CSPC

CENTER FOR THE STUDY OF THE PRESIDENCY & CONGRESS

GEOTECH IN THE EARLY BIDEN ADMINISTRATION

MARCH 2021

CENTER FOR THE STUDY OF THE PRESIDENCY & CONGRESS

GEOTECH IN THE EARLY BIDEN ADMINISTRATION

CSPC GEOTECH UPDATE

March 2021

DAN MAHAFFEE
Project Director

JOSHUA HUMINSKI
MICHAEL STECHER
Report Contributors

MILES ESTERS
SARAH NAIMAN
JACQUELINE RUIZ
Researchers

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The Biden administration has moved quickly to address Geotech issues and the competition with China and Russia. In this report, we first examine the latest actions of these two main competitors and the context provided for the early steps by the Biden administration. This report then looks at some of the key players in the Biden administration's Geotech team, and how their past professional and academic work—as well as statements during the nominating and confirmation process—can inform us about future Geotech policy in this administration. Following the overview of personnel, the report turns to the early steps undertaken by the administration on Geotech—with particular attention to the February 24, 2021, Executive Order launching a review of strategic supply chains and their vulnerabilities. The report concludes with a look ahead towards prospects for cooperation with allies on Geotech issues, particularly as they maintain the preceding administration's tough approach to China with the contrast of a defter touch with allies.

What is clear from the initial steps of the Biden administration—as well as growing bipartisan consensus on Geotech issues on Capitol Hill—is that the United States is moving through the phase of beginning to recognize the Geotech challenge. Now, the emphasis is on building the structures, lines of authority, and institutional capacity to craft and execute needed policies.

China: Geotech, Human Rights, & Security

- China's presents clear security threats in the physical and digital domains, while its actions speak for themselves in terms of human rights, free expression, and other liberal values shared by the United States and fellow liberal democracies. Economic interdependence and commercial interests complicate addressing these former two challenges—yet recognition of supply chain resilience and over reliance on China is growing.
- As the world witnesses, Beijing's crackdown on political freedom, free expression, and the rule of law in Hong Kong continues apace. Across China, in Xinjiang, the continued repression and genocide of the Uighur people continues, with technological tools playing a key role in monitoring, repressing, and imprisoning Uighurs. The examples of Hong Kong and Xinjiang lay bare the approach by Xi Jinping and the Chinese Communist Party to human rights—and the role of Chinese technology companies in furthering repression.
- Recent actions by Chinese security officials suggest that China is further extending censorship measures abroad—including intimidation of dissidents abroad, "online pursuits" by Chinese law enforcement, and harassment of the domestic families and friends of Chinese dissidents abroad.
- Concerns about reliance on China for the processing and supply of rare earth materials are not novel. More explicit discussion from Beijing about using rare earths as leverage against Washington, however, has grown in early 2021. Rare earths are an area that can serve as an opportunity to work with allies to reduce dependence on China based on shared economic interests, security concerns, and environmental values.
- The CCP's efforts toward Military-Civil Fusion (MCF) are policies aimed at economic expansion, industrial base development, and technological innovation. MCF should continue to be an area of particular concern for policymakers. However, that concern should be accompanied with a

thorough understanding of the realities of MCF. misperceptions about the MCF may lead U.S. policymakers to emulate Beijing's policies—which may ultimately be counterproductive by limiting enterprise and innovation—while the best lesson to take from the rhetoric and emphasis on MCF Is the scope of the challenge, but the need to respond in terms of our interests and values.

- The upcoming 2022 Beijing Winter Olympic Games loom as a likely diplomatic flashpoint given the international attention to the quadrennial international winter sports event, Beijing's emphasis on events of international prestige, and the genocide and human rights abuses perpetrated by the host nation government. Policymakers in liberal democracies should carefully consider what official recognition is provided to the games, given the genocide and human rights abuses and the likely showcasing of repressive tools and technologies.

