CRAFTING A MULTILATERAL TECHNOLOGY AND CYBERSECURITY POLICY

ROBERT D. WILLIAMS

EXECUTIVE SUMMARY

Geo-technological changes are driving an array of economic, national security, and human rights concerns in U.S.-China relations. Calibrating technological competition and integration will be one of the foremost foreign policy challenges for the next administration, calling for a multifaceted U.S. strategy that prioritizes cooperation with allies and partners. The Trump administration's technology approach has relied disproportionately on unilateral measures instead of building coalitions of countries willing to adopt and enforce common rules and practices. U.S. policy should seek to protect American intellectual property and strategic technologies, sustain and strengthen the innovation ecosystem that makes those technologies possible and uphold American values of human rights, democracy, and the rule of law.

The task for a realistic foreign policy is to advance American interests and values through multilateral frameworks that recognize the extent to which these objectives are broadly shared. To that end, the next administration should pursue a robust policy agenda in the following categories:

- Establish a National Data Security and Privacy Framework
- Launch a Multilateral Digital Trade Initiative
- Impose Meaningful Penalties for Malicious Cyber Activity
- Revitalize International Law and Institutions Addressing New Technologies
- Empower a Dedicated Body for Internal and External Technology Policy Coordination

THE PROBLEM

In the years coinciding with China's dramatic rise in wealth and power, the world has witnessed a series of geo-technological changes. These changes include major advances in technological innovation owing to a range of factors such as an increase in global interconnectedness and the transnational flow of data and technology, increases in the availability of massive datasets, improvements in computing power, more robust and flexible machine-learning algorithms, and the availability of open source-code libraries and technical frameworks that allow software developers to leverage the work of others for new use cases.[1] In contrast to earlier periods, much of this technological innovation has been driven by the civilian sector, yet many of these advances involve inherently dual-use, "strategic" technologies that are important for national defense. This dynamic has contributed to a blurring of the distinction between economic and national security concerns, confronting policymakers with an innovation-security conundrum: How can strategically sensitive emerging technologies be protected without undermining the economic ecosystem that gives rise to their development?[2] One aspect of the conundrum is the worry that data privacy and national security are increasingly interconnected. Data (and data networks) can be exploited in ways that threaten security, but they also form the lifeblood of technological innovation on which both economic growth and national security depend.[3]

In tandem with these developments, there has been a long-term shift away from U.S. technological supremacy toward a more multipolar world in which no country is technologically self-sufficient and the global economy is physically and digitally integrated and interdependent. In addition, a relative decline in the significance of traditional military power and geopolitical competition has made economic and technological strength a more salient feature of competition among nation-states for political influence.[4] As a paradigmatic case of this interdependence and competition, the economies

of China and the United States have gone from largely complementary — with China supplying low-cost goods to American consumers and the United States providing capital to drive China's export-led growth — to increasingly competitive, with both countries seeking to secure their future prosperity through cutting-edge technologies and innovative capacity. This raises the stakes of longstanding, fundamental disagreements between the United States and China over the ground rules of economic competition, with each side viewing their equities in that competition as vital interests.

The Chinese practices of principal concern for U.S. policymakers were summarized in the U.S. Trade Representative's 2018 Section 301 report and the White House's 2020 summary of the "United States Strategic Approach to the People's Republic of China." These include concerns that the PRC "(1) requires or pressures United States companies to transfer their technology to Chinese entities; (2) places substantial restrictions on United States companies' ability to license their technology on market terms; (3) directs and unfairly facilitates acquisition of United States companies and assets by domestic firms to obtain cutting edge technologies; and (4) conducts and supports unauthorized cyber intrusions into United States companies' networks to access sensitive information and trade secrets."[5] Broadly framed, China has not fully lived up to its WTO commitments and other promises to respect U.S. intellectual property rights or to pursue technological competition on fair market terms.[6] A noteworthy example is the U.S. complaint that China has failed to abide by its 2015 pledge not to "conduct or knowingly support cyber-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors."[7]

