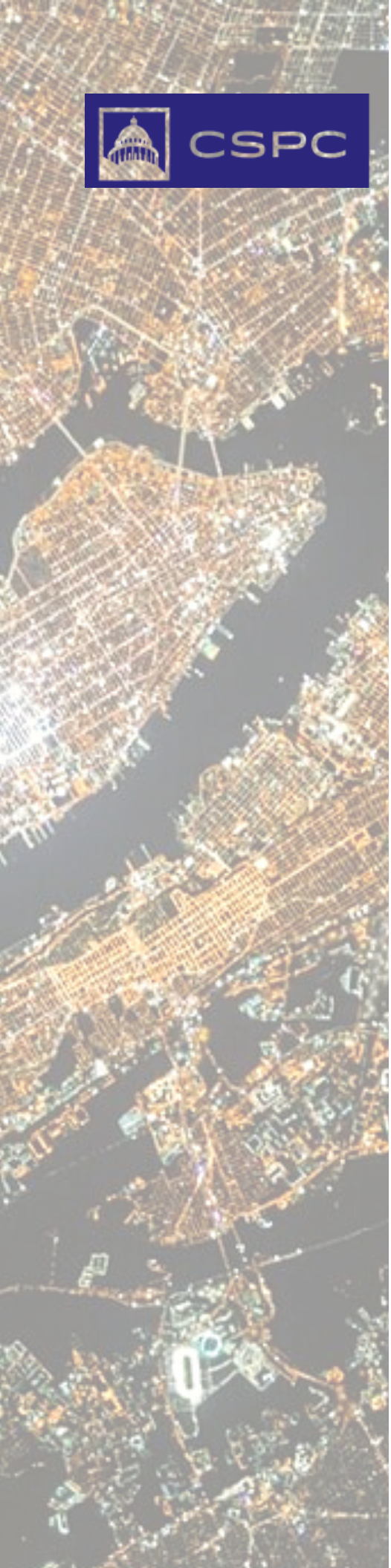

CSPC

CENTER FOR THE STUDY OF THE PRESIDENCY & CONGRESS

GEOTECH:
ENSURING FREE SOCIETIES' INNOVATION LEADERSHIP

DECEMBER 2020

The Center for the Study of the Presidency and Congress, founded in 1965, is a nonprofit, nonpartisan 501(c)(3) organization. The Center's mission is to utilize the lessons of history to address the challenges of today; serve as a strategic honest broker for discussions with leaders from government, the private sector, and the policy community; and to educate the next generation of leaders through the Presidential and International Fellows Program.

GEOTECH: Ensuring Free Societies' Innovation Leadership
December 2020

Published in the United States of America.

CENTER FOR THE STUDY OF THE PRESIDENCY & CONGRESS

601 13th Street, NW – Suite 1050N
Washington, DC 20005
Phone: 202-872-9800
Fax: 202-872-9811
www.thePresidency.org

CENTER FOR THE STUDY OF THE PRESIDENCY & CONGRESS

GEOTECH:

ENSURING FREE SOCIETIES' INNOVATION LEADERSHIP

DECEMBER 2020

CSPC PROJECT TEAM

The Honorable Glenn Nye
President & CEO

The Honorable Mike Rogers
David M. Abshire Chair

Dan Mahaffee
Senior Vice President, Director of Policy

Joshua Huminski
Director, Mike Rogers Center for Intelligence & Global Affairs

Ethan Brown
Policy Analyst

Frank Cilluffo
Senior Fellow

Maia Comeau
Senior Fellow

Samantha Clark
Senior Advisor

Maria Damsgaard
Policy Analyst

Robert Gerber
Senior Fellow

Brendan Hart
Senior Fellow

Andy Keiser
Senior Advisor

James Kitfield
Senior Fellow

Michael Stecher
Senior Advisor

Joshua Walker
Senior Fellow

TABLE OF CONTENTS

EXECUTIVE SUMMARY

In many ways, 2020 has been a year of acceleration. While many things have slowed or come to a stop because of the COVID-19 pandemic or the deadlocked, zero-sum politics of Washington, key geopolitical and technological trends continued to accelerate throughout the year. The pandemic itself has increased our reliance on technology, while also demonstrating the vulnerability of international supply chains to disruption. Geopolitical tensions have grown as great power competition returns to the fore, as liberal societies and authoritarian regimes find themselves in ever greater competition.

The outgoing Trump administration correctly identified and sought to best position the United States for this competition. The 2017 National Security Strategy recognizes the return to great power competition, and even in today's politics, there is largely bipartisan agreement on the importance of innovation leadership for our economic prosperity and national security.

For the incoming Biden administration, many of the same challenges remain. The rivalry between powers, our reliance on technology, and the importance of innovation leadership do not change with party. While the Trump administration and Congress have correctly identified the challenge, the Biden administration has a historic opportunity to organize, prepare, and reform for this competition.

In this report and ongoing conversations, CSPC seeks to identify ways that the incoming Biden administration can best organize itself, work with Congress, and build dialogue with both the U.S. private sector and international allies and partners to address these Geotech concerns.

The Geopolitical Competition

Throughout 2020, geopolitical tensions have grown considerably. The impact of the COVID-19 pandemic and the resulting economic uncertainty have challenged governments while accelerating a range of disruptive, destabilizing trends. Competition between liberal democracies and authoritarian regimes continues apace.

Tensions have grown most significantly with China under the consolidation of power of General Secretary Xi Jinping. In this new China, absent once consensus-driven leadership, Xi is paramount over the Chinese Communist Party (CCP), which in turn is paramount over the state and military, while evermore intertwined with its private sector.

With a historical memory of humiliation at the hands of more technically advanced Western powers and a deep paranoia about domestic plots against the party inspired from within and abroad, the CCP has pursued policies to ensure leadership in key cutting-edge technologies and to leverage those technologies for regime survival at home, military power overseas, leading roles in the technology marketplace, and a narrative of systemic superiority for governance and society.

The growth of these tensions is complicated by the interdependence of the Chinese economy with that of the United States and its allies. Thus, as also described in the previous Geotech reports, lessons from the dueling blocs of the Cold War only go so far. Competition with China will require both a forceful defense of our interests and values alongside the challenging task of finding common ground to confront global challenges.

- BEIJING'S TECHNOLOGY PLAYBOOK
  Throughout the world, the Chinese playbook for technology leadership is becoming clearer to Western policymakers. China's economic and security interests combine, hand-in-glove, to ensure Chinese technology advancement at the expense of international competitors. This technology playbook presents not only a challenge for U.S. and allied policymakers and private sector leaders attempting to compete with China but also unfairly tilts the global marketplace towards China. All of this combines into a model of 21st century technology and innovation mercantilism.

- COVID-19 PANDEMIC RESPONSE
  At the start of 2020, while there were tensions in U.S.-China relations, both Washington and Beijing were emphasizing progress towards the "phase one" trade agreement enacted on February 14, 2020. Since then, the spread of COVID-19 from Wuhan, China, has reversed that progress in U.S.-China relations. On the global stage, China has sought to highlight its effective leadership in dealing with the virus, seeking to hide early missteps in pandemic response while emphasizing how its authoritarian system delivered a better outcome—though through far harsher means than a democracy could implement.

- HUMAN RIGHTS
  Throughout 2020, the CCP has continued its crackdowns on internal dissent. Most notable have been the widespread repression of the Muslim Uighur ethnic minorities of Xinjiang, other non-Han Chinese ethnic minority groups, and the crackdown on dissent in Hong Kong and the application of laws that effectively end the "one country, two systems" dynamic.

- "WOLF-WARRIOR" DIPLOMACY & AUSTRALIA IN THE CROSSHAIRS
  With Chinese diplomats becoming ever more aggressive in social and traditional media, the term "wolf warrior"—from a Chinese Rambo-style action movie—describing the highly nationalistic, often false, and thoroughly insulting rhetoric coming from Chinese diplomats. Facing a coordinated onslaught of economic measures and a war of words, Australia is now the proverbial "canary in the coalmine" for how China and other authoritarians seek to bully free societies.

- TERRITORIAL AGGRESSION
  A key aspect of China's increased assertiveness has been its approach to territorial claims. Continued areas of tension include continued expansion in the South China Sea,

islands disputed with Japan, and deadly quarrels along the "line of actual control" with India. The deadly assault on Indian forces is notable for Delhi's retaliation by banning TikTok and other Chinese apps.

While not nearly as intertwined into the global economy nor advanced in its technological aims, Russia continues to remain a significant technological competitor. Much like the Soviet Union, Russia can match the West and China, or even excel, in some areas of technological acumen, but the challenge is to develop, manufacture, and deploy such technologies at the scale necessary for competition in a global marketplace. Policymakers should continue to remain vigilant though for Russia's efforts to improve its military technology and the blurry line between Russian intelligence operations, organized crime, and technology competition.

Addressing Interdependence & Prospects of Decoupling

While the United States and China are undoubtedly strategic competitors, the deep economic interdependence of the two nations remains. For massive multinationals and small businesses alike, global supply chains are a fundamental reality of how business is done. Decisions by policymakers related to Geotech must consider the balance of security concerns with an understanding of economic and trade impacts—and possible ways to prepare for Chinese retaliation and address the potential collateral damage of more restrictive Geotech policies.

The foundation of security concerns related to China come from its laws that compel cooperation with government and the absence of due process to address government requests for user data, intellectual property, trade secrets, or other sensitive information. In addition to the legal strictures that require compliance with government instructions by all individuals and organizations, international attention has increasingly focused on the relationship between the Chinese government and major "national champions." These close ties between the CCP and Chinese firms have been further strengthened by measures to promote "Military-Civil Fusion" and increase the role of CCP cadres in the private sector. Along with programs like Made in China 2025—designed to foster leadership in key industries—Military-Civil Fusion, or MCF, aims to integrate advances in key technologies, including artificial intelligence and advanced materials engineering, with their military applications.

To address the security threats posed by Chinese firms, the U.S. government has begun to pursue actions related to export controls, investment review, and other measures designed to address concerns about reliance on China and Chinese supply chains—as well as growing concerns about Chinese access to U.S. users' data. These measures have included: Department of Commerce Entity Listings to apply export controls to Chinese firms, increased counterintelligence efforts, and an emphasis on protecting U.S. users' data from Chinese companies—notably TikTok.

