Texas National Security Review: Volume 3, Issue 4 (Fall 2020)
Print: ISSN 2576-1021 Online: ISSN 2576-1153

FROM REACTION TO ACTION: ADOPTING A COMPETITIVE POSTURE IN CYBER DIPLOMACY

Emily O. Goldman

Adversaries probe the United States and its allies daily in cyberspace. American cyber diplomacy has improved but still leaves the United States vulnerable to continuous, state-sponsored cyber aggression that is having strategic effects, even though that aggression never rises to a "significant" level that would elicit an armed response. The State Department can pivot — without risking armed conflict — from a "reaction-after-the-fact" posture to seizing the initiative from adversaries whose cyberspace campaigns erode U.S. economic competitiveness, reduce military advantages, and weaken political cohesion. It should reexamine assumptions about cyber conflict and norm emergence, adopt a competitive mindset, and prioritize efforts tailored for great-power competition.

Most state-sponsored malicious cyber activity takes the form of campaigns conducted outside of armed conflict. The 2017 *National Security Strategy* insists that such campaigns are nonetheless producing meaningful strategic gains for America's adversaries. These gains have come through intellectual property theft that degrades economic competitiveness, as well as theft of research and development. Malign cyber activity could include supply-chain manipulation to undercut U.S. and allied military capabilities. Most prominently, state actors are conducting disinformation campaigns and information manipulation in order to weaken domestic political cohesion and confidence in government institutions. These threats demand an immediate response.

The United States should regain the initiative in strategic cyber competition. The Department of Defense has pivoted to a more assertive posture, but the State Department's pivot has just begun. The 2017 *National Security Strategy* coined the phrase "competitive diplomacy" with appeals to "upgrade our diplomatic capabilities to compete in the current environment and to embrace a competitive mindset."[1] Nowhere is this more necessary than in cyber diplomacy that engages the state sponsors of malicious cyber campaigns while simultaneously working with America's allies and partners in resisting such threats.

This article describes how current cyber diplomatic priorities, approaches, and conceptual frameworks need to change so that the United States can prevail in strategic cyber competition. It recommends new diplomatic initiatives, engagement priorities, operational partnerships, and a shift in mindset for the State Department to help thwart adversary cyber campaigns. These changes can improve alignment and integration across the U.S. government and with foreign allies and partners, and close gaps that continue to slow U.S. military and law enforcement operations, restrain diplomatic and operational freedom of action, and cede to adversaries the initiative to set de facto norms.

The argument unfolds in five sections. The first explains the context of strategic cyber competition. The second summarizes the current state of U.S. cyber diplomacy. The third and fourth explain how and why the State Department should revise its approaches to norm construction and deterrence. The last section offers seven recommendations that — if adopted — would greatly increase the ability of the United States to prevail in great-power competition in cyberspace.

1 The White House, *National Security Strategy of the United States of America*, December 2017, 33, https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf.

Strategic Cyber Competition

Great-power competition is now front and center in American national security and foreign policy. The 2017 *U.S. National Security Strategy* warns that states like China and Russia are "actively competing against the United States and our allies and partners."[2] Inter-state strategic competition supplanted terrorism as the primary focus in the 2018 *National Defense Strategy* and is identified as the most difficult challenge facing U.S. military forces in the 2018 *U.S. National Military Strategy*.[3]

There is also consensus across the U.S. government that great-power competitors are making strategic gains in and through cyberspace with persistent, targeted campaigns that never rise to the level of a catastrophic cyber attack. Strategic gains are being accrued not through the traditional route of war, but cumulatively and persistently over time in cyberspace at unprecedented speed and scale. Adversaries deliberately act below internationally accepted thresholds and never physically cross U.S. borders, thus minimizing risk to themselves while reaping the cumulative benefits of their cyber behavior.[4] Competing below the level of armed conflict and contesting malicious cyber activity in day-to-day competition are consistent themes across the *National Defense Strategy*, the *National Military Strategy*, and the 2018 *Department of Defense Cyber Strategy*.[5]

Cyberspace has become a major battleground for great-power competition because of the nature of the operating environment: It is globally interconnected, distinguished by constant (rather than imminent, potential, or episodic) contact, influenced by difficulty of attribution, characterized by contested borders and informal thresholds that are limited in adherence, and lacks sanctuary and operational pause. In addition, there is an ideological dimension fueling this competition, one that pits free societies against authoritarian regimes that view an open cyberspace and information freedom as existential threats to their power.[6]

Illiberal regimes are working to shape the digital ecosystem in line with authoritarian values and influencing mandates and agendas in standards bodies and international organizations to support information control.[7] They promote, and at times advance, "cyber sovereignty" as an organizing principle of governance in cyberspace.[8] Cyber sovereignty asserts that states have the right to censor and regulate the internet to prevent exposing their citizens to ideas and opinions deemed harmful by the regime. It calls for states to govern the internet instead of the current multi-stakeholder model that also includes businesses, civil society, research institutions, and non-governmental organizations in the dialogue, decision-making, and implementation of solutions. The subordination of cyberspace to the interests of the state reflects the fact that authoritarian governments value regime security over individual liberty.

China is developing and exporting technologies and networks that erode civil society, privacy, and human rights.[9] Russia successfully advocated for the establishment of the Open-Ended Working Group in the United Nations, an alternative norms-creating forum that threatens to dilute

2 *National Security Strategy*, 25.

3 *Summary of the 2018 National Defense Strategy of The United States of America: Sharpening the American Military's Competitive Edge*, 2018, 1, https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf.; The Joint Staff, *Description of the National Military Strategy 2018*, 2018, 3, https://www.jcs.mil/Portals/36/Documents/Publications/UNCLASS_2018_National_Military_Strategy_Description.pdf.

4 Richard J. Harknett and Emily O. Goldman, "The Search for Cyber Fundamentals," *Journal of Information Warfare* 15, no. 2 (Spring 2016): 81-88, https://www.jstor.org/stable/26487534; Richard Harknett and Max Smeets, "Cyber Campaigns and Strategic Outcomes," *Journal of Strategic Studies* (March 2020), https://doi.org/10.1080/01402390.2020.1732354.

5 Department of Defense, *Summary: Department of Defense Cyber Strategy 2018*, 2018, 4, https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF.

6 Michael Warner, "Invisible Battlegrounds: On Force and Revolutions, Military and Otherwise," in *The Palgrave Handbook of Security, Risk and Intelligence*, ed. Robert Dover, Huw Dylan, and Michael Goodman (London: Palgrave Macmillan, 2017), 254.

7 James A. Lewis, "Cyber Solarium and the Sunset of Security," *Center for Strategic & International Studies*, March 13, 2020, https://www.csis.org/analysis/cyber-solarium-and-sunset-cybersecurity; U.S.-China Economic and Security Review Commission, "A 'China Model?' Beijing's Promotion of Alternative Global Norms and Standards," March 13, 2020, https://www.uscc.gov/hearings/postponed-china-model-beijings-promotion-alternative-global-norms-and-standards.

8 Niels Schia, Niels Nagelhus, and Lars Gjesvik, "China's Cyber Sovereignty," *Norwegian Institute for International Affairs (NUPI)*, Jan. 1, 2017, https://www.jstor.org/stable/resrep07952; Niels Nagelhaus and Lars Gjesvik, "The Chinese Cyber Sovereignty Concept (Part 1)," *The Asia Dialogue*, Sept. 7, 2018, https://theasiadialogue.com/2018/09/07/the-chinese-cyber-sovereignty-concept-part-1/.

9 "China Exports AI Surveillance Tech to Over 60 Countries: Report," *Nikkei Asian Review*, Dec. 16, 2019, https://asia.nikkei.com/Business/China-tech/China-exports-AI-surveillance-tech-to-over-60-countries-report; Steven Feldstein, "The Global Expansion of AI Surveillance," *Carnegie Endowment for International Peace*, Sept. 17, 2019, https://carnegieendowment.org/2019/09/17/global-expansion-of-ai-surveillance-pub-79847.

progress made under the U.N. Group of Governmental Experts process.[10] In spite of the Budapest Convention on Cybercrime, Russia secured U.N. support for a cyber crime resolution that may make it easier to repress political dissent.[11] In concert with these diplomatic achievements, authoritarian regimes continually exploit open networks and platforms to destabilize democratic societies from within, illicitly acquire intellectual property and personally identifiable information, and disrupt critical infrastructure.[12] Clearly, states retain significant diverging interests and normative preferences for the future of cyberspace. Renewed great-power competition with ideological adversaries need not alter America's vision for cyberspace (i.e., an open, interoperable, secure, reliable, market-driven domain that reflects democratic values and protects privacy). However, it does require an empirically based view of the cyberspace strategic environment as one characterized by great-power competition and contested principles and norms that has evolved away from the vision of international liberal markets buttressed by an open, worldwide internet.[13] By adopting a competitive mindset, cyber diplomacy can be more responsive to the international environment, better aligned to defense policy, and more deeply integrated into a whole-of-government strategy for strategic cyber competition.