Since at least 2016, an array of issues blending considerations of national security, human rights, and democratic integrity have been added to longstanding economic concerns. These include Chinese disinformation campaigns,[8] the prospect of Chinese interference in U.S. domestic politics,[9] and the export of Chinese censorship and surveillance practices along with the technologies that enable those practices.[10] These concerns are linked by the growing sense outside China that under Xi Jinping's authoritarian policies, the role of the state in China's economy and society has become more far-reaching and coercive; that digital integration with China exposes sensitive U.S. data and technology to actual and potential exploitation by the Chinese government; and that the PRC is pursuing a strategy of technological advancement at least partially at odds with U.S. interests and values.

These complex challenges call for a multifaceted U.S. strategy that recognizes the need for cooperation with allies and partners. On this score, the Trump administration has fallen short, despite its deployment of a wide range of policy tools, including export controls, investment screenings, and presidential emergency authorities. Some of these tools, such as immigration restrictions targeted at preventing "non-traditional collectors" in STEM disciplines, may fail to align means with ends.[11] For others, such as the new Department of Defense "defending forward" cyber strategy targeting persistent network-based threats,[12] a lack of accessible information may limit the public's ability to confidently evaluate the policy. In other areas, U.S. strategy appears incoherent. Take, for example, the approach of indicting-without-prosecuting Chinese hackers for cybertheft on U.S. networks: judging by its publicly stated aims (most notably, deterrence), that strategy appears to be a spectacular failure.[13]

Much of the Trump administration's technology strategy has relied too heavily on unilateral measures instead of building coalitions of countries willing to adopt and enforce common rules and practices. To date, the bilateral tariff war with China has damaged the U.S. economy without resolving structural issues relating to Chinese technology acquisition practices and industrial policies.[14] On cybersecurity, the Trump administration has focused disproportionate attention on specific Chinese companies such as Huawei and ByteDance but neglected the importance of creating a multilateral data protection framework that raises standards across the board for all entities.

The use of export controls has increased in relation to specific entities — most prominently, Huawei and its affiliates — but the Commerce Department has been slow in fulfilling its legislative mandate to broaden the scope of export controls involving "emerging and foundational technologies." This hesitation is due in part to concerns that new

controls will disadvantage U.S. firms, particularly if they are not closely coordinated with partner countries. Executive orders aimed at banning TikTok and WeChat have met with skepticism in allied capitals, where regulators appear unlikely to follow suit.[15] Finally, recent statements of U.S. policy have failed to adequately account for the benefits of technological integration with China, compounded by a failure to appreciate the extent to which U.S. allies are wary of disentanglement with China or a global bifurcation into dueling technological ecosystems.

OBJECTIVES

The objectives of a multilateral U.S. technology and cybersecurity policy are straightforward:

- Strengthen and defend American national security and economic prosperity
- Protect U.S. intellectual property and strategic technologies
- Sustain and strengthen the innovation ecosystem that makes those technologies possible
- Mitigate the risks of espionage, unlawful data exploitation, and sabotage or destruction on U.S. networks or through global supply chains
- Counter foreign disinformation campaigns and censorship on internet platforms that operate in the U.S. market
- Uphold American values of human rights, democracy, and the rule of law
- Prevent a global splintering into rival technological and information systems that would undermine these goals

RECOMMENDATIONS

In an interconnected world in which technological power and capabilities are distributed, none of the aforementioned objectives can be achieved unilaterally. And unilateral policy cannot realistically unwind globalization or interconnectedness. The task for a realistic foreign policy is to advance American interests and values through multilateral frameworks that recognize the extent to which these interests are broadly shared. To that end, the next administration should consider the following policy options:[16]