While the challenge posed by competition from China is clear, policymakers should carefully evaluate how measures designed to confront China may result in retaliation or, due to the interdependence of our economies, threaten to also harm other U.S. interests or competitiveness. In the case of the former,

that should not be a deterrent to action in every case but warrants careful consideration of what U.S. companies—and even citizens—could face from China. These potential retaliations or even the precedents set by U.S. actions are significant concerns, but there is also the risk of disrupting the technology and innovation ecosystem if there is not careful consideration of how to reduce technological and supply chain dependence and vulnerability.

Beyond supply disruptions, more long-term consequences could affect the arc of American competitiveness. Many American companies rely on these international technology ecosystems turning revenues from global operations into research for future innovations. Yet without careful consideration of the consequences, actions undertaken by the U.S. government could endanger U.S. companies' revenues, risking skilled U.S. jobs and U.S. innovation leadership.

Cooperation with Allies

The United States can and should marshal its allies and partners with a vision for liberal democracies' role in setting technology standards and fostering innovation leadership. While China will rely on the size of its own domestic market and seek to partner with existing and aspiring authoritarians—or enmesh the developing world in corruption and debt colonialism—the United States and its allies can build an alternative to China's digital mercantilism. U.S. policymakers should note that allies and partners are something that Washington is lucky to have while Beijing increasingly alienates other nations.

That said, we cannot assume that the security or economic decisions made in Washington will immediately mesh with those of our allies. While an increasing number of countries around the world have banned Huawei from their 5G networks, others remain open to Chinese access to their networks and data for the sake of faster, cheaper 5G deployment. For many countries, there are complicated economic interests in play. On one hand, there are complicated debates in European countries about balancing the relationship with Washington and Beijing, while other allies, like Japan have a more extensive experience with China's Geotech challenge.

These areas of cooperation are of significant importance as U.S. policymakers engage their like-minded counterparts on Geotech issues:

- <u>HARMONIZING DATA REGIMES, ESTABLISHING DATA TRUST</u>
  To continue to grow and develop the data-driven global digital economy—as well as to match the user pool of China's domestic marketplace—it is necessary to find common ground between liberal democracies to allow cross-border data flows. However, significant challenges to finding such trust remain.

  Transatlantic data agreements are among the thorniest issues confronting policymakers, as the European Union has moved firmly to pursue privacy protection regulations and actions, notably the implementation of the GDPR in 2018. Significantly, the European Court of Justice Decision in *Data Protection Commissioner* v. *Facebook Ireland and Maximillian Schrems*—known as

"Schrems II" has invalidated the past European Commission adequacy determination for the EU-U.S. Privacy Shield Framework that brought transatlantic data transfers under the program into compliance with EU privacy rules. it is important to begin a U.S.-Japan-Europe dialogue—which could be expanded to include other international partners—to find a common ground on a data marketplace that addresses privacy and data management concerns, while also competing with both China's domestic marketplace and model for data management.

- INTERNATIONAL STANDARDS

  An area of particular concern is the growing influence of China in international organizations, including bodies that set international standards for technology. Specifically this has manifested itself in increased PRC representation and leadership in key bodies and efforts to promote Chinese technology standards over Western ones. These are areas where the U.S. and its allies have unfortunately ceded influence—across administrations and governments—as Beijing prioritized these international fora. Understanding the importance of these standards-setting bodies and exercises is key to countering China's influence in setting global technology standards. Ceding the playing field to China will allow it to shape the path of future technology and data flows in its favor.

- PROTECTING SUPPLY CHAINS & NETWORKS

  Building on previous agreements the U.S. State Department has expanded the Clean Network (focused on 5G network security) to include app stores, apps themselves, cloud hosting, communications cables, and digital traffic to U.S. facilities. At the same time, U.S. allies and partners have continued to show growing skepticism about Huawei hardware as they plan their nations' 5G rollout. Finally, U.S. and allied policymakers and industry leaders are also moving towards Open RAN and V-RAN architectures that will help to promote a greater number of wireless hardware vendors and break the stranglehold that some vendors, like Huawei, have on soup-to-nuts solutions for network providers. This will open the playing field further for 5G suppliers and promote greater diversity and resilience within supply chains.

- JOINT COOPERATION & SHARED VALUES

  Democracies "standing together" on these issues is important, and high-level discussions can serve to set strategic Geotech goals; lay the foundation for further digital trade and innovation; harmonize data management and privacy protection; and ensure practical-level cooperation on technology security and innovation leadership. What becomes a paradox for policymakers is to explain how some of the measures undertaken by democracies—while appearing similar to some Chinese actions—are in fact grounded in entirely different values to pursue different interests and goals, all the while featuring a variety of guardrails intended to safeguard civil liberties. The fundamental cornerstones of the rule of law, civil liberties, free enterprise, and human rights are far firmer footing than the whims of authoritarian dictators and party cadres.

U.S. Innovation Leadership

The United States is in far more control over what it does to foster its own strengths, ensure economic dynamism, and continue innovation leadership than the choices of Beijing. Policymakers can help to ensure that the United States is best set for this competition by encouraging the roll out and deployment of technologies to speed "first mover" advantages; continuing and providing further measures to support R&D and protect IP; promoting supply chain security and production capacity; honing an innovation-oriented regulatory environment; building a Geotech-ready workforce; and ensuring that government is well-informed and well-organized to address this challenge.

Conclusion & Recommendations

Addressing the complex nature of the Geotech challenge requires strategic thinking and vision. Planning for technological innovations becomes a matter of *when*, not *if*, and policymakers must now focus their concern on *where*. The Geotech competition will continue to be one where interests and innovation will remain constantly fluctuating, while shared values and principles must continue to be the guide star.

- DEVELOP BASIC FEDERAL STANDARDS FOR DATA MANAGEMENT & PRIVACY
  In order to prevent a patchwork of state-level regulations for data management and privacy protections, a basic federal standard should be developed by Congress that balances regulatory predictability for digital services companies with concerns about data privacy and fair competition. This legislation would also boost U.S. prospects for securing important international data transfer agreements by establishing a "U.S. position."

- RESTORE WHITE HOUSE COORDINATING POSITION(S)
  To facilitate the interagency coordination of Geotech issues and commensurate with recommendations from Congress, including the Cyber Solarium Commission, the position of National Cyber Director, responsible for "cybersecurity and associated emerging technologies" should be established. Other more civil- and economic-oriented positions and bodies such as the Office of Science and Technology Policy (OSTP) and Council of Economic Advisors should also be included in Geotech policy coordination for a balance of policy perspectives, while the National Security Council should have a technology directorate for coordination of these issues.

- IMPROVE CONGRESSIONAL TECH SUPPORT
  The recommendations of the Select Committee on the Modernization of Congress provide a pathway forward to improve Congress's staffing on and oversight of technology matters.

- CONTINUE SUPPORT FOR 5G ROLLOUT, OPEN RAN ARCHITECTURE, COMPETITIVE NETWORKS
  The deployment of 5G networks can bridge the digital divide and provide the foundation for developing future innovations, connected industries, and near-constant connectivity.

Policymakers should continue policies hastening 5G deployment. Policies promoting the adoption of Open RAN architectures and reallocation of underutilized spectrum can continue to ensure competition among network suppliers, while not establishing a nationalized 5G network ensures competition among network providers.

- FURTHER EXPORT CONTROLS IF NECESSARY
  Tools like export licensing, export controls, and entity listing should be applied in a targeted manner to ensure that state-supported, state-affiliated, Chinese military fusion firms and researchers do not benefit from high-tech, cutting-edge American technologies.

- YET, UNDERSTAND COMMODITIZED TECH & INTERDEPENDENCE
  Controls applied to the cutting-edge of technology must be balanced with an understanding of the current interdependence of the United States, China, and many other countries through global supply chains. Furthermore, many technologies are highly commoditized, low-tech items that do not post a security risk—and can easily be acquired elsewhere. Carefully reducing dependency on potential adversaries can avoid the unintended consequences of a rapid decoupling.

- LIBERAL DEMOCRACIES STAND TOGETHER ON VALUES, EXPAND & HARMONIZE TECH COOPERATION
  While technologies are finding various fora in which to discuss Geotech issues, it is worth finding common ground and reminding the world of the importance of the shared values that underpin liberal democracies approach to technology and innovation leadership. The underpinnings of the rule of law, due process, civil liberties, and human rights stand in stark contrast to China's model. A U.S.-Europe-Japan dialogue, or similar grouping of democracies, on data management and privacy should be pursued for commercial and security interests. Where possible, and building on the successful model of the "Five Eyes" countries, the U.S. and its closest allies should develop shared standards for intelligence sharing and security clearances; seek harmonization of defense industrial base security, classified patents, and export controls; stand up jointly utilized tools and resources like the Multilateral Microelectronics Security Fund; and pursue joint R&D in advanced emerging technologies.

- CONTINUE CLEAN NETWORK INITIATIVES
  To provide safe and secure networks, supply chains, data management, and data storage, the Clean Network initiatives serve as a useful starting point for cooperation among liberal democracies. Alongside hopeful progress towards U.S. federal data privacy standards, these dialogues and discussions can be also address international data management and digital trade issues.

- INVEST IN R&D & HI-TECH MANUFACTURING CAPACITY
  Along the lines of measures like The CHIPS Act and the American Foundries Act, policymakers

should look to support R&D in advanced emerging technologies, while also addressing supply chains dependent on adversaries or subject to other supply bottlenecks in times of increased tensions or open conflict.

- SUPPORT EDUCATION THROUGH COVID-19 AND BEYOND
  Given the impact of the pandemic across the education system—and upon the progress of students—significant support will be needed for education. State higher education institutions are in particular danger from state and university revenue shortfalls. At the same time, as technological innovations have been applied to virtual learning and other new curriculums and pedagogies during the pandemic, harness lessons learned here to improve education access.

- IMPROVE DIALOGUE BETWEEN TECH & POLICYMAKERS
  Given the importance of these topics for national security and economic prosperity, a growing chasm between government and the private sector—especially in technology—is always of concern. While there are significant policy issues to be addressed because of technology's impact, the politicization of technology regulation threatens one of America's most important industries for its competitiveness and strategic footing.

INTRODUCTION

In many ways, 2020 has been a year of acceleration. While many things seemingly slowed or stopped because of the COVID-19 pandemic or the deadlocked, zero-sum politics of Washington, key geopolitical and technological trends continued to accelerate throughout the year. The pandemic itself has increased our reliance on technology, while also demonstrating the vulnerability of international supply chains to disruption. Geopolitical tensions have grown as great power competition returns to the fore, as liberal societies and authoritarian regimes find themselves in ever greater competition.