The Current State of U.S. Cyber Diplomacy

Cyber diplomacy is the use of diplomatic tools to resolve issues arising in cyberspace.[14] American cyber diplomacy promotes a vision of an open, interoperable, reliable, and secure information and communications technology infrastructure and governance structures to support international trade and commerce, strengthen international peace and security, and foster free expression and innovation.[15] Cyber diplomacy also seeks to build strategic bilateral and multilateral partnerships, expand U.S. capacity-building activities for foreign partners, and enhance international cooperation.[16] Key lines of effort include building consensus among like-minded states on norms of responsible state behavior in cyberspace;[17] encouraging international participation in a deterrence framework that involves collective attribution and swift imposition of consequences on those who violate those norms;[18] exposing and countering foreign disinformation and propaganda efforts;[19] promoting American access to markets and leadership in digital technologies;[20] building cyber security capacity of allies and foreign partners; and more recently, ensuring that 5G (fifth-generation cellular network) technology deployed around the world is secure and reliable.[21]

Yet despite the importance of cyber diplomacy, the State Department has never produced a cyber strategy. The closest approximation may be the Obama administration's 2011 *International Strat-*

10 Samuele de Tomas Colatin, "A Surprising Turn of Events: UN Creates Two Working Groups on Cyberspace," *NATO Cooperative Cyber Defence Centre of Excellence*, https://ccdcoe.org/incyder-articles/a-surprising-turn-of-events-un-creates-two-working-groups-on-cyberspace/; Shannon Vavra, "World Powers Are Pushing to Build Their Own Brand of Cyber Norms," *CyberScoop*, Sept. 23, 2019, https://www.cyberscoop.com/un-cyber-norms-general-assembly-2019/.

11 U.N. General Assembly, "Countering the Use of Information and Communications Technologies for Criminal Purposes," Nov. 2, 2018, https://undocs.org/A/C.3/73/L.9/Rev.1.

12 Andy Greenberg, "The Untold Story of NotPetya, the Most Devastating Cyberattack in History," *Wired*, Aug. 22, 2018, https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/; "Press Briefing on the Attribution of the WannaCry Malware Attack to North Korea," The White House, Dec. 19, 2017, https://www.whitehouse.gov/briefings-statements/press-briefing-on-the-attribution-of-the-wannacry-malware-attack-to-north-korea-121917/.

13 Chris C. Demchak and Peter Dombrowski, "Rise of a Cybered Westphalian Age," *Strategic Studies Quarterly* 5, no. 1 (Spring 2011): 32-61, https://www.jstor.org/stable/26270509.

14 Shaun Riordan, "Cyber Diplomacy v. Digital Diplomacy: A Terminological Distinction," *University of Southern California, Center on Public Diplomacy*, May 12, 2016, https://www.uscpublicdiplomacy.org/blog/cyber-diplomacy-vs-digital-diplomacy-terminological-distinction.

15 U.S. Department of State, International Security Advisory Board, *Report on A Framework for International Cyber Stability*, July 2, 2014, https://2009-2017.state.gov/documents/organization/229235.pdf.

16 Chris Painter, "Diplomacy in Cyberspace," *The Foreign Service Journal*, June 2018, https://www.afsa.org/diplomacy-cyberspace.

17 This mission falls to State's Office of the Coordinator for Cyber Issues. See, Painter, "Diplomacy in Cyberspace."

18 This mission falls to State's Office of the Coordinator for Cyber Issues.

19 This mission falls to the Global Engagement Center, which is distinct from the Office of the Coordinator for Cyber Issues with its focus on technical cyber incidents. Statement of Lea Gabrielle, Special Envoy & Coordinator for the Global Engagement Center, U.S. Department of State, Before the Senate Foreign Relations Subcommittee on State Department and USAID Management, International Operations, and Bilateral International Development, "Executing the Global Engagement Center's Mission," March 5, 2020, https://www.foreign.senate.gov/imo/media/doc/030520_Gabrielle_Testimony.pdf.

20 This mission falls to the Bureau of Economic and Business Affairs, which is lead for the 5G campaign.

21 U.S. Department of State, "Senior State Department Official on State Department 2019 Successes on Cybersecurity and 5G Issues," Jan. 9, 2020, https://www.state.gov/senior-state-department-official-on-state-department-2019-successes-on-cybersecurity-and-5g-issues/.

egy for Cyberspace, an initiative spearheaded by Christopher Painter who became the State Department's top cyber diplomat.[22] Current lines of effort still closely align to the 2011 strategy, even though the world has dramatically changed since that time.

The 2011 strategy ties global stability to the establishment of norms by like-minded states. Toward this end, the strategy calls on the United States to (1) engage in urgent dialogue to build consensus around principles of responsible behavior in cyberspace; (2) build international understanding around cyberspace norms, beginning with like-minded countries in bilateral dialogues; (3) carry this agenda into international organizations; (4) deter malicious actors from violating these norms; and (5) facilitate cyber security capacity-building.[23] The State Department has steadily pursued these goals, even as authoritarian regimes strive to reshape the digital environment and rewrite international norms and standards.[24]

American diplomats have had some success in reaching agreement in international fora on principles of responsible state behavior in cyberspace.[25] The 2013 and 2015 meetings of the United Nations' cyber-specific Group of Governmental Experts reached a consensus on the applicability of international law in cyberspace, but established only voluntary, non-binding norms as was their stated objective.[26] The 2017 U.N. Group of Governmental Experts failed to deliver a consensus report.[27]

The State Department's decades-long cyber norms-building project — determining how existing binding norms apply in cyberspace and using non-binding norms to set expectations of behavior that could eventually be codified — has been a top-down process, based on the belief that diplomatic consensus on normative taboos can shape state behavior. Agreements on the non-proliferation of nuclear weapons and on the non-use of chemical weapons are cited as evidence of this approach.[28] Yet these conventions were possible because the technologies were well-developed and their effects understood. By contrast, the risks and ramifications of cyber capabilities are not yet widely recognized. Norms can be powerful tools, but according to Stefan Soesanto and Fosca D'Incau, "their creation is contingent upon a history of transnational interaction, moral interpretation, and legal internalization. Only through this tedious multi-pronged process is there any hope for national interests to be reframed and national identities to be reconstructed."[29]

International norms should be built from the bottom up in a competition for influence over cyberspace. This will require the departments of State and Defense to work closely together. There have been many calls for better interagency coordination and integration to posture the United States so that it may operate in the murky area between peace and war more effectively. New challenges often prompt calls for structural reform and reorganization as the solution. Since 2019, the State Department has been working hard to establish the Bureau for Cyberse-

22 *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World*, May 2011, https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf. The State Department raised the profile of cyber issues in U.S. foreign policy with Christopher Painter's appointment in 2011 as the department's cyber coordinator and his establishment of the Office of the Coordinator for Cyber Issues.

23 *International Strategy for Cyberspace*, 11-15.

24 Adam Segal, "China's Alternative Cyber Governance Regime," *Council on Foreign Relations*, March 13, 2020, https://www.uscc.gov/sites/default/files/testimonies/March%2013%20Hearing_Panel%203_Adam%20Segal%20CFR.pdf.

25 "G7 Declaration on Responsible States Behavior In Cyberspace," April 11, 2017, https://www.mofa.go.jp/files/000246367.pdf.

26 U.N. General Assembly, "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, Note by the Secretary-General," June 24, 2013, https://www.un.org/ga/search/view_doc.asp?symbol=A/68/98; U.N. General Assembly, "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, Note by the Secretary-General," July 22, 2015, https://www.un.org/ga/search/view_doc.asp?symbol=A/70/174.

27 U.S. Department of State, "Explanation of Position at the Conclusion of the 2016-2017 UN Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security," June 23, 2017, https://www.state.gov/explanation-of-position-at-the-conclusion-of-the-2016-2017-un-group-of-governmental-experts-gge-on-developments-in-the-field-of-information-and-telecommunications-in-the-context-of-international-sec/; Adam Segal, "The Development of Cyber Norms at the United Nations Ends in Deadlock, Now What?" *Council on Foreign Relations*, June 19, 2017, https://www.cfr.org/blog/development-cyber-norms-united-nations-ends-deadlock-now-what; Elaine Korzak, "UN GGE on Cybersecurity: The End of an Era?" *The Diplomat*, July 31, 2017, https://thediplomat.com/2017/07/un-gge-on-cybersecurity-have-china-and-russia-just-made-cyberspace-less-safe/.

28 Richard Price and Nina Tannenwald, "Norms and Deterrence: The Nuclear and Chemical Weapons Taboos," in *The Culture of National Security: Norms and Identity in World Politics*, ed. Peter J. Katzenstein (New York: Columbia University Press, 2009), 114-152.