Establish a national data security and privacy framework: The next administration should work with Congress to enact legislation establishing a federal data protection framework that builds on the catalyzing functions of the California Consumer Privacy Act and the EU General Data Protection Regulation to set "highest common denominator" standards for data brokers operating in the U.S. market, regardless of national origin, while sustaining broadly free flows of data across national borders.[17] The legislation should include clear standards for the collection, processing, and sharing of personal information,[18] and it should be enforceable through a combination of federal regulatory powers and private rights of action.[19] Such legislation would not eliminate differences between the United States and its European allies on data governance, but it could help to narrow the gap and is important for U.S. interests in its own right.[20] At the same time, the U.S. should rationalize its cybersecurity liability regime. Following the recommendations of the Cyberspace Solarium Commission, the administration should work with Congress to pass a law "establishing that final goods assemblers of software, hardware, and firmware are liable for damages from incidents that exploit known and unpatched vulnerabilities."[21] Software vendors should be responsible for developing and distributing patches in a timely manner, and companies should be encouraged to disclose vulnerabilities and implement the basic steps needed to ensure they are regularly updating their systems. These duties of care could be accompanied by requirements for Internet-of-Things producers to certify the security of systems built into their products and to clarify cyber risks for consumers over the life cycle of their products.[22]

Launch a multilateral digital trade initiative: Improving domestic data governance should be viewed as predicate to a broader global strategy. In tandem with legislative reform at home, the United States should seek to find common ground on digital trade with countries that have strong commitments to data security and interoperability, inspired by Japan's proposal for "data free flow with trust."[23] Over the past four years, Washington has lost ground in setting the terms of debate on cross-border data flows. An enforceable digital

trade agreement among a club of like-minded nations could benefit American workers and the innovation base while creating long-term incentives for countries such as China to improve their domestic governance regimes and cut back on state-sponsored theft of foreign IP. The digital trade chapter of the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) largely coheres with provisions in the U.S.-Mexico-Canada Agreement[24] and the U.S.-Japan Digital Trade Agreement.[25] Short of joining CPTPP, the next administration could expand upon its digital trade chapter with more stringent and comprehensive rules to establish a standalone digital trade arrangement.

Impose meaningful penalties for malicious cyber activity: Chinese state-linked hackers have not been appreciably deterred by the recent spate of Justice Department indictments for cybertheft on U.S. networks where there is no realistic chance of extraditing or prosecuting the defendants.[26] Various public reports suggest the U.S. government may be expanding its "defend forward" strategy aimed at disrupting malicious cyber activities at their source, including activities below the threshold of armed conflict.[27] Although clear signaling is needed to ensure these actions do not spark escalation, the U.S. should expand such efforts to impose meaningful costs for specific, attributable incidents of cybertheft.[28] As a next step, Washington should work to organize a coalition of like-minded nations to enforce norms against commercial cybertheft. This could be done through discrete, targeted multilateral sanctions against entities that engage in and benefit from operations for which attribution can be accomplished publicly and jointly with partner governments.[29] Incentives could be offered for demonstrable changes in behavior. For example, existing tariffs could be eased in exchange for progress on IP theft and other practices. The U.S. and its partners could also consider arrangements that acknowledge (without morally sanctioning) China's existential concerns about the free flow of information threatening China's domestic social order. Such an arrangement might include, for example, a commitment to forgoing the government-sponsored provision of software tools that enable Chinese citizens to circumvent the Great Firewall *if and to the extent* that the PRC abandons state-sponsored IP theft and campaigns of disinformation and censorship in the U.S. market.[30]