The outgoing Trump administration correctly identified and sought to best position the United States for this competition. The 2017 National Security Strategy recognizes the return to great power competition, and even in today's politics, there is largely bipartisan agreement on the importance of innovation leadership for our economic prosperity and national security.

For the incoming Biden administration, many of the same challenges remain. The rivalry between powers, our reliance on technology, and the importance of innovation leadership do not change with party. While the Trump administration and Congress have correctly identified the challenge, the Biden administration has a historic opportunity to organize, prepare, and reform for this competition.

In this report and ongoing conversations, CSPC seeks to identify ways that the incoming Biden administration can best organize itself, work with Congress, and build dialogue with both the U.S. private sector and international allies and partners to address these Geotech concerns. First and foremost, these efforts come with a continued recognition of how great power competition with China and Russia extends beyond traditional domains of military and diplomatic competition to include these technological, economic, and commercial factors. In an era of globalized economies and interdependent supply chains, the balance between commercial engagement and national security becomes ever more blurred—and requires thoughtful, strategic policymaking. Also, while great power competition often combines China and Russia together, it is worth noting that the former is a far more significant technology competitor with a clear playbook for technology competition.

Like a preparation for any individual contest, preparation and organization are key to success. While U.S. policymakers can only shape Beijing's approach at the periphery, they are in total control of the U.S. government approach. The recommendations of this report look at how the Executive and Congress can organize for this challenge, coordinate government authorities, and support the private sector engines of technological innovation.

Finally, while the Trump administration had bilateral and some multilateral success in engagement with allies, the Biden administration has the opportunity to further this cooperation. Allies and partners are an asset for the United States, even if managing shared interests can be unwieldy. From the future of 5G networks to cooperation in advanced research to protecting users' data privacy, the best hope for democracies is to foster dialogue and cooperation to stand together.

GROWING GEOPOLITICAL TENSIONS

Throughout 2020, geopolitical tensions have grown considerably. The impact of the COVID-19 pandemic and the resulting economic uncertainty have challenged governments while accelerating a range of disruptive, destabilizing trends. Competition between liberal democracies and authoritarian regimes continues apace. The return to an era of great power competition brings the United States and its allies into a contest with despots in Beijing, Moscow, and other autocracies to determine might. This contest is scored not only in terms of traditional metrics such as military power, gross domestic product, or territorial reach but also leading in technological innovation, setting the standards for future generations of technology, and setting the narrative for humanity's relationship with technological progress.

The Fault Lines with China

Tensions have grown most significantly with China. This section will outline some of the key arenas of contention—ranging from the COVID pandemic response to territorial claims to human rights abuses—but these tensions arise from sea change in China's approach to the world under the consolidation of power of General Secretary Xi Jinping. General Secretary Xi has done away with the consensus-driven approach for Beijing's decision-making. In this new China, Xi is paramount over the Chinese Communist Party (CCP), which in turn is paramount over the state and military, while evermore intertwined with its private sector.

With a historical memory of humiliation at the hands of more technically advanced Western powers and a deep paranoia about domestic plots against the party inspired from within and abroad, the CCP has pursued policies to ensure leadership in key cutting-edge technologies and to leverage those technologies for regime survival at home, military power overseas, leading roles in the technology marketplace, and a narrative of systemic superiority for governance and society. China's effort to espouse the Chinese system's superiority, compared to liberal democracies and free markets, has only accelerated since the COVID-19 pandemic.

The growth of these tensions is complicated by the interdependence of the Chinese economy with that of the United States and its allies. Thus, as also described in the previous Geotech reports, lessons from the dueling blocs of the Cold War only go so far. Competition with China will require both a forceful defense of our interests and values alongside the challenging task of finding common ground to confront global challenges.

- BEIJING'S TECHNOLOGY PLAYBOOK

  Throughout the world, the Chinese playbook for technology leadership is becoming clearer to Western policymakers. China's economic and security interests combine, hand-in-glove, to ensure Chinese technology advancement at the expense of international competitors. CSPC Senior Advisor Andy Keiser describes this playbook—applied across a range of industries and

sectors—in his analysis of the threat China's policies to U.S. national security, focused on the semiconductor industry:[1]

- First, build technical knowhow through the following means: intellectual property (IP) theft overseas; domestic state-sponsored research and development; acquisition of IP via joint venture or direct investment; requirements forcing Chinese business partners and technology transfers for entry into the Chinese market; and, domestic workforce training and support.
- Second, create a robust domestic industry by guaranteeing market share in the world's second largest economy; transfer stolen IP from the Chinese military and intelligence services to domestic companies; secure access to necessary natural resources, provide lines of credit from state-sponsored financial institutions; and, institute quotas and tariffs on foreign competitors in China.
- Third, flood the global market with products at- or below-cost to increase Chinese companies' global market share and bankrupt foreign competitors, while sustaining said losses through lines of credit from state-sponsored financial institutions. [2] [3]

This technology playbook presents not only a challenge for U.S. and allied policymakers and private sector leaders attempting to compete with China but also unfairly tilts the global marketplace towards China. All of this combines into a model of 21st century technology and innovation mercantilism.

- <u>COVID-19 PANDEMIC RESPONSE</u>

  At the start of 2020, while there were tensions in U.S.-China relations, both Washington and Beijing were emphasizing progress towards the "phase one" trade agreement enacted on February 14, 2020. Since then the spread of COVID-19 from Wuhan, China, across the globe and its impact on the United States—with more than 220,000 dead and more than 8.8 million infected as of the writing of this report[4]—has reversed that progress in U.S.-China relations. Once lauding the Chinese leadership for their handling of the virus and the accomplishments of the trade deal, the Trump administration now blames China for the domestic and global impact of the virus.

  At the same time, on the global stage, China has sought to highlight its effective leadership in

[1] Andy Keiser. "Securing the Keys to the Future: Countering the Threat from State-Backed Chinese Semiconductor Companies." CSPC. October 2020. https://static1.squarespace.com/static/5cb0a1b1d86cc932778ab82b/t/5f985cef51f01e306e179e72/1603820785461/CSPC+Semiconductor+White+Paper.pdf

[2] Office of the United States Trade Representative, Executive Office of the President, "Findings of the Investigation Into China's Acts, Policies and Practices Related to Technology Transfer, Intellectual Property, and Innovation Under Section 301 of the Trade Act of 1974." March 22, 2018. https://ustr.gov/sites/default/files/Section%20301%20FINAL.PDF

[3] Joint Hearing Before the Subcommittee on Terrorism, Nonproliferation, and Trade and the Subcommittee on Asian and the Pacific of the Committee on Foreign Affairs, House of Representatives, One Hundred Fifteenth Congress, Second Session. July 11, 2018. https://docs.house.gov/meetings/FA/FA18/20180711/108531/HHRG-115-FA18-Transcript-20180711.pdf

[4] "COVID-19 Dashboard," Center for Systems Science and Engineering, Johns Hopkins University. Accessed October 28, 2020. https://coronavirus.jhu.edu/map.html

dealing with the virus, seeking to hide early missteps in pandemic response while emphasizing how its authoritarian system delivered a better outcome—though through far harsher means than a democracy could implement. It also used "mask diplomacy" to try to win friends and will certainly leverage China's vaccine development to advance its foreign policy goals. That said, global opinion regarding China has reached its nadir in many countries, as blame for COVID-19 is pointed at Beijing.[5]

- HUMAN RIGHTS

  Throughout 2020, the CCP has continued its crackdowns on internal dissent. Most notable have been the widespread repression of the Muslim Uighur ethnic minorities of Xinjiang, other non-Han Chinese ethnic minority groups, and the crackdown on dissent in Hong Kong and the application of laws that effectively end the "one country, two systems" dynamic. In Xinjiang, the repression of the Uighurs—under the aegis of Beijing's "counterterrorism" operations—has resulted in the imprisonment of more than 1 million in camps where they are subject to cultural indoctrination, medical experimentation, forced sterilization, and other egregious abuses. Already described as a "cultural genocide," bipartisan legislation has been introduced in the U.S. Senate to declare China's treatment of Uighurs a genocide.[6]

  Unrest in Hong Kong over the gradual erosion of civil liberties has given way to Beijing's crackdown on the once vibrant entrepot. National security laws applied to the Hong Kong Special Administrative Region have effectively ended the "one country, two systems" framework under which protected the civil liberties of Hong Kongers held over from that territory's time under the sovereignty of the United Kingdom. While the territories political and commercial elite have largely acquiesced to Beijing, unlikely dissidents ranging from students to pensioners now find themselves under the watchful eye of Beijing and subject to laws that criminalize the most basic elements of protest and dissent.[7] Having quashed protests, the CCP has its eyes on reigning in Hong Kong's government, judiciary, and media. Mainland authorities allowed Hong Kong Executive Carry Lam to oust pro-democracy opposition lawmakers, leading to their mass resignation from the territory's legislative council.[8] The separation of powers is anathema to CCP ideology, so the territory's judiciary is now targeted for reform. A newspaper owned by the Beijing's Hong Kong liaison office has called for greater patriotism from judges, while giving Ms.

---

[5] Laura Silver, Kat Devlin, and Christine Huang, "Unfavorable Views of China Reach Historic Highs in Many Countries." *Pew Research Center*. October 6, 2020. https://www.pewresearch.org/global/2020/10/06/unfavorable-views-of-china-reach-historic-highs-in-many-countries/

[6] Yasmeen Serhan, "Saving Uighur Culture from Genocide." *The Atlantic*. October 4, 2020. https://www.theatlantic.com/international/archive/2020/10/chinas-war-on-uighur-culture/616513/ and Shawna Chen, "Senators introduce bipartisan legislation to label Xinjiang abuses 'genocide.'" *Axios*. October 28, 2020. https://www.axios.com/senate-china-uyghur-xinjiang-genocide-5d9507dc-9668-4d24-9bbf-527a20e4f09b.html

[7] Ishaan Tharoor, "China's unrelenting crackdown on Hong Kong." *The Washington Post*. August 11, 2020. https://www.washingtonpost.com/world/2020/08/11/chinas-unrelenting-crackdown-hong-kong/

[8] Nicolle Liu and Primrose Riordan, "Hong Kong pro-democracy lawmakers resign en masse." *The Financial Times*. November 11, 2020. https://www.ft.com/content/39a1d9ae-d238-4e34-a6f0-c04f8cc4c6b5

Lam the power to select which judges are empaneled for national security cases.[9]

- "WOLF-WARRIOR" DIPLOMACY & AUSTRALIA IN THE CROSSHAIRS

  With Chinese diplomats becoming ever more aggressive in social and traditional media, the term "wolf warrior"—from a Chinese Rambo-style action movie—describing the highly nationalistic, often false, and thoroughly insulting rhetoric coming from Chinese diplomats.[10] While Chinese diplomats have long tried to hide behind claims of Chinese sovereignty or concerns for "the feelings of the Chinese people," wolf warrior diplomacy shows no respect for the sovereignty and dignity of other nations and their peoples. It is likely that the rhetoric is designed to win fans at home—both in public and the halls of power—rather than convert opinion abroad.[11] Still, it is revealing to see this mindset growing in influence in the Chinese foreign policy apparatus.