29 Stefan Soesanto and Fosca D'Incau, "The UN GGE is Dead: Time to Fall Forward," *Council on Foreign Relations*, Aug. 15, 2017, https://www.ecfr.eu/article/commentary_time_to_fall_forward_on_cyber_governance; Cedric Sabbah, "Pressing Pause: A New Approach for International Cybersecurity Norm Development," 2018, https://ccdcoe.org/uploads/2018/10/Art-14-Pressing-Pause.-A-New-Approach-for-International-Cybersecurity-Norm-Development.pdf.

curity and Emerging Technologies.[30] A new bureau with more resources and people could expand and sustain initiatives that have been underway since the establishment of the Office of the Coordinator for Cyber Issues.[31] From 2011 onwards, the office has launched cyber dialogues and capacity-building programs, promoted an international framework of cyber stability that includes building a consensus around norms of responsible state behavior, advanced multi-stakeholder internet governance, and championed cyber deterrence. However, strategic cyber competition — continuous campaigns outside of armed conflict that cumulatively produce strategic gains — demands new initiatives, planning assumptions, and thinking. Adapting diplomacy to strategic cyber competition requires dislodging some of the assumptions currently guiding State Department approaches — specifically those associated with how norms are constructed and the applicability of a strategy of deterrence to competition in cyberspace.

INTERNATIONAL NORMS SHOULD BE BUILT FROM THE BOTTOM UP IN A COMPETITION FOR INFLUENCE OVER CYBERSPACE. THIS WILL REQUIRE THE DEPARTMENTS OF STATE AND DEFENSE TO WORK CLOSELY TOGETHER.

Constructing Norms

The 2018 *U.S. National Cyber Strategy* calls on the United States to encourage universal adherence to cyber norms because "[i]ncreased public affirmation by the United States and other governments will lead to accepted expectations of state behavior and thus contribute to greater predictability and stability in cyberspace."[32] Like the 2011 *International Strategy for Cyberspace*, the 2018 *National Cyber Strategy* clings to an imperfect analogy that distorts American approaches to norm development.

The prevailing approach to norm construction that guides U.S. cyber diplomacy has its roots in America's post-World War II success in fashioning a global political-economic structure of rules reinforced with institutions. At the time, the United States produced 60 percent of the world's gross economic product, held a monopoly on nuclear weapons, and had accrued a reservoir of trust in the eyes of most of the international community. America's dominance over the distribution of political-economic benefits meant that Washington could provide those benefits to states that adopted American-inspired norms. Conversely, the United States could deny such advantages to states that rejected those norms. This temporary apex of American influence enabled the United States to reform the world's financial and trading systems, taking key steps at the Bretton Woods conference in 1944. In other words, the United States was in a unique position to credibly establish norms for a critical mass of states.[33] Such is not the case for cyberspace today.

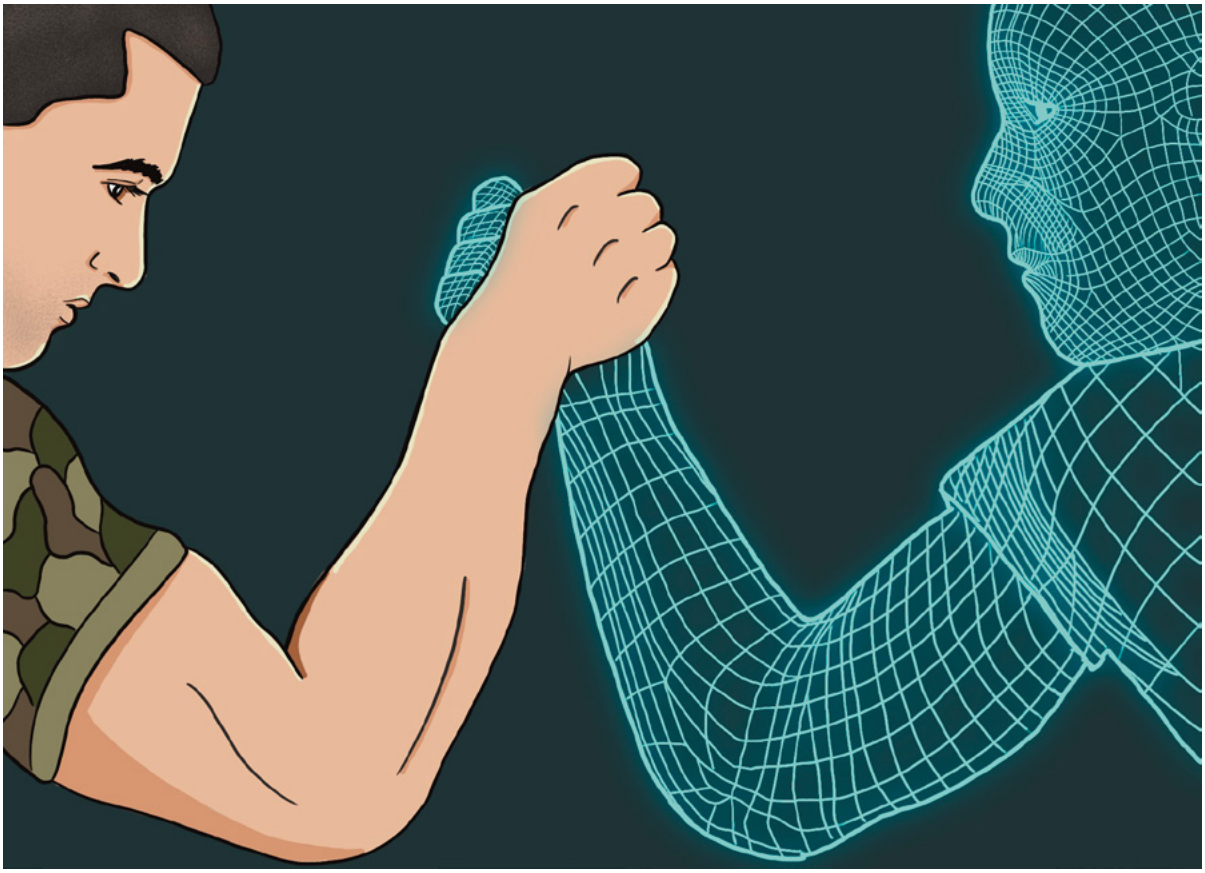
The technology for globally networked, digital information systems was largely invented by American businesses, universities, and government agencies. The National Security Agency (NSA) took an interest in these developments from the beginning and guided key innovations for securing data. When the information revolution went global, however, American dominance inevitably ebbed and was lost by the late 1990s and early 2000s. While American institutions and corporations retain significant influence over the technical aspects of computing, networking, and telecommunications, the U.S. government has not been able to shape and enforce norms of behavior. For example, in September 2016, while President Barack Obama was telling reporters at the G20 Sum-

30 Joshua Rovner, "Did the Cyberspace Solarium Commission Live Up to Its Name?" *War on the Rocks*, March 19, 2020, https://warontherocks.com/2020/03/did-the-cyberspace-solarium-commission-live-up-to-its-name/. The State Department has eyed reorganization when faced with new challenges that do not neatly align with existing structure. See, International Security Advisory Board "Report on Gray Zone Conflict," Jan. 3, 2017, https://2009-2017.state.gov/documents/organization/266849.pdf.

31 The *Cyberspace Solarium Commission Report* supports more resources for existing diplomatic efforts. One can infer that the commissioners concluded current lines of effort are adequately aligned to the challenges facing the United States today. The report's language, in fact, nearly identically mirrors what U.S. diplomats involved with cyber issues have been asserting for years. See, U.S. Cyberspace Solarium Commission, Cyberspace Solarium Commission, March 2020, https://www.solarium.gov.

32 *National Cyber Strategy of the United States*, September 2018, 20, https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.

33 Finnemore and Sikkink define a critical mass as one-third of the total states in the system. Martha Finnemore and Kathryn Sikkink, "International Norm Dynamics and Political Change," *International Organization* 52, no. 4 (Autumn 1998): 901, https://www.jstor.org/stable/2601361.



mit that the U.S. goal is to "start instituting some norms so that everybody's acting responsibly,"[34] Russia was flouting norms of responsible behavior by mounting a multi-pronged cyber campaign to influence the American presidential election.

American diplomats have worked actively as norm entrepreneurs. Specifically, they have attempted to call attention to problematic cyber behavior; set the agenda in international venues that possess the requisite membership, mandate, and legitimacy; advocated candidate norms; persuaded and pressured (through naming, blaming, and shaming) other states to embrace these norms; and built coalitions of like-minded norm addressees to lead by example.[35] These efforts have yielded some positive results. The year 2013 was a high-water mark for U.S. cyber diplomacy, as both Russia and China agreed that "international law, and in particular, the United Nations Charter, applies in cyberspace."[36] From the U.S. perspective, agreement on the U.N. Charter implied acceptance of the Geneva Conventions and the applicability of the laws of armed conflict to cyberspace. However, progress stalled shortly thereafter. Chinese officials emphasized the U.N. Group of Governmental Experts' embrace of state authority over cyber issues. The 2015 Group of Governmental Experts made incremental progress by recommending 11 voluntary, non-binding norms, rules, or principles of responsible behavior of states for consideration.[37] The 2016-2017 Group of Governmental Experts failed to reach consensus and advance how international law applies in cyberspace.

