projects Agency (DARPA) utilizes such a model, facilitating the rotation of top talent into government for 2-3 year tours.

Over-Securitization

Security concerns represent only one piece of the puzzle in grasping the impacts of emerging technology on society. In fact, the disruption caused by new innovations is often largely commercial, cultural, or social. For example, the consequences of 5G technology or autonomous vehicles may be primarily economic, though there are certainly geopolitical and national security implications of their rollout as well. By locating primary responsibility for emerging technology in the NSC, there is a risk that security dimensions of an issue are overemphasized, when in fact the more important concern is one of American competitiveness (raising economic and immigration concerns more than security ones).[51] It has also led, in some cases, to an exaggeration of the magnitude of a specific threat, for example, the often-overstated risk of academic espionage as a result of admitting Chinese nationals to American universities.

Given that much of the NSC's work is classified in nature, the practical impact of giving NSC oversight over emerging tech may be the systematic exclusion of other science & technology policymakers from the conversation, including those from Commerce, Treasury, U.S. Trade Representative, and the Council of Economic Advisors. Private sector technology companies may also be more inclined to engage with the White House on tech policy when the discussion is not security or defense-oriented. Dual-hatting some members of an emerging technology directorate may be one way to avoid the pitfalls of over-securitization. For example, the Obama Administration's first cybersecurity strategy in 2009 attempted to thread this needle by creating a "cyber czar" who was a member of the National Security Council but reported to both the national security advisor and to a senior economic advisor to ensure that security and economic concerns were properly balanced.

Urgency and Relevance

Emerging threats often appear so far on the horizon that they are systematically deprioritized in the security agenda. It is therefore critical to design a structure or set of processes that ensures that emerging technology issues have day-to-day relevance in the eyes of senior staff. Staffers from both the Obama and Trump administrations noted

[51] Jeffrey Prescott, Interview with Author, Sept. 12, 2019.

the difficulty of attracting sustained attention to technology issues. (The Strategic Planning Directorate was established in part to combat the NSC's natural tendency to gravitate toward immediate crises, with some success.)

Historian John Gans has noted that historically, influence at the NSC is determined by the issue's relevance in urgent, day-to-day decision-making.[52] While those with responsibility for less-urgent subjects may occasionally secure an audience with the National Security Advisor or the President, their influence and credibility will remain limited unless those topics are top of mind across the security establishment. In Gans' estimation, the NSC is typically at its best when focused either on supporting the president in daily activities and meetings, or on architecting large, strategic visions. The middle zone of substantive policymaking is where the NSC tends to overreach and infringe on matters that may be better-handled by agency heads. Unfortunately, oftentimes technology issues fall squarely into the middle zone—requiring deeper and more consistent engagement than high-level strategic planning can afford, but not quite attracting attention in the day-to-day firefights. The historical difficulty of elevating technology issues in the White House may underscore the need for a new Deputy National Security Advisor on Technology. In any case, all changes to the NSC structure must be made with this dilemma in mind, and processes must be designed to compel regular engagement with technology issues.

Role of the Private Sector

The private sector represents a key node in the security formula. Technology companies have become the primary drivers of research and development of new technology.[53] They are the primary trainers and employers of the country's most sophisticated tech talent.[54] And leading companies themselves have become the battleground on which foreign adversaries stage attacks (from high-profile hacks to election interference on social media platforms). And yet, the White House has

[52] John Gans, Interview with Author, Oct. 8, 2019.

[53] The Congressional Budget Office estimates that private-sector firms spent $333 billion in R&D in 2015 (the most recent available data), representing 67 percent of the national total, with the federal government comprising only 24 percent. Sheila Campbell & Chad Shirley, *Estimating the Long-Term Effects of Federal R&D Spending: CBO's Current Approach and Research Needs*, Congressional Budget Office (June 21, 2018).

[54] High-tech industries employed nearly 17 million U.S. workers in 2014, according to the Bureau of Labor Statistics. Michael Wolf & Dalton Terrell, *Beyond the Numbers: The High-Tech Industry, What It Is and Why It Matters to our Economic Future*, Bureau of Labor Statistics, Vol. 5 No.8 (May 2016).

struggled to find ways to reliably tap private sector talent and expertise, or work collaboratively to combat security threats. While there is no formal blanket prohibition preventing NSC staffers from consulting with technology companies, in practice it appears to happen infrequently, either because of the classified nature of matters, executive privilege issues, potential or perceived conflicts, lack of interest alignment, absence of familiarity, or custom.[55]

In 2009 the White House announced the President's Council of Advisors on Science and Technology (PCAST), which assembled a group of leading scientists and engineers outside of government to advise the president on issues of science and innovation.[56] But PCAST was often out of reach for NSC staffers, who were often unable to share work with PCAST members or consult them for a variety of reasons.

The NSC will need to find a way to better draw on the private sector expertise and coordinate in formulating strategic response. One option would be to establish a private sector technology advisory council (with clearances) to serve as a brain trust on security issues. But some have warned against the proliferation of advisory committees, expressing concern that the added value is outweighed by the headaches caused, noting that that they can be disruptive to the policy process, give an outsize influence to only a few voices, and at times divert attention from the most critical issues. An alternative solution would be to convene ad hoc sessions with industry or bring in subject matter experts for specific briefings. It would also be worth exploring ways to rotate technical talent from private sector or academia into the NSC for 1-3 year tours, perhaps in a structure similar to the Defense "delivery unit" envisioned by Section 913 of the 2017 National Defense Authorization Act, though never implemented. Whether or not a standing body is necessary, connective tissue with the private sector will be required to inform responses to the thorniest security threats.

CONCLUSION

Throughout history, policymakers have often suffered from a form of continuity bias, failing to appreciate paradigm shifts, underweighting looming threats, and over-

[55] The notable exception here may be the Cyber Directorate under the Obama administration, which more frequently engaged with industry and civil society, after receiving broad clearances from NSC legal and the White House Counsel's Office.
[56] December 19, 2011, Executive Order 13596; Amended Executive Order 13539.

indexing on past experiences. Today we find ourselves in one of those moments. Technological innovation has been an exceptional source of American progress and vitality, but it may also be its Achilles heel. The security landscape is evolving so rapidly and unexpectedly, the institutions we trust to protect us are struggling to keep up. While departments and agencies throughout the executive branch have begun to take meaningful steps toward updating their strategy and operations in light of new technology, the NSC continues to wrestle with how best to reinvent itself to keep pace. This structural weakness at the very top practically guarantees that critical threats related to emerging technology will never receive the attention they deserve.

The time has come for a holistic and comprehensive reassessment of the NSC's handling of emerging technology. Detailed analysis and examination of bureaucratic systems may appear mundane compared to the substantive and pressing policy issues that routinely capture attention in the national security community. And yet, without the structures supporting meaningful work on emerging technology risks at the NSC, those substantive policy areas will systematically fall through the cracks. There are numerous models or approaches worthy of consideration for solving this problem, but the continuation of the status quo will ensure that the United States lags behind our adversaries. The start of a new administration provides a unique opportunity to reconceive of the NSC, and in turn, to establish a strong framework for securing America's future.

APPENDIX

Scorecard: 6 Reform Options for the National Security Council