  In November 2020, Australia has been the most direct target of China's ire, as the premiership of Scott Morrison has reviewed a range of Australian economic, security, and cultural vulnerabilities that have grown as China's influence has. This has drawn anger from China, including a 14-count list of grievances issued by Beijing in mid-November.[12] The Chinese regime further escalated tensions at the end of November, when foreign ministry spokesman and noted wolf warrior Zhao Lijian tweeted a faked image of an Australian soldier holding a knife to an Afghan child following a scandal regarding Australian forces in that conflict. It is worth noting that the anti-Australian rhetoric coming from Beijing is coordinated with Moscow's spokespersons.[13] Facing this coordinated onslaught of economic measures and a war of words, Australia is now the proverbial "canary in the coalmine" for how China and other authoritarians seek to bully free societies.

- TERRITORIAL AGGRESSION

  A key aspect of China's increased assertiveness has been its approach to territorial claims. Continued areas of tension include continued expansion in the South China Sea, islands disputed with Japan, and deadly quarrels along the "line of actual control" with India. In the South China Sea, China has continued to expand and militarize artificial islands throughout the region, while expanding the presence of its naval and coast

[9] Austin Ramzy, "Hong Kong's Courts are Still Independent. Some Want to Rein Them In." *The New York Times*. November 30, 2020. https://www.nytimes.com/2020/11/30/world/asia/hong-kong-china-courts.html

[10] Ben Wescott and Steven Jiang, "China is embracing a new brand of foreign policy. Here's what wolf warrior diplomacy means." *CNN*. May 29, 2020. https://www.cnn.com/2020/05/28/asia/china-wolf-warrior-diplomacy-intl-hnk/index.html

[11] "China's Wolf Warriors Diplomats Slam Australia, Win Fans at Home." *Bloomberg*. December 1, 2020. https://www.bloomberg.com/news/articles/2020-12-01/china-s-wolf-warrior-diplomats-slam-australia-win-fans-at-home

[12] Finbarr Bermingham, "China-Australia relations: Beijing blames Canberra for trade spat, citing grievances from Huawei to Taiwan." *South China Morning Post*. November 18, 2020. https://www.scmp.com/economy/china-economy/article/3110257/china-australia-relations-beijing-blames-canberra-trade-spat

[13] Gerry Shih, "Chinese official fuels outrage with doctored image depicting Australian soldier cutting Afghan child's throat." *The Washington Post*. November 30, 2020. https://www.washingtonpost.com/world/asia_pacific/china-australia-tweet-afghanistan/2020/11/30/546a2512-32b8-11eb-9699-00d311f13d2d_story.html

guard patrols—as well as a maritime fishing militia known to act aggressively.[14] In the East China Sea, China continues to claim the Senkaku Islands, and tests the Japanese Self Defense Forces through regular incursions of this contested airspace and waters. In recent exercises, Lt. Gen. Kevin Schneider, Commander of U.S. Forces Japan, announced that U.S. forces could be deployed to help defend the contested islands.[15] Finally, in June 2020, twenty Indian soldiers and an unknown number of troops of the People's Liberation Army were killed in hand-to-hand combat along the disputed Himalayan borders between the two nations. China has continued to encroach upon Indian-claimed territory, while India has responded by banning TikTok and WeChat among nearly sixty other now-forbidden mobile Chinese apps.[16]

This action is notable as the first "Geotech"retaliation for kinetic military action.

Russia's Destabilizing Role

While not nearly as intertwined into the global economy nor advanced in its technological aims, Russia continues to remain a significant technological competitor. Much like the Soviet Union, Russia can match the West and China, or even excel, in some areas of technological acumen, but the challenge is to develop, manufacture, and deploy such technologies at the scale necessary for competition in a global marketplace—given that the needs of military and state procurement at home still prevail over consumer-driven innovation.

Where Russia will be of concern is how it may apply advanced technologies such as AI to existing military hardware or intelligence operations. These still present significant risks in terms of the U.S.-Russia military balance of power and the offense-defense balance in cyberspace. Russia's technology efforts are largely focused on military hardware, with abortive attempts to build the nation's digital might. That said, Russian hackers and trolls remain effective, and Russian experience in cyber and information operations continues to grow. Of particular note for policymakers should be the increasingly blurred line between state intelligence and organized crime that Russia uses to maximize the advantages of both—in terms of technology, deniability, and profitability—in cyber operations. Thus, Russia remains a significant geopolitical competitor but not a major technology competitor.

The key lesson of Russia for Geotech policymakers is the importance of the broader ecosystem of human capital, economic prosperity, and international engagement that is vital to ensure innovation leadership. Having turned its back on globalization and economic engagement, while encouraging its best and

---

[14] Drake Long, "China Lurks Around Disputed South Sea Features for Months on End." *Radio Free Asia*. October 26, 2020. https://www.rfa.org/english/news/china/southchinasea-lurking-10262020174503.html

[15] Laura Zhou, "American troops could be sent to 'defend the Senkaku Islands', US commander says." *The South China Morning Post*. October 27, 2020. https://www.scmp.com/news/china/diplomacy/article/3107291/american-troops-could-be-sent-defend-senkaku-islands-us

[16] Maria Abi-Habib, "India Bans Nearly 60 Chinese Apps, Including TikTok and WeChat." *The New York Times*. June 30, 2020, update. https://www.nytimes.com/2020/06/29/world/asia/tik-tok-banned-india-china.html

brightest to emigrate abroad, Russia's technological acumen does not translate into a vibrant technology sector or cutting-edge innovation.

The Need for a Strategic Approach to Great Power Competition

Geotech competition is part and parcel of the larger great power competition. While a Geotech strategy can address the technological challenge of our adversaries and ensure that the United States and its allies are best positioned for innovation leadership, it alone cannot address the rise and revanchism of 21st century peer competitors. While a Geotech strategy can ensure excellence in technology, it must be part of a broader grand strategy to marshal all the elements of national power for the 21st century. Beyond its work on Geotech, CSPC continues to examine great power competition in the context of recommendations for the next administration.

INTERDEPENDENCE & DECOUPLING

While the United States and China are undoubtedly strategic competitors, the deep economic interdependence of the two nations remains. For massive multinationals and small businesses alike, global supply chains are a fundamental reality of how business is done. Decisions by policymakers related to Geotech must consider the balance of security concerns with an understanding of economic and trade impacts—and possible ways to prepare for Chinese retaliation and address the potential collateral damage of more restrictive Geotech policies.

China's Legal & Political Approach to Industry

The foundation of security concerns related to China come from its laws that compel cooperation with government and the absence of due process to address government requests for user data, intellectual property, trade secrets, or other sensitive information. The Counterespionage, Cybersecurity, and Intelligence Laws have put together a network of strictures designed to compel cooperation with Chinese state agencies. Article Seven of the Intelligence Law, states that "any organization or citizen shall support, assist, and cooperate with state intelligence work according to law;" Article Fourteen states that "state intelligence work organs, when legally carrying forth intelligence work, may demand that concerned organs, organizations, or citizens provide needed support, assistance, and cooperation."[17]

In addition to the legal strictures that require compliance with government instructions by all individuals and organizations, international attention has increasingly focused on the relationship between the Chinese government and major "national champions." Telecommunications firms like Huawei and ZTE are known for their close ties to the Chinese government and military, and only recently have U.S. and allied policymakers addressed—albeit in fits and starts—the threat posed by these firms to the security

[17] Murray Scot Tanner, "Beijing's New National Intelligence Law: From Defense to Offense." *Lawfare*. July 20, 2017. https://www.lawfareblog.com/beijings-new-national-intelligence-law-defense-offense

of critical telecommunications infrastructure. For Beijing, development and control of 5G hardware and standards has been and remains not only as a key near-term economic goal, but also the foundation to ensure Chinese telecommunications dominance in the decades to come.[18]

These close ties between the CCP and Chinese firms have been further strengthened by measures to promote "Military-Civil Fusion" and increase the role of CCP cadres in the private sector. Along with programs like Made in China 2025—designed to foster leadership in key industries—Military-Civil Fusion, or MCF, aims to integrate advances in key technologies, including artificial intelligence and advanced materials engineering, with their military applications. In the words of the U.S.-China Economic and Security Review Commission:

> The Chinese government's military-civil fusion policy aims to spur innovation and economic growth through an array of policies and other government-supported mechanisms, including venture capital (VC) funds, while leveraging the fruits of civilian innovation for China's defense sector. The breadth and opacity of military-civil fusion increase the chances civilian academic collaboration and business partnerships between the United States and China could aid China's military development.[19]

Furthermore, in September of 2020, the CCP called for closer cooperation between government and the private sector in the document "Opinion on Strengthening the United Front Work of the Private Economy in the New Era." Chinese leaders have described this new structure as "modern private enterprise with Chinese characteristics." Since January 2020, General Secretary Xi Jinping had pursued policies that emphasized a greater role for the party in the management of China's state-owned industries (SOEs). While SOEs have long been known for their close ties to the state, the measures connecting the party to wholly private firms had been opaquer. By announcing this the CCP has laid the groundwork for a greater role for CCP leadership within the management of private firms.[20] At a time when most of the world has been looking for China to liberalize its economy and reduce the role of the state and party in the private sector, this represents a step in an entirely different direction that raises questions about the independence of Chinese business and the risks of commercial ties.