Research has shown that certain states are critical to norm adoption — particularly those states without which the achievement of the substantive norm goal is compromised, either because they possess the capabilities or engage in the behavior the norm is intended to regulate, or because they possess a moral stature in the view of most members of the community.[38] Clearly, China and Russia qualify as critical

34 The White House, Office of the Press Secretary, "Press Conference by President Obama after G20 Summit," Sept. 5, 2016, https://obamawhitehouse.archives.gov/the-press-office/2016/09/05/press-conference-president-obama-after-g20-summit.

35 Elvira Rosert, "Norm Emergence as Agenda Diffusion: Failure and Success in the Regulation of Cluster Munitions," *European Journal of International Relations* 25, no. 4 (2019): 1103-1131, https://doi.org/10.1177%2F1354066119842644.

36 U.N. General Assembly, "Group of Governmental Experts," 2013.

37 U.N. General Assembly, "Group of Governmental Experts," 2015.

38 Finnemore and Sikkink, "International Norm Dynamics," 901.

states because of their cyberspace capabilities and willingness to use them, yet neither are signatories to the Budapest Convention on Cybercrime. States opposed to a particular norm may be motivated to adhere to it because they identify as a member of an international society and thus will behave in a manner conducive to cementing their status within that society.[39] China, in particular, wants to be accepted as a member of international society but as a norm maker, not a norm taker: It does not wish to yield to the self-interested standards of liberal states.[40] China is currently acting on the belief that it can shape norms to serve its specific interests.

America's approach to building cyber norms should adapt to the following realities. First, the United States is not in a hegemonic position to define the agenda for norms in cyberspace. For a single actor to set the public agenda and drive a convergence of behavior, it would need to have control over the primary incentives and disincentives within the system, which the United States does not possess. Nor is there a clear manner in which the United States could obtain such primary control, due to the highly diffuse nature of cyberspace. Second, what is and what is not currently acceptable varies greatly depending on national perspectives, even among liberal democratic states. Despite the stated desire of the United States to establish norms through international cooperation, such norms have not emerged. The result is intense competition to drive a convergence of expectations on behavior in cyberspace.

An alternative yet related approach to building norms is to model good behavior. Convergence of norms will occur over time as other actors see that more beneficial outcomes flow from modelled good behavior than from bad behavior. This approach presents several challenges. First, behavior that might be categorized as unacceptable still produces benefits that outweigh costs. Second, adversaries cite various allegations of American bad behavior in cyberspace — global surveillance and the Stuxnet hack of the Iranian nuclear program are two examples — in labeling the United States a hypocritical standard-bearer for norms. Third, as both state and nonstate actors continue to advance their interests through behaviors that the United States considers unacceptable, modelling can easily be misunderstood as tacit acceptance.[41]

A third approach is reaction to a massively disruptive or destructive event that galvanizes global attention. This is how norms against genocide were set after the Holocaust. This approach presents obvious challenges. Relying on disaster to set norms is not an acceptable strategy. Nor does it seem likely that cyber capabilities will generate the level of abhorrence that characterize attitudes toward nerve agents, for example, and which have led to self-imposed proscriptions on their use.[42]

A fourth approach is for convergence of expectations to organically evolve through interaction. Common law demonstrates how norms emerge through practice and mature through political and legal discourse. The process of norm convergence for cyberspace has been troubling, however. For the last 10 years, the United States has witnessed the emergence of de facto norms antithetical to U.S. interests, defined by massive theft of intellectual property, expanding control of internet content, attacks on data confidentiality and availability, violations of privacy, and interference in democratic debates and processes. These activities have become normalized because the United States did not push back on them persistently and early on.[43] This has encouraged more experimentation and envelope-pushing short of armed conflict. Conversely, if the United States began countering such practices, it could help to counteract this trend and encourage a form of normalization more suited to meeting U.S. interests.

These pathways can be mutually reinforcing. The first two approaches have largely succeeded with U.S. allies and partners, but important differences with major competitors remain. Existing conditions do not allow the United States to dictate norm adoption: The opening decades of the 21st century are not the late 1940s, and no state is sufficiently powerful to dictate the rules of the road. Moreover, the third approach may be inoperable. Waiting for a disaster is politically and morally problematic. The fourth approach of "normalization" holds more promise for engaging with competitors and steering Moscow and Beijing toward preferred norms. Norms are constructed through "normal" practice and then become codified in in-

39 Finnemore and Sikkink, "International Norm Dynamics," 902.

40 Ian Clark, "International Society and China: The Power of Norms and the Norms of Power," *The Chinese Journal of International Politics* 7, no. 3 (Autumn 2014): 315–340, https://doi.org/10.1093/cjip/pot014.

41 I am indebted to Richard Harknett for these insights.

42 Scott N. Romaniuk and Francis Grice, "Norm Evolution Theory and World Politics," *E-International Relations*, Nov. 15, 2018, https://www.e-ir.info/2018/11/15/norm-evolution-theory-and-world-politics/.

43 Martin C. Libicki, "Norms and Normalization," *The Cyber Defense Review* (Spring 2020): 41-52, https://cyberdefensereview.army.mil/Portals/6/CDR%20V5N1%20-%2004_Libicki_WEB.pdf.

ternational agreements. By persistently engaging and contesting cyberspace aggression, the United States can draw parameters around what is acceptable, nuisance, unacceptable, and intolerable. The United States should not abandon U.N. First Committee processes on responsible state behavior in cyberspace, or other avenues for socialization such as international institutions or cyber capacity-building programs. But to be more effective, explicit bargaining can be reinforced by tacit bargaining through maneuver with non-likeminded states in the strategic space below armed conflict.[44] Diplomats have an important role to play in this process, by engaging directly with opponents and communicating and explaining U.S. preferences to allies and partners.[45] Diplomats can also assist by mobilizing coalitions — of governments, industries, academia, and citizenry, at home and abroad — for competition with ideological foes.

Scoping Deterrence

Another major thrust in the State Department's cyber diplomacy is developing and socializing an international cyber deterrence initiative.[46] The 2018 *U.S. National Cyber Strategy* asserts that, "the imposition of consequences will be more impactful and send a stronger message if it is carried out in concert with a broader coalition of like-minded states." Therefore, "the United States will launch an international Cyber Deterrence Initiative to build such a coalition ... The United States will work with like-minded states to coordinate and support each other's responses to *significant malicious cyber incidents*."[47] The cyber deterrence initiative is a U.S. government-wide, State Department-led initiative with other agencies, including the Department of Defense, proposing for consideration options for use in response to a significant cyber incident. However, the preponderance of cyberspace aggression falls outside the initiative's purview.

The cyber deterrence initiative strives for collective attribution and responses when norms are violated. It concentrates on responding to significant cyber incidents, which aligns with deterrence strategy's focus on reaction and episodic contact. Yet the empirical reality in cyberspace is that adversaries are continuously operating against the United States and its allies outside of armed conflict. Strategic significance in cyberspace, moreover, is not the result of any single event, but stems from the cumulative effect of a campaign comprising many individually less-consequential operations and activities carried out toward a coherent strategic end. A strategy based on response after the fact to significant incidents is not flexible enough to address most malicious cyber activity. Deterrence has conspicuously failed to prevent cyberspace aggression where it is most prevalent — outside of armed conflict — yet the deterrence frame, rather than the realities of strategic cyber competition, continues to guide key elements of U.S. cyber diplomacy.[48]

In 2018, the Department of Defense concluded that measures to ensure deterrence of significant cyber incidents (i.e., cyber "armed-attack" equivalent operations) should be pursued in tandem with steady, sustained activities that persistently contest and frustrate adversary cyberspace campaigns below the level of armed conflict.[49] As a result, the department adopted the strategy of "defend forward" and the operational approach of "persistent engagement."[50] These represent an important pivot in how the Department of Defense handles cyber threats. As the leader of U.S. Cyber Command Gen. Paul Nakasone explained:

> To defend critical military and national interests, our forces must operate against our enemies on their virtual territory as well. ...

44 Michael P. Fischerkeller and Richard J. Harknett, "Persistent Engagement and Tacit Bargaining: A Path Toward Constructing Norms in Cyberspace," *Lawfare*, Nov. 9, 2018, https://www.lawfareblog.com/persistent-engagement-and-tacit-bargaining-path-toward-constructing-norms-cyberspace.

45 Laura Bate, Phoebe Benich, Val Cofield, Karrie Jefferson, Ainsley Katz, and Sang Lee, "Defending Forward by Defending Norms," *Lawfare*, March 11, 2020, https://www.lawfareblog.com/defending-forward-defending-norms.

46 Theresa Hitchens, "US Urges 'Like-Minded Countries' to Collaborate on Cyber Deterrence," *Breaking Defense*, April 24, 2019, https://breakingdefense.com/2019/04/us-urging-likeminded-countries-to-collaborate-on-cyber-deterrence/.

47 *National Cyber Strategy*, 21. Emphasis added by author.

48 It also pervades the Cyberspace Solarium Commission, as James Lewis cogently explains; see, Lewis, "Cyber Solarium and the Sunset of Security." A focus on "attacks of significant consequence" by Cyberspace Solarium Commission staff reveal that they have not internalized core tenets of cyber competition. See, Laura Bate et al., "Defending Forward by Defending Norms."