Revitalize international law and institutions addressing new technologies: Recognizing the importance of cooperation on cybersecurity and emerging technologies, the U.S. should recommit to multilateral efforts such as the United Nations Group of Governmental Experts on developments in the field of information and communications technologies in the context of international security, which address norms, confidence-building measures, and the question of how international law applies to cyberspace and lethal autonomous weapons systems.[31] The next administration should make clear that it recognizes common interests with China and among all countries in the integrity and stability of the global financial system; in not being misled into armed conflict by third-party malefactors; in counter-proliferation measures to prevent cyber weapons or autonomous weapons systems from getting into the hands of malicious non-state actors; in better understanding how other countries approach legal-policy questions such as the definitions of "armed conflict" or "critical infrastructure" or "human control" over autonomous systems; and in cooperating to combat transnational cybercrime, among other objectives.[32] At the same time, the U.S. should spur the launch of a new multi-stakeholder initiative aimed at ensuring the scientific independence of international standard-setting bodies for 5G and other technologies, monitoring and publicizing efforts by governments and their proxies to manipulate technical standard-setting processes for political ends.[33] Similarly, the U.S. could coordinate the expansion of NATO's efforts on countering disinformation to like-minded nations in the Indo-Pacific and other regions.[34]

Empower a dedicated body for internal and external technology policy coordination: The next administration should consider establishing an interagency, CFIUS-like coordinating group to examine the practical implications of prospective technology policies such as export controls, entity listings, supply chain risk standards, immigration policies, subsidies, and more. Whether designed as a joint committee with a lead agency (perhaps housed in the Commerce Department) or as an expansion and elevation of the White House Office of Science and Technology Policy (with enhanced oversight power) or within the National Security Council, the group would seek to ensure that federal policies are as narrowly tailored as possible to protect sensitive technologies without cutting off

the lifeblood of their development: data, investment, and human capital.[35] Such an entity should have the flexibility to coordinate innovation policy proposals among allies and partners by proposing economic incentives for countries with varying threat perceptions to join together in adopting narrowly scoped technology protections while spurring intra-group cooperation through targeted bilateral and multilateral pooling of data, funding for innovation, and reduction of licensing and regulatory barriers to cooperation among allies in sensitive technologies.[36] The coordinating group could advise on multilateral principles for supply chain security, building on inclusive statements such as the May 2019 Prague Proposals[37] and the EU Toolbox on 5G Security.[38] It could guide joint funding for research and development on potential software-based solutions to 5G (and eventually 6G) cybersecurity.[39] And it could advise on how to craft sanctions and articulate clear diplomatic signals for entities that enable human rights abuses through the use of digital tools for surveillance and repression, especially in Xinjiang.[40] In carrying out these functions, the coordinating group would benefit from consulting a range of perspectives, including technical and subject-matter experts outside the federal government. Private-sector experts could be engaged in accordance with the Federal Advisory Committee Act to help decision-makers "game out" the downstream consequences of mooted policies and to calibrate strategies that account for the competing values and interests at stake.

REFERENCES

1 Greg Allen, "Understanding AI Technology," (Washington, DC: Department of Defense Joint Artificial Intelligence Center, April 2020), https://www.ai.mil/docs/Understanding%20AI%20Technology.pdf.

2 Robert D. Williams, "In the Balance: The Future of America's National Security and Innovation Ecosystem," *Lawfare*, November 30, 2018, https://www.lawfareblog.com/balance-future-americas-national-security-and-innovation-ecosystem; Robert D. Williams, "The Innovation-Security Conundrum in U.S.-China Relations," *Lawfare*, July 24, 2018, https://www.lawfareblog.com/innovation-security-conundrum-us-china-relations.

3 Robert D. Williams, "Reflections on TikTok and Data Privacy as National Security," *Lawfare*, November 15, 2019, https://www.lawfareblog.com/reflections-tiktok-and-data-privacy-national-security.

4 Harvey Brooks et al., *Mastering a New Role: Shaping Technology Policy for National Economic Performance* (Washington: National Academy Press, 1993), 28-60, https://www.nap.edu/read/2103/chapter/4.

5 "United States Strategic Approach to the People's Republic of China," The White House, May 2020, https://www.whitehouse.gov/wp-content/uploads/2020/05/U.S.-Strategic-Approach-to-The-Peoples-Republic-of-China-Report-5.20.20.pdf.