Notable U.S. Government Actions

To address the security threats posed by Chinese firms, the U.S. government has begun to pursue actions related to export controls, investment review, and other measures designed to address concerns

---

[18] Andy Keiser & Bryan Smith, "Chinese Telecommunications Companies Huawei and ZTE: Countering a Hostile Threat." The National Security Institute at George Mason University's Antonin Scalia Law School. January 24, 2019. https://nationalsecurity.gmu.edu/chinese-telecommunications/

[19] U.S.-China Economic and Security Review Commission, "2019 Report to Congress: Chapter 3 Section 2 – Emerging Technologies and Military-Civil Fusion – Artificial Intelligence, New Materials, and New Energy." Accessed October 20, 2020. https://www.uscc.gov/sites/default/files/2019-11/Chapter%203%20Section%202%20-%20Emerging%20Technologies%20and%20Military-Civil%20Fusion%20-%20Artificial%20Intelligence,%20New%20Materials,%20and%20New%20Energy.pdf

[20] Scott Livingston, "The Chinese Communist Party Targets the Private Sector." Center for Strategic and International Studies, October 8, 2020. https://www.csis.org/analysis/chinese-communist-party-targets-private-sector

about reliance on China and Chinese supply chains—as well as growing concerns about Chinese access to U.S. users' data.

- DEPARTMENT OF COMMERCE ENTITY LIST ACTIONS

  Throughout 2020, the U.S. government continued to expand the scope of export controls to major Chinese technology firms. Most notably, the restrictions on business with Huawei and Huawei-affiliates continued to expand, while existing licenses were allowed to expire.[21] Because of these restrictions, Huawei finds itself, in its own words, "fighting for survival." Attempts are being made to stockpile chips that would be affected by these export controls, while also accelerating efforts to develop domestic chip-making and the development of native operating systems.[22]

  While covered in greater detail in an October 2020 CSPC Geotech White Paper focused on the semiconductor sector, restrictions have also been applied to the Chinese semiconductor firm Semiconductor Manufacturing International Company, or SMIC. Since September of 2020, the U.S. Department of Commerce has required that U.S. firms apply for a "military end user" license before exporting key systems to SMIC.[23]

- COUNTERINTELLIGENCE

  The U.S. Department of Justice has continued to focus on the activities of Chinese agents on U.S. soil and their efforts ranging from industrial espionage to ties with academia to intimidation of Chinese dissidents abroad.[24] FBI Director James Wray described the scope of Chinese intelligence efforts, and the FBI response, in July of 2020:

  > We've now reached a point where the FBI is now opening a new China-related counterintelligence case every 10 hours…Of the nearly 5,000 active counterintelligence cases currently under way across the country, almost half are related to China."

  The FBI also continues to increase its outreach to the private sector, academia, and other organizations that might not have previously been seen as critical infrastructure but are also the target of Chinese intelligence and influence campaigns.

---

[21] Grant Leach, Cortney O'Toole Morgan, and Camron Greer, "U.S. Adds 38 New Huawei Affiliates to Entity List While Again Expanding Foreign-Produced Direct Product Rule." *Global Trade*. August 26, 2020. https://www.globaltrademag.com/u-s-adds-38-new-huawei-affiliates-to-entity-list-while-again-expanding-foreign-produced-direct-product-rule/

[22] "Huawei: 'Survival is the goal' as it stockpiles chips," *BBC World News*. September 23, 2020. https://www.bbc.com/news/technology-54266531

[23] "U.S. tightens exports to China's chipmaker SMIC, citing risk of military use," *Reuters*. September 26, 2020. https://www.reuters.com/article/us-usa-china-smic/u-s-imposes-curbs-on-exports-to-chinas-top-chipmaker-smic-idUSKBN26H0LN

[24] "Harvard University Professor and Two Chinese Nationals Charged in Three Separate China Related Cases," U.S. Department of Justice Office of Public Affairs. January 28, 2020. https://www.justice.gov/opa/pr/harvard-university-professor-and-two-chinese-nationals-charged-three-separate-china-related and "FBI charges 'Chinese agents who coerced dissidents,'" *BBC News*. October 28, 2020. https://www.bbc.com/news/world-us-canada-54724471

- PROTECTING U.S. USERS' DATA

  Significant actions have also been undertaken by the U.S. government to address the threat to U.S. citizens' personal data from Chinese social media and chat apps. The most notable, due to its widespread popularity, has been TikTok—a short video app that utilizes an artificial intelligence and algorithmic predictions to send users new videos based on their viewing habits of previous videos. While many of the videos range from playful to nonsensical, the data gathered about young Americans via these apps is of concern. Security researchers discovered that the app was copying the text a phone's clipboard without the user's knowledge. The app's developers claimed that the measure was for security purposes, but later removed it from the software.[25] This and other concerns led the Trump administration to push for a deal which would—after some relative drama—ultimately result in Oracle and Wal-Mart taking a stake in a new entity separate from the original Chinese firm with U.S. users' data in the United States.[26]

  At the same time as actions against TikTok, the Trump administration also took measures to block the app WeChat, a commonly used chat app in China and amongst the Chinese diaspora. Given its popularity as well as its widespread use in mainland China, it is also heavily censored and monitored by the Chinese government. It is also increasingly necessary for daily life in digital China, and, in addition to being used to communicate among friends and family, many U.S. companies utilize WeChat for customer service in China.[27]

  As of this report's writing, court cases are pending regarding both the TikTok and WeChat bans and the first amendment implications, while negotiations continue to finalize arrangements for the new TikTok entity involving Oracle and Wal-Mart.[28] Whatever the short-term outcome, the United States needs to develop a systematic process of review of potential threats to American citizen data that incorporate criteria that can be applied methodically to these and future questions of American technology dependence on Chinese apps and systems. Be it the architecture of certain apps or the broader use of data by the CCP for national security and social credit scoring, a rules-based framework is needed to address these concerns. Ad-hoc nationalization, mercurial presidential statements, and the prospect of crony capitalism do little to demonstrate a difference between our system compared to that of authoritarians, while also forsaking principles like due process and the rule-of-law.

---

[25] Kim Lyons, "TikTok says it will stop accessing clipboard content on iOS devices." *The Verge.* June 26, 2020. https://www.theverge.com/2020/6/26/21304228/tiktok-security-ios-clipboard-access-ios14-beta-feature

[26] Stephen Nellis, David Shepardson, and Echo Wang, "How a marked-up term sheet and messy rollout threw TikTok deal into disarray." *Reuters.* September 23, 2020. https://www.reuters.com/article/idUSKCN26E2S9

[27] Liza Lin, "U.S. Firms in China Say Trump's WeChat Ban Will Hit Them Where It Hurts." *The Wall Street Journal.* August 26, 2020. https://www.wsj.com/articles/u-s-firms-in-china-say-trumps-wechat-ban-will-hit-them-where-it-hurts-11598437779

[28] David McCabe, "U.S. Appeals Injunction Against WeChat Ban." *The New York Times.* October 2, 2020. https://www.nytimes.com/2020/10/02/technology/wechat-ban-court.html; John D. McKinnon, Georgia Wells, and Kate Davidson, TikTok Deal Makers Await Court Ruling on U.S. Ban." *The Wall Street Journal.* October 22, 2020. https://www.wsj.com/articles/tiktok-deal-makers-await-court-ruling-on-u-s-ban-11603359016; and David Shepardson, "U.S. appeals court rejects immediate WeChat ban." *Reuters.* October 26, 2020. https://www.reuters.com/article/usa-wechat-idUSKBN27C059

Warnings of Retaliation & Unintended Consequences

While the challenge posed by competition from China is clear, policymakers should carefully evaluate how measures designed to confront China may result in retaliation or, due to the interdependence of our economies, threaten to also harm other U.S. interests or competitiveness. In the case of the former, that should not be a deterrent to action in every case but warrants careful consideration of what U.S. companies—and even citizens—could face from China. In the case of the latter, it is an argument for carefully crafted, targeted measures wherever possible.

- THE RISK OF RETALIATION

  It can be debated whether Beijing has shown restraint as Geotech tensions have escalated. However, it is notable that while there has been harassment of U.S. citizens in China, there have not been actions similar to the use of the Chinese legal system for the hostage-taking of Canadians Michael Spavor and Michael Kovrig, detained "coincidentally" following the arrest in Vancouver of Meng Wangzhou, CFO of Huawei and daughter of the firm's founder.[29] Beijing has also put forward its own "Unreliable Entities List" designed to target foreign firms deemed by the CCP to be a risk to China's "sovereignty, security, or development."[30] Beijing's retaliation could severely affect the revenue of significant U.S. companies that are innovation engines and market leaders in technology, heavy manufacturing, and consumer goods and services.

- SETTING THE WRONG PRECEDENT

  In addressing the Geotech challenge, it is also important that liberal democracies do not avail themselves of the methods of authoritarians to try to match them. Simply put, one cannot "out-China, China." In fact, one of China's most notable digital hawks, often known as "wolf warriors," praised the heavy-handedness of the Trump administration approach to the TikTok deal as U.S. affirmation of China's model for digital sovereignty and government interference in private sector deal making.[31]

  Whether it be how the government addresses foreign ownership concerns or investigations into foreign espionage, the United States must continue to uphold due process, the rule of law, and transparent, consistent policymaking. Overt politicization of measures related to national security, innovation leadership, or trade competitiveness often undermines the efficacy and reasoning of those goals in the first place.

[29] "Michael Kovrig and Michael Spavor: China charges Canadians with spying." *BBC World News*. June 19, 2020. https://www.bbc.com/news/world-asia-china-53104303

[30] Adrianna Zhang, "China Releases Details on Its Own Unreliable Entity List." *Voice of America*. September 22, 2020. https://www.voanews.com/east-asia-pacific/voa-news-china/china-releases-details-its-own-unreliable-entity-list

[31] Hu Xijin, Twitter post, September 20, 2020, 2:14 p.m. https://twitter.com/HuXijin_GT/status/1307744976864833536

- DISRUPTION OF THE TECHNOLOGY & INNOVATION ECOSYSTEM

  One of the most common euphemisms to describe the complex underpinnings of innovation leadership and the web of global supply chains is to refer to various technology "ecosystems." Borrowing from the description of the natural world and the complex relationships in a natural ecosystem, these technology ecosystems have their own intricacies that policymakers should understand as they approach Geotech policies. Supply chains, especially for advanced components, cannot relocate as easily as those of more basic, commoditized goods. Disruptions to supply chains or capacity could disrupt high-tech commerce.

  Beyond supply disruptions, more long-term consequences could affect the arc of American competitiveness. Many American companies rely on these international technology ecosystems turning revenues from global operations into research for future innovations. Yet without careful consideration of the consequences, actions undertaken by the U.S. government could endanger U.S. companies' revenues, risking skilled U.S. jobs and U.S. innovation leadership. Finally, the lessons of trade conflicts and other past competitions provide plenty of lessons on how tariffs, quotas, and other measures more often inspire competitors to switch away from American vendors, develop their own capabilities, and climb the value chain.