49 Richard J. Harknett and Michael P. Fischerkeller, "Deterrence is Not a Credible Strategy for Cyberspace," *Orbis* 63, no. 1 (Summer 2017): 381-39, https://doi.org/10.1016/j.orbis.2017.05.003.

50 "Defend forward" and "persistent engagement" are new terms that were introduced into the Defense Department lexicon in 2018. Both terms first appear in the U.S. Cyber Command Vision released in March 2018. Defend forward next appears in the *Department of Defense Cyber Strategy* released in September 2018. See, Department of Defense, *Summary: Department of Defense Cyber Strategy 2018*, 2018; U.S. Cyber Command, *Achieve and Maintain Cyber Superiority: Command Vision for US Cyber Command*, March 2018, https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf?ver=2018-06-14-152556-010.

DEPARTMENT OF DEFENSE AND STATE DEPARTMENT EFFORTS TO COUNTER MALICIOUS CYBERSPACE BEHAVIOR SHOULD BE MUTUALLY REINFORCING INSTEAD OF PROCEEDING IN PARALLEL.

> We cannot afford to let adversaries breach our networks, systems, and data (intellectual property and personally identifiable information). If we are only defending in "blue space," we have failed. We must instead maneuver seamlessly across the interconnected battlespace, globally, as close as possible to adversaries and their operations, and continuously shape the battlespace to create operational advantage for us while denying the same to our adversaries.[51]

Nakasone has emphasized that persistent engagement is the doctrine by which U.S. cyber forces compete with adversaries in cyberspace.[52]

Defend forward and persistent engagement depart from the 2015 *Department of Defense Cyber Strategy*'s "doctrine of restraint" and from the 2011 *International Strategy for Cyberspace*'s reliance on "credible response options" to dissuade and deter — passive approaches based on threats of prospective action and episodic response after a declared threshold has been crossed.[53] They also depart from policy guidance that had confined cyber operations to the Department of Defense information networks, including rules limiting cyber activities to the support of military operations within areas of declared hostilities and responding to cyber attacks of significant consequence.

The Department of Defense's pivot hinged on several insights. First, the pivot acknowledges the fact that traditional doctrines designed for the physical domains do not align to the strategic imperatives and operational realities of cyberspace.[54] Second, the department's new strategy recognizes that in cyberspace, costs and benefits can be cumulative. Thus, it is insufficient to concentrate on individually significant incidents or catastrophic attacks when ongoing campaigns comprised of activities whose effects never rise to the level of a significant incident, and therefore rarely generate a timely response, cumulatively produce strategic gains. Third, the new approach incorporates the idea that relying on threats to impose consequences after the fact cedes initiative and lets adversaries set norms by default.

The Defense Department's cyber strategy is also informed by real-world experience. Operation Glowing Symphony was U.S. Cyber Command's first global-scale operation, which aimed to persistently disrupt and degrade Islamic State infrastructure worldwide. This and other operations gave U.S. Cyber Command, as well as the Department of Defense, confidence in its tactics, organization, and capabilities. It also engendered a feeling for how campaigns can be won in cyberspace by seizing and retaining the operational initiative. Nakasone (then commander of Joint Task Force-Ares) observed, "The first thing we learned the day after OGS [Operation Glowing Symphony] is this idea that threats are not going to stop after one engagement. This is going to be continuous. This is going to require our persistence."[55] What began as a 10-minute operation grew into a seven-month campaign and dramatically reduced the scale and speed of the virtual caliphate.[56] Operations in advance of the 2018 U.S. congressional elections further validated the notion that persistent engagement could disrupt cyber aggression without escalating to armed conflict.[57]

Department of Defense and State Department efforts to counter malicious cyberspace behavior should be mutually reinforcing instead of proceeding in parallel. The core objective of the 2018 *National Cyber Strategy's* "Pillar III: Preserve Peace through Strength" is "Identify, counter, disrupt, degrade, and deter behavior in cyberspace that is destabilizing and contrary to national interests, while preserving United States overmatch in and through cyberspace."[58] Specific guidance in that pillar was adopted by the State Department and informed the launch of the cyber deterrence initiative in support of the objective of deterrence. But deterrence was not the only objective laid out in the strategy. The Department of Defense chose to address deterrence *and* to counter, disrupt, and degrade hostile cyber-

51 Paul M. Nakasone, "A Cyber Force for Persistent Operations," *Joint Forces Quarterly* 92, no. 1 (2019), 12-13, https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-92/jfq-92_10-14_Nakasone.pdf.

52 Paul M. Nakasone and Michael Sulmeyer, "How to Compete in Cyberspace: Cyber Command's New Approach," *Foreign Affairs*, Aug. 25, 2020, https://www.foreignaffairs.com/articles/united-states/2020-08-25/cybersecurity.

53 Defend forward and persistent engagement do not reject a deterrence strategy entirely. The United States is deterring cyber aggression that causes death and destruction. Defend forward and persistent engagement were adopted to address continuous cyberspace campaigns and operations in the strategic competition space below the level of armed conflict.

54 Harknett and Fischerkeller, "Deterrence is Not a Credible Strategy for Cyberspace."

55 Text of Interview of Gen. Paul M. Nakasone with *NPR*, Aug. 7, 2019 (not published).

56 Darknet Diaries, "Operation Glowing Symphony," *Malicious Life*, https://malicious.life/episode/episode-76/.

57 Ellen Nakashima, "U.S. Cyber Command Operation Disrupted Internet Access of Russian Troll Factory on Day of 2018 Midterms," *Washington Post*, Feb. 27, 2019, https://www.washingtonpost.com/world/national-security/us-cyber-command-operation-disrupted-internet-access-of-russian-troll-factory-on-day-of-2018-midterms/2019/02/26/1827fc9e-36d6-11e9-af5b-b51b7ff322e9_story.html.

58 *National Cyber Strategy*, 20.

space behavior in its 2018 cyber strategy pivot.

The Department of State should contribute more directly to efforts to disrupt, degrade, and contest malicious cyberspace behavior. It can do so by leveraging diplomatic channels to increase routine and agile collaboration with partners and allies for continuous pressure against adversary campaigns below the level of armed conflict. The goal would be to frustrate and thwart cyberspace aggression before it harms the United States and its allies. This approach would allow the United States to be more responsive to great-power competition, enable and sustain similar efforts by the Department of Defense, and complement the cyber deterrence initiative. Closer synergy between promoting norms of responsible state behavior in international venues and conducting persistent cyberspace operations that expose and contest behavior inconsistent with such norms has the best chance of producing a convergence of expectations (i.e., norms) on acceptable behavior. Mutually reinforcing efforts across the U.S. government to deter, disrupt, expose, and contest malicious cyberspace behavior can produce the synergy between defense and foreign policy needed for great-power competition. This, however, requires a reevaluation of cyber diplomacy priorities, activities, lines of effort, and mindset.[59]

Cyber Diplomacy for Great-Power Competition: Seizing and Sustaining Initiative

Political conditions today favor an energetic U.S. diplomatic campaign. Russia and China's aggressive information, political, and economic warfare campaigns have highlighted the risks to U.S. partners and allies.[60] Those allies are eager to improve their cyberspace security and to work cooperatively with the United States. The U.S. government can capitalize on this favorable environment by forging agreements with foreign partners that encourage a deeper level of interaction. The United States can build coalitions for continuous pressure against adversary cyberspace campaigns outside of armed conflict.[61] Such agreements and the joint efforts that follow will normalize collaborative cyberspace operations for mutual defense.

Essentially, the State Department needs to operationalize the core objective of cyber persistence: seizing and sustaining initiative. The State Department is uniquely positioned to convene interagency discussions on defining boundaries of acceptable behavior below the level of armed conflict, to forge consensus with allies and partners on boundaries of acceptable competition, and to mobilize international coalitions to enforce those boundaries. It can better enable the Department of Defense to persistently engage and defend forward in cyberspace below the level of armed conflict — a necessary ingredient for constructing norms through interaction. Diplomats should be well-versed in the full range of U.S. cyber activities and explain them to U.S. partners in order to set the international conditions for the United States to compete in a globally interconnected domain. With these goals in mind, the following recommendations are offered as a roadmap for improving U.S. cyber diplomacy.

Communicate and Build Consensus

The State Department's foreign service officers forward-deployed as "cyber diplomats" can strengthen consensus among allies and partners on the nature of the cyber security problem and on the need for action to address it. To do so, they should be conversant with the U.S. government's efforts to address cyber competition and armed with information to speak authoritatively about them. The State Department has long promoted a framework for responsible state behavior in cyberspace. The key elements of that framework include: (1) affir-

59 Laura Bate et al., "Defending Forward by Defending Norms."

60 China, Russia, and Iran are currently executing widescale disinformation and influence operations around coronavirus. See, U.S. Department of State, "Briefing on Disinformation and Propaganda Related to COVID-19," Lea Gabrielle, Special Envoy and Coordinator of The Global Engagement Center, March 27, 2020, https://www.state.gov/briefing-with-special-envoy-lea-gabrielle-global-engagement-center-on-disinformation-and-propaganda-related-to-covid-19/. See also, Julian E. Barnes, Matthew Rosenberg, and Edward Wong, "As Virus Spreads, China and Russia See Openings for Disinformation," *New York Times*, March 28, 2020, https://www.nytimes.com/2020/03/28/us/politics/china-russia-coronavirus-disinformation.html; Sarah Jacobs Gamberini and Amanda Moodie, "The Virus of Disinformation: Echoes of Past Bioweapons Accusations in Today's Covid-19 Conspiracy Theories," *War on the Rocks*, April 6, 2020, https://warontherocks.com/2020/04/the-virus-of-disinformation-echoes-of-past-bioweapons-accusations-in-todays-covid-19-conspiracy-theories/.