6 Bob Davis and Lingling Wei, *Superpower Showdown: How the Battle Between Trump and Xi Threatens a New Cold War* (New York: Harper Business, 2020).

7 "Fact Sheet: President Xi Jinping's State Visit to the United States," The White House, September 25, 2015, https://obamawhitehouse.archives.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states; Robert D. Williams, "The 'China, Inc.+' Challenge to Cyberspace Norms," (Stanford, CA: Hoover Institution, February 2018), https://www.hoover.org/sites/default/files/research/docs/williams_webreadypdf1.pdf.

8 Kate Conger, "Twitter Removes Chinese Disinformation Campaign," *The New York Times*, June 11, 2020, https://www.nytimes.com/2020/06/11/technology/twitter-chinese-misinformation.html.

9 Rush Doshi and Robert D. Williams, "Is China Interfering in American Politics?," *Lawfare*, October 1, 2018, https://www.brookings.edu/blog/order-from-chaos/2018/10/02/is-china-interfering-in-american-politics/; David E. Sanger and Julian E. Barnes, "U.S. Warns Russia, China and Iran Are Trying to Interfere in the Election. Democrats Say It's Far Worse.," *The New York Times*, July 24, 2020, https://www.nytimes.com/2020/07/24/us/politics/election-interference-russia-china-iran.html/.

10 Alina Polyakova and Chris Meserole, "Exporting digital authoritarianism: The Russian and

Chinese models," (Washington, DC: The Brookings Institution, August 2019), https://www.brookings.edu/research/exporting-digital-authoritarianism/; Sheena Chestnut Greitens, "Dealing with Demand for China's Global Surveillance Exports," (Washington, DC: The Brookings Institution, April 2020), https://www.brookings.edu/wp-content/uploads/2020/04/FP_20200428_china_surveillance_greitens_v3.pdf.

11 Christopher Wray, "Responding Effectively to the Chinese Economic Espionage Threat," (remarks, Washington, DC, February 6, 2020), https://www.fbi.gov/news/speeches/responding-effectively-to-the-chinese-economic-espionage-threat.

12 "Summary: Department of Defense Cyber Strategy," U.S. Department of Defense, 2018, https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF.

13 Jack Goldsmith and Robert D. Williams, "The Failure of the United States' Chinese-Hacking Indictment Strategy," *Lawfare*, December 28, 2018, https://www.lawfareblog.com/failure-united-states-chinese-hacking-indictment-strategy; Robert D. Williams, "America's Hopelessly Anemic Response to One of the Largest Personal-Data Breaches Ever," *The Atlantic*, February 12, 2020, https://www.theatlantic.com/ideas/archive/2020/02/whats-behind-the-indictment-of-the-equifax-hackers/606466/.

14 Ryan Hass and Abraham Denmark, "More pain than gain: How the US-China trade war hurt America," The Brookings Institution, August 7, 2020, https://www.brookings.edu/blog/order-from-chaos/2020/08/07/more-pain-than-gain-how-the-us-china-trade-war-hurt-america/.

15 Vincent Manancourt and Laura Kayali, "TikTok finds safe haven in Europe," *Politico*, August 6, 2020, https://www.politico.com/news/2020/08/06/tiktok-finds-safe-haven-in-europe-392274.

16 Aspects of these recommendations are drawn from the author's October 2020 working paper published by the University of Pennsylvania as part of its Project on the Future of U.S.-China Relations. See Robert D. Williams, "Beyond Huawei and TikTok: Untangling U.S. Concerns over Chinese Tech Companies and Digital Security," (Philadelphia, PA: University of Pennsylvania, October 2020), https://web.sas.upenn.edu/future-of-us-china-relations/technology-2/.

17 Anupam Chander, Margot E. Kaminski, and William McGeveran, "Catalyzing Privacy Law" (April 24, 2020), Minnesota Law Review, Forthcoming, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3433922.