Russia: SolarWinds and the Geotech Impact of Cybersecurity Threats

- After four years of what could best be described as a curious public policy towards Russia under the Trump administration, it appears that the newly elected Biden administration aims for a "return to normal" in style.
- What this "return to normal" means in practice very much remains to be seen. For one, it should be noted that on-the-ground, the Trump administration's policies towards Biden administration appointees, thus far, are believers in multilateralism and engagement, both of which could potent well for the future of U.S.-Russia relations. President Trump's antagonism of NATO allies undermined a key tool in confronting Russia. Smart engagement is critical—isolation and refusing to talk is not a strategy. Even during the Cold War, the United States engaged with the Soviet Union while competing globally with Moscow.
- The ultimate threat Russia presents in terms of Geotech is not in that it offers a competing model for governance as China does. Russia is not in the business of exporting its model of authoritarian kleptocracy as Beijing seeks to do with its techno-authoritarianism. Russia does not aim to define a new international order so much as it seeks to reclaim its great power status and undermine the western liberal order led by or embodied by the United States.
- International adventurism serves two concurrent purposes for President Putin and the Kremlin. First, there is the obvious direct benefit to Russia's national security and foreign policy. A weakened and divided West is less a threat to Russia's interest than a unified, coordinated NATO or European Union. Second, the foreign adventurism provides the Kremlin with a means to mobilize domestic support and undermine domestic opposition.
- Given the aforementioned interests and societal conditions, cyber warfare and cyber conflict represent, perhaps, the greatest tool for Moscow—comparably cheap (when set against conventional and nuclear forces), deniable (to a degree), and hugely impactful.
- The last five years alone are replete with examples of Russia's hacking efforts in terms of preparation of the battlefield, intelligence collection, mis- and dis-information, and more. Russia has demonstrated a propensity and talent for cyber operations; a propensity for which was vividly on display with the SolarWinds breach
- It is important to recognize that the SolarWinds breach was not an attack per se. Rather, it was an intelligence-gathering effort. The Russians achieved a significant success, collecting information and data for nearly a year before being detected and exposed. The investigation

and remediation of this breach will take a considerable amount of time. Nearly three-months-on from the attack and the federal government is still unsure of just how widespread the breach was and how many users were affected.

- How did the Russians achieve such a spectacular intelligence success? There are three key components to this attack that are worth noting. First, the Russians piggy-backed on the SolarWinds regular network update software to get behind the security measures of the agencies and companies they targeted. This use of the supply chain as a trusted vector proved to be a novel mechanism to circumvent security protocols. Second, the breach used domestic, U.S. servers allowing the hackers to not only mask the hack's origin, but to use U.S.-law against itself. Finally, once onto the networks, the Russians waited, watching first to see if their penetration had been detected, but then, and more importantly, to learn what the cybersecurity protections were and what protocols existed.
- The mechanism and process by which the SolarWinds breach occurred is unlikely to stay in the proverbial box. Given the previous attempts at mimicking trusted vendors and supply chain attacks, and the success of the SolarWinds breach, this type of hack is likely to be replicated by other actors—Russian or otherwise.

Early Biden Administration Geotech Appointments

- President Biden enters office with a very well-established cadre of advisors across a variety of policy areas, but in foreign policy, especially with regards to China, the initial group of advisors in the White House, State Department, and Defense Department come to office as a preexisting network.
- In analyzing the appointees for key posts on the National Security Council and cabinet agencies, it is clear that President Biden comes to office with a group of advisors and senior officials who already have his trust and have collaborated publicly for several years to develop a Geotech strategy nested within a China strategy.
- This group has identified that China is a strategic rival that is trying to set the rules of the road in high technology, establish at least regional economic and military preeminence, and close off the global commons to create a sphere of influence.

Early Administration Actions

EXECUTIVE ORDER ON SUPPLY CHAINS

- As its personnel have taken their places, the Biden administration has also moved quickly on Geotech issues, especially in setting their mark on U.S.-China policy and cooperation with allies and partners. The tone has been set directly from the top, as President Biden has said that China should expect "extreme competition."
- The most impactful early action by the Biden administration, thus far, is the February 24, 2021, Executive Order on America's Supply Chains. Of immediate importance is the 100-day review launched in the key areas of semiconductors, batteries, rare earths, and pharmaceuticals.
- The attention to semiconductors is grounded in their strategic importance, as well as the current semiconductor shortage that has slowed goods ranging from Ford F-150s to PlayStation 5s.

- Similarly, the attention to batteries and rare earths reflects both the strategic importance of certain minerals—lithium for batteries in addition to the other rare earths—and how China has a powerful position in those supply chains.
- Following the COVID-19 pandemic, the attention to pharmaceuticals comes at a time when concerns have been raised about reliance on foreign suppliers for key chemicals and compounds, as well as basic medical equipment.
- Indications are that key industry groups are welcoming this review, and government and private sector cooperation will be key to ensuring that this is an effective exercise to secure vital supply chains.

POTENTIAL FUTURE TECHNOLOGY RESTRICTIONS

- While the private sector has been complementary regarding the Executive Order on the supply chain, they are more concerned about rules that remain from the Trump administration that would give the Department of Commerce authority to restrict trade and commerce with China related to advanced technologies and information technology that is a threat to U.S. national security.
- Where industry objects are in terms of the broad scope of the measures, and the impact that it may have on industries that are particularly reliant on information technology supply chains that have yet to readjust to Geotech concerns. Policymakers should also be aware of the likelihood of Chinese retaliation, which, as we have seen, can include detention of executives.