61 The 5G campaign reflects this new set of priorities but it should be set within the broader context of strategic cyber competition to counterbalance the market incentives for partners to adopt Huawei in their 5G networks.

mation that established principles of international law apply to state behavior in cyberspace;[62] (2) adherence to certain non-binding norms of state behavior in cyberspace during peacetime; and (3) consideration, development, and implementation of practical confidence-building measures to reduce the risk of conflict in cyberspace. Since not all states share American views on responsible behavior in cyberspace, the United States is working with partners and allies on collective attribution and imposition of consequences.

These initiatives are now being complemented by the Department of Defense's strategy of defend forward and U.S. Cyber Command's operational approach of persistent engagement. The State Department and United States Agency for International Development (USAID) officers in missions around the world need to be well-versed in these other efforts and prepared to explain them to foreign partners on a routine basis. America's partners want to understand U.S. government strategy and policies.[63] It is U.S. policy that cross-domain responses to cyber aggression should be complemented with steady and sustained activities to make networks more resilient, to defend them as far forward as practicable, and to contest the most dangerous adversaries.[64] Every diplomatic engagement that includes cyber issues would be an opportunity to build support for these mutually reinforcing approaches.

Bolster Cyber Cadre

The greatest talent, most consequential research and development, and most innovative applications of cyber and other emerging technologies are globally distributed across individuals, commercial entities, governments, and academia. Competing successfully requires recognizing, understanding, and leveraging insights and advances wherever they reside in real time. The nation that best understands and can most rapidly harvest the benefits of changing knowledge (e.g., quantum encryption, artificial intelligence, machine learning, high performance computing, big data, 5G) will be best positioned to secure its future. Conversely, states that lag behind competitors will find closing gaps a daunting and risky challenge. 5G represents the proverbial canary in the coal mine because the United States lags behind China in deployment. Unless the United States ensures the talent is in place to monitor and lead on future technologies, it may again be caught unprepared.

The State Department does designate foreign service officers with a cyber portfolio, but they are usually assigned as an additional duty, often to economic officers at embassies and consulates. One option would be a dedicated cadre of "cyber diplomacy-coned" officers,[65] or even a regional dedicated officer cadre located at a large or strategic embassy in each region to augment the part-time officers at post. These cyber diplomacy-coned foreign service officers would report on priorities and trends in research and investments across governments, industries, academia, and research institutes worldwide, and identify where adversary regimes are vulnerable to diplomatic, information, military, and economic threats.[66] They would "identify and catalyze opportunities," in the words of the *U.S. National Security Strategy*,[67] helping to set the conditions for competition by building mechanisms for information sharing and agile collaboration.

Enable Defend Forward

The *U.S. National Cyber Strategy's* guidance to promote a framework of responsible state behavior in cyberspace, one that ensures there are consequences for irresponsible behavior, is a key objec-

62 Harold Hongju Koh, Legal Advisor U.S. Department of State, "International Law in Cyberspace," USCYBERCOM Inter-Agency Legal Conference, Sept. 18, 2012, https://2009-2017.state.gov/s/l/releases/remarks/197924.htm. "Question 1: Do established principles of international law apply to cyberspace? Answer 1: Yes, international law principles do apply in cyberspace. Everyone here knows how cyberspace opens up a host of novel and extremely difficult legal issues. But on this key question, this answer has been apparent, at least as far as the U.S. Government has been concerned. Significantly, this view has not necessarily been universal in the international community. … But the United States has made clear our view that established principles of international law do apply in cyberspace."

63 Partners want to understand U.S. strategy and policy as articulated in official government guidance, in legal authorities, and in executed operations. This should be distinguished from independent studies and recommendations, like the *Cyberspace Solarium Commission* report, which are likely to confuse partners by redefining concepts, such as defend forward, that are already delineated in official guidance and widely in use. Michael P. Fischerkeller, "The Cyberspace Solarium Commission Report and Persistent Engagement," *Lawfare*, March 23, 2020, https://www.lawfareblog.com/cyberspace-solarium-commission-report-and-persistent-engagement.

64 National Security Presidential Memorandum (NSPM) 13, passed in August 2018, gives the Defense Department the authorities to conduct daily cyberspace operations within very specific parameters. See, Mark Pomerlau, "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/.

65 U.S. foreign service officers can serve in one of five career tracks, or "cones," as political, economic, consular, management, or public diplomacy officers.

66 DIME reflects the instruments of national power which are all the means available to a government in its pursuit of national objectives. U.S. Joint Chiefs of Staff, *Doctrine for the Armed Forces of the United States*, July 12, 2017, GL-8, https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp1_ch1.pdf.

67 *National Security Strategy*, 33.

tive for the United States. To succeed, this framework should be pursued in tandem with an active approach to stem ongoing adversary cyberspace campaigns outside of armed conflict. The Department of Defense is now defending forward, outside its existing networks, to mitigate threats before they reach the United States. It is time for the State Department to join in these efforts.

An informal division of labor currently exists between the departments of State and Defense, whereby the former promotes norms in traditional diplomatic channels while the latter pursues defend forward through military channels. Yet this leaves several problems unresolved. Parallel communication increases the risk of messaging fratricide across military and diplomatic channels in partner nations. Military cyber operations may engage foreign policy sensitivities that the State Department is better equipped to address. On the other hand, State Department desk officers may throw a wrench into planning because they do not understand Defense Department strategy.

The United States needs to operate continuously alongside allies and partners. Leadership from the State Department can increase the speed, agility, and scale of defend forward activities and operations by working through diplomatic channels to set the conditions for the United States to operate by, with, and through foreign partners and their networks in order to expose, contest, and defend against adversary cyber aggression. Sustained diplomacy can help institutionalize these operational partnerships and make defend forward more anticipatory and effective. Institutionalized cooperation, including the conduct of joint and coalition operations and the development of agreed-upon legal and policy frameworks, is essential to prevail in long-term strategic competition.

The State Department can set the conditions for consensual foreign partner-enabled discovery operations (i.e., "hunt forward" operations) through bilateral engagements.[68] These operations enable the United States and its partners to understand an adversary's tactics, techniques, and procedures. This will in turn enable network defense of U.S. partners, improve anticipatory resilience of U.S. and partner networks, and thwart cyberspace aggression. The State Department can scale the process of explaining the Defense Department's defend forward strategy, enabling the United States to proactively set the conditions for "hunt forward" operations. The State Department can also actively ensure Defense Department cyber teams receive support from U.S. embassy country teams and benefit from insights about foreign partner networks gained through State and USAID-led cyber security capacity-building programs.

LEADERSHIP FROM THE STATE DEPARTMENT CAN INCREASE THE SPEED, AGILITY, AND SCALE OF DEFEND FORWARD ACTIVITIES AND OPERATIONS...

Mobilize Coalitions

The *National Security Strategy* calls on U.S. diplomats to "build and lead coalitions that advance shared interests" in the ongoing contests for power.[69] The State Department has a history of coalition building, most recently with the Global Coalition to Defeat ISIS formed in 2014. The State Department is thus uniquely positioned to mobilize partners to sustain pressure on adversary cyberspace behavior and cyber-enabled campaigns. A three-tiered coalition could increase information sharing, agile collaboration, and operational agility.

At the core of this coalition would be states that possess the capability and capacity to conduct full-spectrum cyberspace operations and work with diplomatic, law enforcement, and industry partners. A second tier would comprise less-capable or less-committed states that core states operate with (and through) to counter and contest aggression below the level of armed conflict. The United States has extensive experience negotiating basing and transit rights in sovereign territory along the Soviet perimeter during the Cold War. It should negotiate the cyber analogue of basing and transit rights to set the conditions for swift and persistent action. The transit issue is likely to be less controversial for allies and partners than remote cyber operations on infrastructure within another state's territory (addressed below).

68 "Hunt forward" operations deploy defensive cyber teams around the world at the invitation of allies and partners to look for adversaries' malicious cyber activity.

69 *National Security Strategy*, 33.

A third tier would comprise public and private actors across the broadest practicable set of countries in a resilience consortium to leverage collective market power, secure the internet, and counterbalance the illiberal vision of information control promoted by Russia and China.[70] This is especially urgent as countries shift from 3G and 4G (third and fourth generation) to 5G communications networks. By offering attractive financial terms, authoritarian governments can dominate the telecommunications industry in developing countries and control digital tools that increase censorship, repression, and surveillance. It is imperative that public and private actors assist the broader coalition in combating such trends.