18 Jennifer Daskal and Samm Sacks, "The Furor Over TikTok Is About Something Much Bigger," *Slate*, November 8, 2019, https://slate.com/technology/2019/11/tiktok-bytedance-china-geopolitical-threat.html.

19 In addition to supporting broad-based data protection legislation, the next administration should work with Congress to reform the Foreign Intelligence Surveillance Act (FISA) and consider adopting the recommendations of the Justice Department's Inspector General to improve public confidence in the FISA process. For examples of policy proposals along these lines, see Bob Bauer and Jack Goldsmith, "The FBI Needs to Be Reformed," *The Atlantic*, December 16, 2019, https://www.theatlantic.com/ideas/archive/2019/12/fisa-process-broken/603688/; Margaret Taylor, "The Senate Proposes Five Amendments to FISA Reform," *Lawfare*, May 12, 2020, https://www.lawfareblog.com/senate-proposes-five-amendments-fisa-reform; Elliot Setzer, "Justice Department Inspector General Finds Broader Pattern of Errors in FISA Applications," *Lawfare*, March 31, 2020, https://www.lawfareblog.com/justice-department-inspector-general-finds-broader-pattern-errors-fisa-applications.

20 Joshua P. Meltzer, "The Court of Justice of the European Union in Schrems II: The impact of GDPR on data flows and national security," *VoxEU*, August 5, 2020, https://voxeu.org/article/impact-gdpr-data-flows-and-national-security.

21 "Report of the United States Cyberspace Solarium Commission," (Washington, DC: U.S. Cyberspace Solarium Commission, March 2020), at 76, https://www.solarium.gov/report.

22 Robert D. Williams, "Securing 5G Networks: Challenges and Recommendations," Council on Foreign Relations, July 15, 2019, https://www.cfr.org/report/securing-5g-networks.

23 Nigel Cory, Robert D. Atkinson, and Daniel Castro, "Principles and Policies for 'Data Free Flow With Trust'," Information Technology & Innovation Foundation, May 27, 2019, https://itif.org/publications/2019/05/27/principles-and-policies-data-free-flow-trust.

24 "Comparison of Selected Digital Trade Provisions in the United States-Mexico-Canada Agreement (USMCA) and the Trans-Pacific Partnership (TPP)," The Software Alliance, April 11, 2019, https://www.bsa.org/files/policy-filings/04112019tppvusmcacomparison.pdf.

25 "Agreement Between the United States of America and Japan Concerning Digital Trade," January 1, 2020, https://ustr.gov/sites/default/files/files/agreements/japan/Agreement_between_the_United_States_and_Japan_concerning_Digital_Trade.pdf.

26 Goldsmith and Williams, "The Failure of the United States' Chinese-Hacking Indictment Strategy."

27 Erica D. Borghard and Mark Montgomery, "Defend Forward as a Whole-of-Nation Effort," *Lawfare*, March 11, 2020, https://www.lawfareblog.com/defend-forward-whole-nation-effort; Jeffrey A. Rosen, "Remarks by Deputy Attorney General Jeffrey A. Rosen at an Announcement of Charges and Arrests in Computer Intrusion Campaigns Related to China," (remarks, Washington, DC, September 16, 2020, https://www.justice.gov/opa/speech/remarks-deputy-attorney-general-jeffrey-rosen-announcement-charges-and-arrests-computer ("[T]he Department of Justice and the FBI have been working with seven private sector partners, including Microsoft Corporation, Google, Facebook, and Verizon Media, to identify and neutralize the computer infrastructure that APT-41 uses to conduct its crimes: its virtual private servers, malware, malicious domains, and other tools. We have done this through a combination of public and private actions, including technical measures to block this threat actor from accessing victims' computer systems, issuing a public safety announcement outlining their tactics, techniques, and procedures (to aid network defenders), and by taking control of, or otherwise disabling, their accounts pursuant to court orders or terms of service violations.").