  Understanding these technology ecosystems, much like their natural counterparts, should steer policymakers from solutions that appear plug-and-play, while continuing dialogue with the private sector to best identify shared solutions to this challenge. Where possible, clarifying existing legislation or codifying new laws—rather than a reliance on executive orders—can help the private sector plan for the long-term. While the former is more challenging in a time of partisan deadlock, the latter is often subject to legal challenges and changes of administration.

BUILDING INTERNATIONAL COALITIONS

Throughout the course of the CSPC Geotech project, one point has become abundantly clear, the United States can and should marshal its allies and partners with a vision for liberal democracies' role in setting technology standards and fostering innovation leadership. While China will rely on the size of its own domestic market and seek to partner with existing and aspiring authoritarians—or enmesh the developing world in corruption and debt colonialism—the United States and its allies can build an alternative to China's digital mercantilism. U.S. policymakers should note that allies and partners are something that Washington is lucky to have while Beijing increasingly alienates other nations. The stakes are particularly high. For example, as data volume drives artificial technology development, China has few limits to how much data it can appropriate from its citizens without recourse, as well as a simple mathematical advantage in the size of its domestic population. Building shared technology approaches can address some of these advantages that China has established simply through size and volume.

That said, we cannot assume that the security or economic decisions made in Washington will immediately mesh with those of our allies. While an increasing number of countries around the world

have banned Huawei from their 5G networks, others remain open to Chinese access to their networks and data for the sake of faster, cheaper 5G deployment. For many countries, there are complicated economic interests in play. Take, for example, Germany where many in major car companies like VW, BMW, or Daimler have close ties to Huawei—on top of their firms' massive revenues from the Chinese market.[32] Economic interests have limited Germany's willingness to confront China on human rights, even as broader German industry groups—breaking from the big players—urge less reliance on China.[33] European awareness of the risks of China has grown, but suspicion of Washington remains.

On the other hand, as past Geotech reports have highlighted, allies like Japan have long understood the Geotech challenge from China. Tokyo was aware of China's approach to technology and trade long before Washington, as Japan's experience with the 2011 rare earths embargo, and the successful effort to prepare domestic industries to be less dependent on China, for example, also serves as an example of other nations shared Geotech challenges. How democracies might organize together, or espouse shared values for technology and innovation leadership, will be a key concern for policymakers focused on building Geotech coalitions.

- HARMONIZING DATA REGIMES, ESTABLISHING DATA TRUST

  Previous CSPC Geotech reports highlighted the proposals put forth by then Japanese Prime Minister Shinzo Abe for a "data free flow, with trust," designed to provide a shared foundation for global data management. To continue to grow and develop the data-driven global digital economy—as well as to match the user pool of China's domestic marketplace—it is necessary to find common ground between liberal democracies to allow cross-border data flows. However, significant challenges to finding such trust remain.

  Transatlantic data agreements are among the thorniest issues confronting policymakers, as the European Union has moved firmly to pursue privacy protection regulations and actions, notably the implementation of the GDPR in 2018. Significantly, the European Court of Justice Decision in *Data Protection Commissioner* v. *Facebook Ireland and Maximillian Schrems*—known as "Schrems II" has invalidated the past European Commission adequacy determination for the EU-U.S. Privacy Shield Framework that brought transatlantic data transfers under the program into compliance with EU privacy rules.

  As officials from the Office of Director of National Intelligence, Department of Justice, and Department of Commerce stated at the end of September 2020:

  > The need for constructive and good faith engagement between the EU and the United States on cross-border data issues has never been more urgent. More than

[32] Katrin Bennhold and Jack Ewing, "In Huawei Battle, China Threatens Germany 'Where It Hurts': Automakers." *The New York Times.* January 16, 2020. https://www.nytimes.com/2020/01/16/world/europe/huawei-germany-china-5g-automakers.html
[33] Matthew Karnitschnig, "How Germany opened the door to China—and threw away the key." *POLITICO.* September 10, 2020. https://www.politico.eu/article/germany-china-economy-business-technology-industry-trade-security/

> two months after the ECJ's decision, the operative rules remain decidedly unclear. While the U.S. government remains committed to negotiations with the European Commission on enhancing Privacy Shield to address the ECJ's concerns in *Schrems II*, the ongoing uncertainty surrounding EU-U.S. data transfers puts companies and individuals on both sides of the Atlantic in an increasingly untenable position.[34]

Beyond the transatlantic disputes, newly crafted U.S. trade agreements have addressed digital trade concerns. Both the U.S.-Japan and U.S.-Canada-Mexico trade agreements have developed common standards for promoting and protecting digital trade.[35] Such progress has so far eluded negotiators in the U.S.-EU trade space under both the Obama and Trump Administrations.

Building on this progress, it is important to begin a U.S.-Japan-Europe dialogue—which could be expanded to include other international partners—to find a common ground on a data marketplace that addresses privacy and data management concerns, while also competing with both China's domestic marketplace and model for data management.

- INTERNATIONAL STANDARDS

  An area of particular concern is the growing influence of China in international organizations, including bodies that set international standards for technology. Specifically this has manifested itself in increased PRC representation and leadership in key bodies and efforts to promote Chinese technology standards over Western ones. These are areas where the U.S. and its allies have unfortunately ceded influence—across administrations and governments—as Beijing prioritized these international fora. This has provided China with increased influence as the pathways for future technologies are set, while also allowing international standards to be tilted towards China's model.

  These efforts run the gamut from high-level strategic decisions to the nuts-and-bolts of international commerce. On one hand, for example, China is advocating for a more top-down, state run internet before the International Telecommunication Union, the UN-body for international communications standards and agreements—which happens to be run by Chinese telecom engineer Houlin Zhao.[36]

  On the other hand, there are a range of other, less significant but equally important standards to consider. As Emily De La Bruyere and Nathan Picarsic noted in their research on the Chinese Ministry of Transport's National Transportation Logistics System, or LOGINK, a Chinese

[34] Bradley Booker, Sujit Raman, and James M. Sullivan, "The Need for Clarity After Schrems II." *Lawfare*. September 29, 2020. https://www.lawfareblog.com/need-clarity-after-schrems-ii

[35] "Fact Sheet on U.S.-Japan Digital Trade Agreement." Office of the United States Trade Representative. October 2019. https://ustr.gov/about-us/policy-offices/press-office/fact-sheets/2019/october/fact-sheet-us-japan-digital-trade-agreement

[36] Anna Gross and Madhumita Murgia, "China and Huawei propose reinvention of the internet." *The Financial Times*. March 27, 2020. https://www.ft.com/content/c78be2cf-a1a1-40b1-8ab7-904d7095e0f2

government-run "Facebook for global transportation" serves Beijing's economic and security interests, even as the rest of the world buys into the system for commercial convenience:

> A logistics information system hardly sounds like the stuff of great power politics. It certainly does not sound like a bid to redefine global affairs. In fact, it sounds unfathomably boring. But this integrated, multi-dimensional, Beijing-controlled information system fuels a revolutionary form of power…It allows Beijing to control how resources are exchanged by controlling the information on their exchange. Chinese leaders promote LOGINK as a global standard and platform for modern transportation and exchange. If LOGINK is accepted as such, Beijing will be able to cement international information superiority and control. Those promise enduring and mutually reinforcing advantages in commerce, military affairs, and global governance.[37]

Understanding the importance of these standards-setting bodies and exercises is key to countering China's influence in setting global technology standards. Ceding the playing field to China will allow it to shape the path of future technology and data flows in its favor.

- PROTECTING SUPPLY CHAINS & NETWORKS

  Building on previous agreements—including "The Prague Proposals" from the May 2019 Prague 5G Security Conference and the *Criteria for Security and Trust in Telecommunications Networks and Services* developed by Washington, D.C., think tank CSIS with input from international telecommunications experts[38]—the U.S. State Department expanded the Clean Network (focused on 5G network security) to include app stores, apps themselves, cloud hosting, communications cables, and digital traffic to U.S. facilities.[39]

  At the same time, U.S. allies and partners have continued to show growing skepticism about Huawei hardware as they plan their nations' 5G rollout. In addition to those nations already restricting Huawei, ZTE, and others, the Trump administration has reached bilateral deals with Central and Eastern European countries on 5G security; Sweden has banned Huawei and ZTE; and the UK reversed its previous decision to allow Huawei in the "peripheral network" in favor of

[37] Emily De La Bruyere and Nathan Picarsic, "Beijing's Innovation Strategy: Threat-Informed Acquisition for an Era of Great Power Competition." Acquisition Research Program, Naval Postgraduate School. Monterey, CA. April 28, 2020. https://event.nps.edu/conf/app/researchsymposium/unsecured/file/697/SYM-AM-20-091_Panel#7_de-La-Bruyere_Paper_04-28-2020.pdf

[38] "Prague 5G Security Conference announced series of recommendations: The Prague Proposals," Government of the Czech Republic. May 3, 2019. https://www.vlada.cz/en/media-centrum/aktualne/prague-5g-security-conference-announced-series-of-recommendations-the-prague-proposals-173422/ and "Criteria for Security and Trust in Telecommunications Networks and Services," Center for Strategic and International Studies. May 2020. https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/200511_Lewis_5G_v3.pdf

[39] "Remarks to the Press, April 29, 2020," Secretary of State Michael Pompeo. Washington, D.C. https://www.state.gov/secretary-michael-r-pompeo-at-a-press-availability-4/

removing and banning their hardware.[40] The United Kingdom has begun to finalize its proposals for a 2021 deadline to remove Huawei equipment, upending expectations that Huawei hardware would remain in the UK up until 2027.[41]

U.S. and allied policymakers and industry leaders are also moving towards Open RAN and V-RAN architectures that will help to promote a greater number of wireless hardware vendors and break the stranglehold that some vendors, like Huawei, have on soup-to-nuts solutions for network providers. By utilizing Open RAN and other virtualization architectures, many of the key processes in the 5G network are moved into data centers rather than network hardware. Like the proliferation of suppliers for personal computers and information technology as computing moved from mainframes to personal devices, this will open the playing field further for 5G suppliers and promote greater diversity and resilience within supply chains.