THERE IS NO U.S. DECLARATORY POLICY ON THE SOVEREIGNTY IMPLICATIONS OF CYBER OPERATIONS.

Several pillars for a resilience consortium already exist. Cyber security capacity-building received a boost when the State Department and USAID launched the Digital Connectivity and Cybersecurity Partnership in July 2018, with a focus on the Indo-Pacific region.[71] In July 2019, USAID launched a development framework called Countering Malign Kremlin Influence. The framework was designed to build the economic and democratic resilience of countries targeted by Russia. Cyber security is considered high priority.[72] The launch of the U.S. Development Finance Corporation in October 2019 can attract private capital flows into contested markets to stem the spread of surveillance networks.[73] In November 2019, the United States, Australia, and Japan announced the Blue Dot Network to promote high-quality and trusted standards for global infrastructure development as an alternative to the predatory lending and debt-trap diplomacy of China's Belt and Road Initiative.[74] By re-prioritizing emerging market economies for affordable and reliable internet access and infrastructure, the United States can shore up internet freedom, ensure economic prosperity for the United States and its partners, and secure the outer ring of telecommunications networks as America's first line of cyber defense.

Another important initiative is the Clean Network program. Building upon the 5G Clean Path initiative, the Clean Network is a comprehensive effort by a coalition of like-minded countries and companies to secure their critical telecommunications, cloud, data analytics, mobile apps, Internet of Things, and 5G technologies from malign actors. The coalition relies on trusted vendors that are not subject to unjust or extra-judicial control by authoritarian governments.[75] Five new lines of effort were recently announced to ensure telecommunication carriers, mobile app stores, apps, cloud-based systems, and undersea cables are all rooted in digital trust standards.[76] More than 30 countries and territories are now Clean Countries, and many of the world's biggest telecommunications companies are Clean Telcos.[77] These efforts have laid the foundation for a broader coalition the State Department could mobilize to implement competitive cyber strategies.

70 Chris C. Demchak, "Three Futures for a Post-Western Cybered World," *Military Cyber Affairs* 3, no. 1 (2018), https://scholarcommons.usf.edu/cgi/viewcontent.cgi?article=1044&context=mca.

71 USAID, "Advancing Digital Connectivity in the Indo-Pacific Region," https://www.usaid.gov/sites/default/files/documents/1861/USAID_DCCP_Fact_Sheet_080719f.pdf.

72 USAID, "USAID Administrator Mark Green's Remarks on Countering Malign Kremlin Influence," July 5, 2019, https://www.usaid.gov/news-information/press-releases/jul-5-2019-administrator-mark-greens-remarks-countering-malign-kremlin-influence; USAID, "Remarks by Assistant Administrator Brock Bierman at the German Marshall Fund: USAID's Countering Malign Kremlin Influence Development Framework," Oct. 1, 2019, https://www.usaid.gov/news-information/speeches/remarks-assistant-administrator-brock-bierman-german-marshall-fund-usaids.

73 Daniel F. Runde, "America's Global Infrastructure Opportunity: Three Recommendations to the New U.S. Development Finance Corporation," *Center for Strategic & International Studies*, April 11, 2019, https://www.csis.org/analysis/americas-global-infrastructure-opportunity-three-recommendations-new-us-development-finance.

74 U.S. Department of State, "Blue Dot Network," https://www.state.gov/blue-dot-network/.

75 U.S. Department of State, "The Clean Network," https://www.state.gov/5g-clean-network/.

76 U.S. Department of State, "Announcing the Expansion of the Clean Network to Safeguard America's Assets," Aug. 5, 2020, https://www.state.gov/announcing-the-expansion-of-the-clean-network-to-safeguard-americas-assets/.

77 U.S. Department of State, "The Tide is Turning Toward Trusted 5G Vendors," June 24, 2020, https://www.state.gov/the-tide-is-turning-toward-trusted-5g-vendors/.

Accelerate Interagency Consensus on Conventions Below the Use of Force

What constitutes acceptable behavior in competition below the level of armed conflict? While there is a normative prohibition against crossing the threshold of armed conflict and while states appear to tacitly agree on many types of behavior that cross that threshold, the unilateral ingenuity states display in developing novel approaches to achieving strategic gains invites the potential for miscalculations on and around this threshold. Moreover, the strategic competitive space outside of armed conflict is still maturing. It is a space where the rules are malleable and where mutual understandings of acceptable and unacceptable behavior are few.[78]

The U.S. government needs to reach an interagency consensus on the preferred boundaries of acceptable behavior outside of armed conflict and promote them in international fora. The State Department is the natural leader for these efforts. Interagency discussions should proceed in tandem with consultations with the private sector. Currently, discussions with private sector entities all too often are isolated within individual agencies, with little coordination between agencies — even between the State Department and USAID. Agreed-upon conventions can then be reinforced by the actions of all departments and agencies. Working bilaterally, multilaterally, and through international institutions, the United States — led by the State Department — can influence and message what behaviors it views as unacceptable. This can help reduce the ambiguity that adversaries exploit, enhance the ability to build coalitions to support the U.S. view, and enable the United States to more effectively secure commitments from like-minded countries to impose consequences on those whose actions are counter to the principles.

However, the United States should first decide what it believes are the boundaries of acceptable and unacceptable behavior, which requires it to detail how national interests manifest in cyberspace and the security postures needed to defend those interests.[79] Other nations will need to do the same. The issue is where there is convergence, not just with like-minded states, but with adversaries. Examples that come to mind are the integrity of the global financial infrastructure; nuclear command, control, and communications; and disinformation that disrupts public health efforts — an issue which is of special relevance in light of the current global health crisis.[80]

Shape International Discourse on Cyber Operations and Sovereignty

One of the greatest concerns for allies and partners are operations that generate cyber effects outside U.S. military networks. These operations are designed to disrupt the ability of an adversary to conduct cyber operations against the United States and its allies — what the 2018 U.S. Cyber Command vision refers to as "contest."[81] There is no U.S. declaratory policy on the sovereignty implications of cyber operations. Specifically, the United States has not declared its position on whether remote cyber operations that generate effects on infrastructure within another state's territory require that state's consent. There is a divide among states on this issue, and on whether such acts require international legal justification. There is also divergence in state views on how international law applies to states' conduct of cyber operations below the threshold of a use of force and outside the context of armed conflict.[82] On one end of the spectrum is the United Kingdom, which has publicly declared that remote cyber operations below the non-intervention threshold are not prohibited by international law and do not require consent.[83] On the other end of the spectrum, the Netherlands agrees with the 2017 *Tallinn Manual 2.0 on the International Law Applicable to Cyber Opera-*

78 Dr. Catherine Lotrionte, "Reconsidering the Consequences for State-Sponsored Hostile Cyber Operations Under International Law," *Cyber Defense Review* 3, no. 2 (Summer 2018): 73-114, https://cyberdefensereview.army.mil/Portals/6/Documents/CDR%20Journal%20Articles/CDR_V3N2_ReconsideringConsequences_LOTRIONTE.pdf?ver=2018-09-05-084840-807.

79 For an approach to how the United States can identify how its national interests manifest in cyberspace, see, Jan-Philipp Brauchle, Matthias Gobel, Jens Seiler, Christoph Von Busekist, "Cyber Mapping the Financial System," *Carnegie Endowment for International Peace*, April 7, 2020, https://carnegieendowment.org/2020/04/07/cyber-mapping-financial-system-pub-81414.

80 Gary Corn, "Coronavirus Disinformation and the Need for States to Shore Up International Law," *Lawfare*, April 2, 2020, https://www.lawfareblog.com/coronavirus-disinformation-and-need-states-shore-international-law.

81 U.S. Cyber Command, *Achieve and Maintain Cyberspace Superiority*; Max Smeets, "Cyber Command's Strategy Risks Friction With Allies," *Lawfare*, May 28, 2019, https://www.lawfareblog.com/cyber-commands-strategy-risks-friction-allies.

82 Michael Schmitt, "The Netherlands Releases a Tour de Force on International Law in Cyberspace: Analysis," *Just Security*, Oct. 14, 2019, https://www.justsecurity.org/66562/the-netherlands-releases-a-tour-de-force-on-international-law-in-cyberspace-analysis/; Michael N. Schmitt, "Taming the Lawless Void: Tracking the Evolution of International Law Rules for Cyberspace," *Texas National Security Review* 3, no. 3 (Summer 2020), Published Online, https://tnsr.org/2020/07/taming-the-lawless-void-tracking-the-evolution-of-international-law-rules-for-cyberspace/.