28 Ben Buchanan and Robert D. Williams, "A Deepening U.S.-China Cybersecurity Dilemma," *Lawfare*, October 24, 2018, https://www.lawfareblog.com/deepening-us-china-cybersecurity-dilemma.

29 Lorand Laskai, "A New Old Threat: Countering the Return of Chinese Industrial Cyber Espionage," Council on Foreign Relations, December 6, 2018, https://www.cfr.org/report/threat-chinese-espionage.

30 Jack Goldsmith, "The Failure of Internet Freedom," Columbia University Knight First Amendment Institute, June 13, 2018, https://knightcolumbia.org/content/failure-internet-freedom ("Network interventions to promote freedom and democracy are not on the same moral plane as network interventions to disrupt or undermine democracy. But regardless of the morality of the situation, it is fanciful to think that the digitally dependent United States can continue its aggressive cyber operations in other nations if it wants to limit its own exposure to the same. Unless the United States can raise its cyber defenses or improve its cyber deterrence — a dim prospect at the moment — it will need to consider the possibility of a cooperative arrangement in which it pledges to forgo threatening actions in foreign networks in exchange for relief from analogous adversary operations in its networks.").

31 Nele Achten, "New U.N. Debate on Cybersecurity in the Context of International Security," *Lawfare*, September 30, 2019, https://www.lawfareblog.com/new-un-debate-cybersecurity-context-international-

security; Christian Ruhl, Duncan Hollis, Wyatt Hoffman, and Tim Maurer, "Cyberspace and Geopolitics: Assessing Global Cybersecurity Norm Processes at a Crossroads," Carnegie Endowment for International Peace, February 26, 2020, https://carnegieendowment.org/2020/02/26/cyberspace-and-geopolitics-assessing-global-cybersecurity-norm-processes-at-crossroads-pub-81110.

32 Buchanan and Williams, "A Deepening U.S.-China Cybersecurity Dilemma."

33 Jack Kamensky, "China's Participation in International Standards Setting: Benefits and Concerns for U.S. Industry," *China Business Review*, February 7, 2020, https://www.chinabusinessreview.com/chinas-participation-in-international-standards-setting-benefits-and-concerns-for-us-industry/.

34 "NATO's approach to countering disinformation: a focus on COVID-19," North Atlantic Treaty Organization, July 17, 2020, https://www.nato.int/cps/en/natohq/177273.htm. Recognizing the constitutional implications of speech regulation, such efforts should focus primarily on transparency and education around disinformation rather than government interventions to curate online speech.

35 Robert D. Williams, "In the Balance: The Future of America's National Security and Innovation Ecosystem."

36 Daniel Kliman, Ben FitzGerald, Kristine Lee, and Joshua Fitt, *Forging an Alliance Innovation Base*, (Washington, DC: Center for a New American Security, March 2020), https://s3.amazonaws.com/files.cnas.org/documents/CNAS-Report-Alliance-Innovation-Base-Final.pdf?mtime=20200329174909.

37 "Prague 5G Security Conference announced series of recommendations: The Prague Proposals," Government of the Czech Republic, March 3, 2019, https://www.vlada.cz/en/media-centrum/aktualne/prague-5g-security-conference-announced-series-of-recommendations-the-prague-proposals-173422/.

38 "Secure 5G Networks: Questions and Answers on the EU Toolbox," European Commission, January 29, 2020, https://ec.europa.eu/commission/presscorner/detail/en/qanda_20_127.

39 Dwight Weingarten, "Open RAN Bill Included in Senate NDAA, Sen. Warner Pushes for More Funding," *MeriTalk*, June 30, 2020, https://www.meritalk.com/articles/open-ran-bill-included-in-senate-ndaa-sen-warner-pushes-for-more-funding/.

40 "Xinjiang Supply Chain Business Advisory," U.S. Department of State, July 1, 2020, https://www.state.gov/xinjiang-supply-chain-business-advisory/.