- JOINT COOPERATION & SHARED VALUES

  Recently, there have been discussions about what a gathering of democracies focused on Geotech might entail. How might the G-7 address this topic? Could it be expanded to proposed "D-10" to encompass more democracies beyond the Japan and the transatlantic partners?[42] President-elect Biden has called for such a summit of democracies.[43] While questions remain about who would be invited and what would be on the agenda, these groups present an opportunity to build multilateral coordination on technology policy, trade, data management, supply chain security, and other Geotech issues.

  While questions about those high-level fora are considered, policymakers should continue to recognize that much of the cooperation on these security issues is happening in ad-hoc forums, bilateral dialogues, and various government and industry working groups. At the practical level, a range of measures to further integrate security cooperation, promote threat and intelligence information-sharing, establish common security clearance protocols, harmonize export controls, etc. have been discussed by policymakers and private sector leaders.

  Democracies standing together on these issues is important, and high-level discussions can serve to set strategic Geotech goals; lay the foundation for further digital trade and innovation; harmonize data management and privacy protection; and ensure practical-level cooperation on technology security and innovation leadership.

---

[40] Robbie Gramer, "Trump Turning More Countries in Europe Against Huawei." *Foreign Policy*. October 27, 2020. https://foreignpolicy.com/2020/10/27/trump-europe-huawei-china-us-competition-geopolitics-5g-slovakia/

[41] Sebastian Payne and Nick Fildes, "UK to ban installation of Huawei 5G equipment from September." *The Financial Times*. November 29, 2020. https://www.ft.com/content/c8e7ee9a-4661-4890-a41a-6a7b59f1caba

[42] Erik Brattberg and Ben Judah, "Forget the G-7, Build the D-10." *Foreign Policy*. June 10, 2020. https://foreignpolicy.com/2020/06/10/g7-d10-democracy-trump-europe/

[43] "The Power of America's Example: The Biden Plan for Leading the Democratic World to Meet the Challenges of the 21st Century." Biden Harris 2020. https://joebiden.com/americanleadership/

What becomes a paradox for policymakers is to explain how some of the measures undertaken by democracies—while appearing similar to some Chinese actions—are in fact grounded in entirely different values to pursue different interests and goals, all the while featuring a variety of guardrails intended to safeguard civil liberties. Surveillance in western societies is for protecting citizens, not for regime protection and internal suppression. Data rules are designed to protect users' privacy and ensure flows of data and information, rather than to steal intellectual property, surveil citizens, and censor debate. Policies designed to promote innovation leadership are built upon competitive market economies, not state-support ranging from subsidies to espionage. At the highest level—both in rhetoric and action—leaders and policymakers in liberal democracies must continue to espouse this difference. The fundamental cornerstones of the rule of law, civil liberties, free enterprise, and human rights are far firmer footing than the whims of authoritarian dictators and party cadres.

FOSTERING INNOVATION LEADERSHIP

The United States cannot expect to compete in Geotech if it does not foster continued innovation leadership. As was stated in the September 2019, CSPC Geotech program report, *Geotech: Fostering Competitiveness for Technological Competition:*

> To win the Geotech competition, the United States needs a robust, 21st-century economy. The long-term nature of this competition means that focusing solely on confronting our competitors will likely isolate the United States from the dynamism of the world economy, creating uncertainty across sectors and stifling innovation. Positioning the United States for long-term success requires bolstering the ecosystem that ensures that the United States can reach its competitive potential. Across-the-board, this requires a careful examination of what policies can promote innovation and strengthen the United States, ensuring that entrepreneurialism, innovation, and openness are harnessed, rather than stifled by attempts to "out-China, China."

This fundamental dynamic remains unchanged. The United States is in far more control over what it does to foster its own strengths, ensure economic dynamism, and continue innovation leadership than the choices of Beijing.

Policymakers can help to ensure that the United States is best set for this competition by encouraging the roll out and deployment of technologies to speed "first mover" advantages; continuing and providing further measures to support R&D and protect IP; promoting supply chain security and production capacity; honing an innovation-oriented regulatory environment; building a Geotech-ready workforce; and ensuring that government is well-informed and well-organized to address this challenge.

- <u>DEPLOYMENT & 'FIRST MOVER' ADVANTAGE: 5G EXAMPLES</u>
  One of the key factors in determining technology leadership is the "first mover" advantage that comes from developing technologies, deploying them, and developing use cases for them. For

example, early U.S. leadership in 4G technology laid the foundation for smartphones and the app-based ecosystem that we use today. Deployment of technologies like 5G networks covering American communities or the training of artificial intelligence in real world environments is key to improving these technologies and furthering their development and use.

For example, as the COVID-19 pandemic has forced Americans to work and learn at home, the digital divide in American society has become more apparent. The need to ensure reliable, high speed internet access is vital for Americans to be full participants in a modern society and economy. However, underserved urban areas and parts of the rural and exurban areas do not have wired internet access needed for broadband. Hastening the deployment of 5G and its reach can help these communities, while also providing coverage for the growing number of 5G handsets now on the marketplace. Further 5G coverage provides opportunities for commercial efforts, as well as to apply 5G connectivity in fields like agriculture, transportation, and manufacturing.

These deployments also hasten further advances and innovations within these important technologies. For example, a joint deployment of mmWave systems in Wisconsin, by U.S. Cellular, Ericsson, and Qualcomm, has demonstrated how long-range 5G coverage can be provided on mmWave spectrum—once believed to be best suited for dense urban coverage.[44] Continuing to test these technologies in real world environments provides opportunities for testing technology, honing it, and developing future innovative applications and uses.

At the same time, the measures taken by the FCC to open un-used or under-utilized spectrum for 5G and other telecommunications purposes are also worth noting as 5G networks grow. As noted in previous CSPC Geotech reports, spectrum allocation is key for speeding the 5G rollout, alongside policies that continue to promote competition amongst network providers.

- <u>SUPPORTING R&D & PROTECTING ITS FRUITS</u>

  In a range of measures, the U.S. government is moving to enhance its support for technology R&D. The 2021 National Defense Authorization Act, or FY21 NDAA, provides measures supporting 5G development, artificial intelligence, quantum computing, and a range of other advanced technologies.[45] The CHIPS for America Act—introduced by Senators John Cornyn and Mark Warner and Rep. Michael McCaul in their respective chambers—provides $22 billion in various incentives and support for semiconductor R&D and other measures to protect and promote the American semiconductor industry.[46] Recognizing the importance of global supply chains and allied partnerships, the CHIPS for America measures included in the FY21 NDAA call

[44] "U.S. Cellular, Qualcomm and Ericsson Achieve Extended-Range 5G Data Call Over mmWave," Qualcomm Press Release. September 17, 2020. https://www.qualcomm.com/news/releases/2020/09/17/us-cellular-qualcomm-and-ericsson-achieve-extended-range-5g-data-call-over

[45] "Fiscal Year 2021 National Defense Authorization Act," U.S. Senate Committee on Armed Services. Accessed October 20, 2020. https://www.armed-services.senate.gov/imo/media/doc/FY%2021%20NDAA%20Summary.pdf

[46] https://www.congress.gov/bill/116th-congress/senate-bill/3933

for the creation of a Multilateral Microelectronics Security Fund—for U.S. and allied harmonization of semiconductor policies and research.

If the results of R&D support—technology innovations and intellectual property—find their way into Chinese hands, then all the U.S. government will have done is support China's advances. Therefore, be it patent enforcement or counterintelligence, protecting IP must go hand-in-hand with developing it.

Finally, as discussed in the conceptualization of technology ecosystems, R&D in the United States is driven by firms' revenues from sales in dynamic global economies. Disrupting or decoupling would have an impact on this revenue and capacity for R&D. Therefore, policymakers should be aware of this interrelationship between international commerce, revenue, and innovation as they plan policies to address global technology competition and security.

- GETTING REGULATION RIGHT

  When it comes to technology, the U.S. political and regulatory environment is becoming ever more complex. "Big tech" finds itself facing bipartisan suspicion over its size, control of content, and accusations of anti-competitive behavior, yet they are the main U.S. players in this international tech competition. Popular perceptions of technology run amok can push policymakers to pursue counterproductive policies.

  The Department of Justice antitrust case against Google and the House Judiciary Committee report addressing Amazon, Apple, Facebook, and Google both represent the increased attention from Washington to these large and often-popular companies. A challenge is that anti-trust laws and regulations have little to do with policymakers' concerns about privacy, data protection, and restrictions on content. Where the laws and regulations can be applied to competitiveness must be considered in balance with multinational competition and the fundamental differences between the digital and physical economy—where often the products are provided free of charge.

  A challenge for the United States in dealings with international partners regarding data management is the lack of a national data management or data privacy law. While the Europeans have the GDPR, the United States features a 50-state patchwork of sectoral and state laws, with California's Consumer Privacy Act, or CCPA, often serving as the most prominent example. Beyond addressing the uncertainty in the current legal environment and questions about what the "U.S. position" on data privacy in fact is, such a measure can also put into place the type of data protection requirements and consumer notifications that could also serve to strengthen national cyber defenses.

Finally, there have also been rumored discussions, that regularly resurface, about the creation of a nationalized 5G network. The creation of nationalized networks, further regulatory capture, and overly prescriptive regulation would threaten the competitive, dynamic, free enterprise that has led to current U.S. technology leadership and serves as the foundation for future success.

- THE GEOTECH WORKFORCE

  In discussions largely focused on technology, the human element cannot be forgotten. Ensuring that the United States has a well-educated, highly trained workforce is needed to ensure innovation leadership. The U.S. lags behind China in the key STEM workforce metrics for competitiveness.[47] The pandemic is likely to further exacerbate divides within the United States in terms of quality of education, as well as the courses of education and launchings of careers disrupted by this crisis. There is also the severe institutional impact of the pandemic, as research universities and other institutions of higher learning are forced to tighten their belts.

  While it is important to ensure that our universities are not leaking national secrets to foreign agents, international students are vital to U.S. research—and to the bottom line of our universities and overall economy. Students coming from abroad to study in the United States contributed $41 billion to the U.S. economy, supporting nearly half a million jobs, in the 2018-2019 academic year.[48] At the same time, the U.S. immigration system needs significant reform to address both security and economic needs. For the sake of Geotech competition, this is important, as the United States needs to attract and keep, students and immigrants that will become entrepreneurs, scientists, and engineers.