83 Jeremy Wright, "Speech: Cyber and International Law in the 21st Century," United Kingdom Attorney General, May 23, 2018, https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century.

tions that such operations violate state sovereignty and require consent.[84]

The United Kingdom and the Netherlands have officially declared their respective positions and they have polar opposite views on this core question. Moreover, Estonia, Australia, and the United States have officially articulated their positions on the applicability of international law to cyber operations yet have not weighed in on this particular issue. Gary Corn considers this range of positions "*prima facie* evidence of the unsettled nature of the question."[85] The United States needs to seize the diplomatic initiative and publicly articulate its stance on this issue to help influence the court of world opinion. The most explicit official U.S. statement comes from the Department of Defense general counsel:

> For cyber operations that would not constitute a prohibited intervention or use-of-force, the Department believes there is not sufficiently widespread and consistent State practice resulting from a sense of legal obligation to conclude that customary international law generally prohibits such non-consensual cyber operations in another State's territory. This proposition is recognized in the Department's adoption of the "defend forward" strategy: "We will defend forward to disrupt or halt malicious cyber activity at its source, including activity that falls below the level of armed conflict." The Department's commitment to defend forward including to counter foreign cyber activity targeting the United States — comports with our obligations under international law and our commitment to the rules-based international order.[86]

This is an area where the State Department should be leading internationally if the United States hopes to persuade others to adopt its preferred norms, particularly as allies wrestle with legal ambiguities surrounding cyber operations.[87]

Adopt a Competitive Mindset

The 2018 *U.S. National Defense Strategy* challenged the Defense Department to adopt a "competitive mindset" in order to "out-think, out-maneuver, out-partner, and out-innovate" threat actors.[88] The department responded to this challenge. It reorganized, fielded new technologies and capabilities, created cross-functional teams that effectively work across traditional bureaucratic lines to prepare for long-term strategic challenges from China and Russia, and pivoted to the proactive cyber strategy of defend forward.

There is progress at the State Department in adapting to great-power competition. Secretary Mike Pompeo has given a series of speeches on the challenges posed by China, most forcefully on July 23, 2020, at the Nixon Presidential Library.[89] In 2019, all policy bureaus were directed to build strategic plans that prioritize competing with China.[90] China's challenge to the Western-led, liberal world order has impacted decisions on foreign assistance. USAID's "Clear Choice" framework provides alternatives in the energy, digital, and infrastructure sectors to China's development model.[91] The State Department-led campaign to convince countries to ban Huawei equipment from their 5G networks is bearing fruit as a growing number of states, including all members of the Five Eyes intelligence-sharing alliance, exclude Huawei from their 5G networks. China's crackdown in Hong Kong and its lack of transparency about the origins of the

84 The Netherlands, Ministry of Foreign Affairs, "Letter of 5 July 2019 from the Netherlands Minister of Foreign Affairs to the President of the House of Representatives on the International Legal Order in Cyberspace," 2019, https://www.government.nl/ministries/ministry-of-foreign-affairs/documents/parliamentary-documents/2019/09/26/letter-to-the-parliament-on-the-international-legal-order-in-cyberspace.

85 Gary Corn, "Punching on the Edges of the Grey Zone: Iranian Cyber Threats and State Cyber Responses," *Just Security*, Feb. 11, 2020, https://www.justsecurity.org/68622/punching-on-the-edges-of-the-grey-zone-iranian-cyber-threats-and-state-cyber-responses/.

86 Hon. Paul C. Ney, Jr., "DOD General Counsel Remarks at U.S. Cyber Command Legal Conference," March 2, 2020, https://www.defense.gov/Newsroom/Speeches/Speech/Article/2099378/dod-general-counsel-remarks-at-us-cyber-command-legal-conference/.

87 Matthias Schulze, "German Military Cyber Operations are in a Legal Gray Zone" *Lawfare*, April 8, 2020, https://www.lawfareblog.com/german-military-cyber-operations-are-legal-gray-zone.

88 *National Defense Strategy,* 5.

89 U.S. Embassy in Paraguay, "Speech of Secretary of State Michael R. Pompeo: The China Challenge," Oct. 30, 2019, https://py.usembassy.gov/speech-of-secretary-of-state-michael-r-pompeo-the-china-challenge/; U.S. Department of State, "U.S. States and the China Competition," Feb. 8, 2020, https://www.state.gov/u-s-states-and-the-china-competition/; U.S. State Department, "Communist China and the Free World's Future," July 23, 2020, https://www.state.gov/communist-china-and-the-free-worlds-future/.

90 U.S. Department of State, "Bureaucracy and Counterstrategy: Meeting the China Challenge," Sept. 11, 2019, https://www.state.gov/bureaucracy-and-counterstrategy-meeting-the-china-challenge/.

91 USAID, "U.S. Agency for International Development Administrator Mark Green's Interview with C-Span's 'Newsmakers' Host Susan Swain and Washington Post's Carol Morello and Wall Street Journal's Ben Kesling," Nov. 26, 2018, https://www.usaid.gov/news-information/press-releases/nov-26-2018-administrator-mark-green-interview-cspan-newsmakers/.

novel coronavirus no doubt added to concerns regarding the use of Chinese technology.[92]

Thus, the State Department has begun to adopt a competitive mindset. Yet much remains to be done. Framing the Huawei issue as a strategic competition over the future of digital governance and control of the global digital backbone, in addition to the security risks of embedding a Chinese provider into critical communications infrastructure, reflects a competitive mindset. So does the proactive approach of the Global Engagement Center, which leads interagency efforts to address foreign adversary disinformation and propaganda that undermines U.S. interests. Cyber diplomacy by the State Department needs to embrace this competitive mindset, and this will require reprioritizing resources and revisiting current lines of effort.

Conclusion: A State Department Cyber Strategy

A new bureau for cyberspace within the U.S. State Department can help to consolidate cyber issues. However, it will remain an incomplete effort, as cyber issues touch nearly every bureau and require a broad-based approach. This reflects the pervasiveness of digital technologies across all facets of human endeavor — economic, social, political, and security. It also reflects adversaries' integrated strategies that use cyberspace to gain strategic advantage and redefine the policies, principles, and standards of the global order. Consequently, no single bureau can manage the full panoply of cyber issues.

More importantly, making bureaucratic changes divorced of strategy is just rearranging deck chairs. The State Department should understand its role and then strategically reorient its bureaucracy to meet that strategy's objectives. A cyber strategy is not a panacea. However, properly applied across the whole department, an effective strategy would unify efforts and ensure the State Department's cyber priorities are aligned with the *National Security Strategy*'s focus on great-power competition, and improve coordination and integration — particularly between the Office of the Coordinator for Cyber Issues, which focuses on technical cyber incidents, and the Global Engagement Center, which focuses on information and influence operations. Like the Department of Defense, the Department of Homeland Security, USAID, and the Department of Justice have all produced department-wide cyber strategies or frameworks that are internally focused and externally nested.[93] An effective cyber strategy could build upon the progress the United States has already made and posture the nation to regain the initiative in cyberspace competition with authoritarian rivals. It should include the creation of a cyber diplomacy-coned career track for its foreign service officers. It should articulate how the State Department will lead, partner, and act in order to set the conditions for the United States to compete and sustain strategic advantage in cyberspace. And it should support U.S. government efforts to persistently counter and contest malicious foreign cyberspace campaigns and influence operations.

Adversaries of the United States and its allies and partners employ highly variable approaches, aligned to their national interests and competitive advantages against U.S. vulnerabilities across all elements of national power. Although competition in physical space is episodic, it is continuous in the cyber and information spaces where persistent campaigns gradually accrete meaningful advantage short of war. Without adopting and employing a proactive strategy against these threats across the whole of government, the United States may eventually find itself in a position of parity or even disadvantage with adversaries. In such a situation, emboldened adversaries will have shaped the competitive space to the point where they will have won without fighting.

Dr. Emily O. Goldman *is a cyber strategist and cyber persistence subject-matter expert at U.S. Cyber Command and the National Security Agency. From 2018 to 2019, she was cyber adviser to the director of policy planning at the U.S. Department of State. The opinions recorded in this essay are hers alone and do not necessarily reflect official positions of the Department of Defense or any other U.S. Government entity.*

Acknowledgements*: The author would like to thank the following people for helpful comments on earlier drafts: Jake Bebber, Amy Chao, Gary Corn, Chris Demchak, Michael Fischerkeller, Richard Harknett, James Lewis, Eduardo Monarez, Steven Rynecki, Max Smeets, Stafford Ward, and Michael Warner.*

Photo: Ron Przysucha / Public Domain

92 Ellen Nakashima and William Booth, "Britain Bars Huawei From Its 5G Wireless Networks, Part of a Growing Shift Away From the Chinese Tech Giant," *Washington Post*, July 15, 2020, https://www.washingtonpost.com/national-security/britain-to-bar-huawei-from-its-5g-wireless-networks-part-of-a-growing-shift-away-from-the-chinese-tech-giant/2020/07/13/44f6afee-c448-11ea-b037-f9711f89ee46_story.html.

93 U.S. Department of Homeland Security, *Cybersecurity Strategy*, May 15, 2018, https://www.dhs.gov/sites/default/files/publications/DHS-Cybersecurity-Strategy_1.pdf; USAID, "Draft USAID Digital Strategy," https://www.ictworks.org/wp-content/uploads/2019/10/USAID_Digital_Strategy_Draft.pdf; U.S. Department of Justice, Office of Public Affairs, "Attorney General Sessions Announces Publication of Cyber-Digital Task Force Report," July 19, 2018, https://www.justice.gov/opa/pr/attorney-general-sessions-announces-publication-cyber-digital-task-force-report.