COOPERATION WITH ALLIES

- While continuing approaches towards Beijing similar to the Trump administration, the Biden administration has placed a greater emphasis on the role that U.S. allies and partners can have in the Geotech competition.
- The Biden administration has spoken of a summit of democracies, a concept designed to bring together nations beyond the traditional G-7 to discuss democratic values and shared challenges. This has been seen by many as an opportunity to further Geotech cooperation, as the idea of a "Democratic 10" or "Tech 10" grouping of nations has been bandied about. That said, a major challenge continues to be what nations would be included in such a grouping, depending on how matters of security, commercial interests, and shared values are weighed.
- Where these summits might prove to be of the most utility is not at the summit itself, but in the groundwork laid before and after for continued dialogues on a range of technology policies and issues.
- While most attention on matters of Geotech diplomacy first looks abroad, measures at home are what will put the United States in the strongest position for both the competition with adversaries and cooperation with allies. It is important for the United States to establish its own standards reflecting our interest and values for data management and privacy. This can serve as the framework to build harmonization, compatibility, and adequacy with foreign partners—rather than leaving U.S. companies and consumers to deal with a patchwork of foreign rules and state laws.
- Additionally, how the administration organizes for the Geotech challenge will be important. Beyond the roles played on domestic Geotech policy—including in each cabinet agency and

sector specific agencies for various industrial sectors—these officials will increasingly interface with foreign counterparts.

- As the executive agencies are reoriented bureaucratically to address this challenge, the signaling from the White House of the urgency of the issues, as well as the designation at each relevant agency of a key leading individual empowered to move policy will be vital as the broader administration comes together.
- In terms of direct cooperation with allies and partners, several early actions of the Biden administration are of note. Readouts from both Washington and Tokyo illustrated President Biden and Prime Minister Suga's commitment to strengthening the U.S.-Japan alliance. Early dialogue with the Quad members was largely focused on traditional security issues and pandemic response, but can serve as a foundation for future Geotech cooperation.
- As the Biden administration undertakes its supply chain security review, coordination with key allied partners is vital. Japan, South Korea, and the Netherlands, for example, are the technology leaders in semiconductors, while U.S. and Japanese automakers increasingly share supply chains and build partnerships for electric motors and vehicle batteries. Just as U.S. policymakers consult with allies on matters of military exercises and countering China's territorial incursions, these discussions should be accompanied by greater dialogue on supply chain security, resilience, and capacity.
- The U.S. administration should look to measures already undertaken by allies as both an example for potential U.S. policies and an expression of their willingness to address the shared Geotech challenge. Past and contemporary efforts by the Japanese government demonstrate this, and serve as an avenue for Geotech cooperation with a key ally.
- As Taiwan has grown into one of the major powers in terms of semiconductors, particularly in manufacturing, it has become a vital lynchpin of Geotech supply chains, while its democratic ideals and culture stand in stark contrast to what the Chinese Communist Party seeks to define as Chinese history, culture, and politics.
- Taiwan's importance in Geotech supply chains, as well as its democratic example and strategic location, require U.S. and allied policymakers to approach policy to Taiwan in a manner that reflects its importance to both our national security and economic prosperity.

Conclusion

The Biden administration has approached the Geotech challenge with purpose and alacrity. While this report has largely focused on the administration's approach and the developments in the challenge from key adversaries, there is also an opportunity for bipartisan cooperation with Congress on these issues. The new administration has the opportunity not only to work with allies, but also with U.S. allies and partners. While the Trump administration years raised questions about U.S. reliability—and allied concerns about that may continue—the Biden administration has the opportunity to not only rededicate, but also realign our partnerships and alliances to reflect new technology challenges. The upcoming review of policy chain security presents an opportunity to not only promote domestic supply chains, but also to work with our close allies and partners who share common values and join us as innovation leaders. Many priorities will compete with Geotech for attention, particularly given the magnitude of the many other challenges the administration faces. Still, this is an opportunity to institutionalize and build rules and norms around cutting edge technologies and set the stage for future innovation leadership.

INTRODUCTION

Over the past two years, the CSPC Geotech project has explored the growing and active competition between open societies and authoritarian regimes for leadership in advanced technologies vital for national security and economic prosperity. Unlike the Cold War, this competition is marked by the economic interdependence of a globalized world. Furthermore, in contrast to the Cold War, there is no longer the guarantee that the United States and its allies will maintain their technological edge. Instead, this is a period of great power competition, where commercial, security, and values-based factors weigh on our approach to competitors, adversaries, and even allies.