- ORGANIZING GOVERNMENT

  One challenge for U.S. policymakers is that the United States does not have the types of ministries that other nations may have for Geotech policy. On the other hand, presidential authorities and White House advisors combine to be effective super-ministries for many issues—including Geotech. During the Trump administration, many authorities were streamlined and consolidated within the White House. When its last occupant departed in 2018, the Trump administration shelved the "cyber czar" post.[49] There is bipartisan pressure in Congress to restore such a position.[50]

  Within the agencies themselves there are a range of Geotech programs: from research at the Pentagon to the Clean network initiatives at the State Department to the export controls at the

[47] Arthur Herman, "America's High-Tech Stem Crisis." *Forbes.* September 10, 2018. https://www.forbes.com/sites/arthurherman/2018/09/10/americas-high-tech-stem-crisis/#253a6075f0a2

[48] "Economic Value Statistics," NAFSA: Association of International Educators. Washington, DC. Accessed September 22, 2020. https://www.nafsa.org/policy-and-advocacy/policy-resources/nafsa-international-student-economic-value-tool-v2

[49] "Trump scraps cyber czar post after first appointee leaves: White House." *Reuters.* May 15, 2018. https://www.reuters.com/article/us-usa-cyber-whitehouse/trump-scraps-cyber-czar-post-after-first-appointee-leaves-white-house-idUSKCN1IG3GG

[50] Maggie Miller, "Congress backs push for national cyber czar." *The Hill*. July 16, 2020. https://thehill.com/policy/cybersecurity/507583-congress-backs-push-for-national-cyber-czar

Commerce Department's Bureau of Industry & Security. Coordination of the interagency process could be better supported through a combination of White House-level coordination through the National Security Council, Council of Economic Advisors, and the Office of Science and Technology Policy, as well as the consolidation of Geotech portfolios within departments and agencies themselves. For example, current Under Secretary of State for Economic Growth, Energy, and the Environment Keith Krach has been responsible for the expansion of the Clean network initiatives.[51] This position, or an Assistant Secretary role reporting to it, could serve as a point person for international cooperation on digital trade, data management, data privacy, and cybersecurity.

To improve lawmakers' capabilities to address Geotech issues, some of the proposed reforms of the House Select Committee on Modernization are worth noting. First, the re-creation of the Office of Technology Assessment (OTA) would reverse past cuts to research support related to legislators' inquiries regarding science, technology, and innovation. The proposals also include increased resources and budget for Congressional staff, allowing for more competitive salaries and additional staffing.[52]

[51] Peter Coy, "U.S. Policy on China May Move from 'America First' to America & Co." *Bloomberg Businessweek*. December 9, 2020. https://www.bloomberg.com/news/articles/2020-12-09/u-s-policy-against-china-america-first-is-becoming-america-and-others

[52] Derek Kilmer, chair, and Tom Graves, v. chair, "The Select Committee on the Modernization of Congress Final Report." October 2020. https://modernizecongress.house.gov/imo/media/doc/ModernizationCommittee_10152020r1Compressed%20(newest%20gpo%20report).pdf

CONCLUSION & RECOMMENDATIONS

Addressing the complex nature of the Geotech challenge requires strategic thinking and vision. While the zero-sum nature of recent Washington politics has made achieving either of those challenging, there is now bipartisan agreement on the importance of Geotech. There is a shared recognition of the challenge posed by China's adversarial approach, as well as the importance of the technological underpinning of our national security and economic prosperity. Planning for technological innovations becomes a matter of *when*, not *if*, and policymakers must now focus their concern on *where*. It requires a careful balance of protecting secrets while ensuring an open door for commerce and engagement. Industries should be protected from hostile foreign governments and their authoritarian, mercantilist policies, not from competition, consumer trends, or their own mismanagement. Clear rules of the road must be established for a level playing field—one that ensure equal opportunity, fair trade, and protections of fundamental rights and privacies. The Geotech competition will continue to be one where interests and innovation will remain constantly fluctuating, while shared values and principles must continue to be the guide star.

Recommendations

- DEVELOP BASIC FEDERAL STANDARDS FOR DATA MANAGEMENT & PRIVACY
  In order to prevent a patchwork of state-level regulations for data management and privacy protections, a basic federal standard should be developed by Congress that balances regulatory predictability for digital services companies with concerns about data privacy and fair competition. This legislation would also boost U.S. prospects for securing important international data transfer agreements by establishing a "U.S. position."

- RESTORE WHITE HOUSE COORDINATING POSITION(S)
  To facilitate the interagency coordination of Geotech issues and commensurate with recommendations from Congress, including the Cyber Solarium Commission, the position of National Cyber Director, responsible for "cybersecurity and associated emerging technologies" should be established. Other more civil- and economic-oriented positions and bodies such as the Office of Science and Technology Policy (OSTP) and Council of Economic Advisors should also be included in Geotech policy coordination for a balance of policy perspectives, while the National Security Council should have a technology directorate for coordination of these issues.

- IMPROVE CONGRESSIONAL TECH SUPPORT
  The recommendations of the Select Committee on the Modernization of Congress provide a pathway forward to improve Congress's staffing on and oversight of technology matters.

- CONTINUE SUPPORT FOR 5G ROLLOUT, OPEN RAN ARCHITECTURE, COMPETITIVE NETWORKS
  The deployment of 5G networks can bridge the digital divide and provide the foundation for developing future innovations, connected industries, and near-constant connectivity.

Policymakers should continue policies hastening 5G deployment. Policies promoting the adoption of Open RAN architectures and reallocation of underutilized spectrum can continue to ensure competition among network suppliers, while not establishing a nationalized 5G network ensures competition among network providers.

- FURTHER EXPORT CONTROLS IF NECESSARY
  Tools like export licensing, export controls, and entity listing should be applied in a targeted manner to ensure that state-supported, state-affiliated, Chinese military fusion firms and researchers do not benefit from high-tech, cutting-edge American technologies.

- YET, UNDERSTAND COMMODITIZED TECH & INTERDEPENDENCE
  Controls applied to the cutting-edge of technology must be balanced with an understanding of the current interdependence of the United States, China, and many other countries through global supply chains. Furthermore, many technologies are highly commoditized, low-tech items that do not post a security risk—and can easily be acquired elsewhere. Carefully reducing dependency on potential adversaries can avoid the unintended consequences of a rapid decoupling.

- LIBERAL DEMOCRACIES STAND TOGETHER ON VALUES, EXPAND & HARMONIZE TECH COOPERATION
  While technologies are finding various fora in which to discuss Geotech issues, it is worth finding common ground and reminding the world of the importance of the shared values that underpin liberal democracies approach to technology and innovation leadership. The underpinnings of the rule of law, due process, civil liberties, and human rights stand in stark contrast to China's model. A U.S.-Europe-Japan dialogue, or similar grouping of democracies, on data management and privacy should be pursued for commercial and security interests. Where possible, and building on the successful model of the "Five Eyes" countries, the U.S. and its closest allies should develop shared standards for intelligence sharing and security clearances; seek harmonization of defense industrial base security, classified patents, and export controls; stand up jointly utilized tools and resources like the Multilateral Microelectronics Security Fund; and pursue joint R&D in advanced emerging technologies.

- CONTINUE CLEAN NETWORK INITIATIVES
  To provide safe and secure networks, supply chains, data management, and data storage, the Clean Network initiatives serve as a useful starting point for cooperation among liberal democracies. Alongside hopeful progress towards U.S. federal data privacy standards, these dialogues and discussions can be also address international data management and digital trade issues.

- INVEST IN R&D & HI-TECH MANUFACTURING CAPACITY

  Along the lines of measures like The CHIPS Act and the American Foundries Act, policymakers should look to support R&D in advanced emerging technologies, while also addressing supply chains dependent on adversaries or subject to other supply bottlenecks in times of increased tensions or open conflict.

- SUPPORT EDUCATION THROUGH COVID-19 AND BEYOND

  Given the impact of the pandemic across the education system—and upon the progress of students—significant support will be needed for education. State higher education institutions are in particular danger from state and university revenue shortfalls. At the same time, as technological innovations have been applied to virtual learning and other new curriculums and pedagogies during the pandemic, harness lessons learned here to improve education access.

- IMPROVE DIALOGUE BETWEEN TECH & POLICYMAKERS

  Given the importance of these topics for national security and economic prosperity, a growing chasm between government and the private sector—especially in technology—is always of concern. While there are significant policy issues to be addressed because of technology's impact, the politicization of technology regulation threatens one of America's most important industries for its competitiveness and strategic footing.

ACKNOWLEDGMENTS

On behalf of the Center for the Study of the Presidency & Congress, I want to thank the following for their contributions to CSPC's work on Geotech strategy.

The Japan External Trade Organization, Qualcomm, NTT, and the Dr. Scholl Foundation for their generosity, expertise, and engagement. Thanks to these groups, we are able to continue our research and convening on this important topic.

I want to also thank the lawmakers and the members of their staffs—in Washington and other allied capitals—who have engaged in these dialogues and worked with CSPC staff on framing policy challenges and identifying solutions. I want to particularly acknowledge the support and expertise of Dr. Kenzo Fujisue, Member of the House of Councilors of Japan.

The Trustees and Counselors of CSPC, thanks to their support and wisdom, CSPC is able to ensure its mission of learning the lessons of history, address today's strategic challenges, and educating the leaders of tomorrow.

Our David M. Abshire Chairholder, former House Intelligence Chairman Mike Rogers, as he continues to demonstrate his strategic vision, leadership, and a commitment to protecting the United States while championing a bi-partisan approach to national security.

Dan Mahaffee, the Senior Vice President and Director of Policy at CSPC, for his leadership of this project and related outreach, as well as writing and editing many of our Geotech materials; Joshua Huminski, the Director of the Mike Rogers Center, for his research work on great power competition and technology and his coordination of virtual events; and Erica Ngoenha, the Director of Fellows and External Affairs, for her outreach to Capitol Hill.

Our Senior Fellows and Advisors who contributed to this project—Frank Cilluffo, Maia Comeau, Samantha Clark, Brendan Hart, Robert Gerber, Andy Keiser, James Kitfield, Michael Stecher, and Joshua Walker—who applied their expertise from a range of fields to analyze the impact of these technologies and the challenges they pose for policymakers.

Our entire team at the Center that made this report possible: Danielle Anjeh, Oscar Bellsolell, Ethan Brown, Chris Condon, Eric Dai, Maria Damsgaard, Bekah DeBoer, Michelle Miller, Wyatt Newsome, Aida Olivas, Nick Schroeder, Sara Spancake, Emily Stone, Thomas Triedman, and Tania Vazquez.

Finally, I would like to thank all of those who dedicated time to our effort by attending roundtables and offering frank and invaluable advice.

Glenn Nye
President & CEO
Center for the Study of the Presidency & Congress