Facing this challenge as they take office, the Biden administration has moved quickly to address Geotech issues and the competition with China and Russia. In this report, we first examine the latest actions of these two main competitors and the context provided for the early steps by the Biden administration. This report then looks at some of the key players in the Biden administration's Geotech team, and how their past professional and academic work—as well as statements during the nominating and confirmation process—can inform us about future Geotech policy in this administration. Following the overview of personnel, the report turns to the early steps undertaken by the administration on Geotech—with particular attention to the February 24, 2021, Executive Order launching a review of strategic supply chains and their vulnerabilities. The report concludes with a look ahead towards prospects for cooperation with allies on Geotech issues, particularly as they maintain the preceding administration's tough approach to China with the contrast of a defter touch with allies.

What is clear from the initial steps of the Biden administration—as well as growing bipartisan consensus on Geotech issues on Capitol Hill—is that the United States is moving through the phase of beginning to recognize the Geotech challenge. Now, the emphasis is on building the structures, lines of authority, and institutional capacity to craft and execute needed policies. At a time when the tech industry finds itself in the crosshairs of political opprobrium and public opinion, a key challenge is bridging the gap between government and the private sector to balance the aforementioned goals of growing businesses for jobs and innovation, securing key technologies, and ensuring that U.S. and allied values are reflected in our technology, its use, and its standards.

Alone, the Geotech challenge would be immense—the shortage currently experienced in the semiconductor supply chains demonstrates the dynamic challenge of Geotech—but this competition also comes while policymakers confront truly unprecedented challenges: the impact of the COVID-19 pandemic and economic recovery; addressing U.S inequity and inequality; and our politics following the Trump administration, falsehoods about the 2020 election, and the January 6th insurrection. The collapse of the electric grid in Texas also reminds Americans that the most advanced technology is a moot point when the foundations of basic infrastructure are hollowed out—as well as the danger when politics seeps into matters of technology, infrastructure, and science. We are also reminded of the importance of technology in keeping us connected to drive commerce, keep us informed, and hold the powerful accountable.

Still, the actions of the administration and Congress suggest that the United States is now addressing the Geotech competition—and seeks to work with allies on these vital technological and policy matters. As competitors challenge the United States and its allies, this report will show the next steps on the path to addressing this challenge.

CHINA'S CONTINUED GEOTECH CHALLENGE

As Geotech competition has burgeoned, no competitor has loomed larger than China. During the Trump administration, a range of measures from the 2018 National Defense Strategy to actions securing advanced technologies and restricting Chinese suppliers. All of this was born of the recognition that future security, economic, political, and economic competition would come from great power peer competitors.

China's presents clear security threats in the physical and digital domains, while its actions speak for themselves in terms of human rights, free expression, and other liberal values shared by the United States and fellow liberal democracies. Economic interdependence and commercial interests complicate addressing these former two challenges—yet recognition of supply chain resilience and over reliance on China is growing.

The conceptual underpinning of U.S.-China competition and analysis of key strategic technologies and industries is covered in detail in the previous CSPC Geotech reports. For the purposes of this examination of the early actions of the Biden administration and Geotech context, this section will look at the latest developments on technology and human rights in China, with developments regarding Xinjiang, Hong Kong, and international digital dissent; threats and bluster from Beijing on rare earth materials; latest analysis of China's military-civil fusion; and, looking ahead, the looming questions that the 2022 Beijing Winter Olympics may present in terms of Geotech and human rights.

Repression in Hong Kong; Genocide in Xinjiang

As the world witnesses, Beijing's crackdown on political freedom and free expression in Hong Kong continues apace. Applying the new National Security Law, authorities have continued mass arrests of pro-democracy advocates, while pursuing draconian sentences under new legal authorities, seeking to replace existing Hong Kong legal norms and values with "patriotism" towards Beijing, and further actions to limit judiciary independence and further restructure the territory's laws and governance to bring to an end "one country, two systems." As February 2021 report from the Center for Asian Law at the Georgetown University Law School opens their report on the National Security Law, "The National Security Law (NSL) constitutes one of the greatest threats to human rights and the rule of law in Hong Kong since the 1997 handover."[1]

These measures raise significant questions about the future of Hong Kong and the foreign response to China's crackdown. In terms of the business environment and commercial interests, Beijing and their apparatchiks in Hong Kong seek to bifurcate business matters from the new national security legal regime, but the environment that once attracted foreign business and talent has been replaced by one where talented Hong Kongers are looking to flee. Furthermore, the free expression that had allowed Hong Kong to thrive, both as an international entrepôt and gateway into China, is under threat from Beijing's actions. In February 2021, for the first time the National Security Law was used to block access

[1] Lydia Wong and Thomas E. Kellogg, "Hong Kong's National Security Law: A Human Rights and Rule of Law Analysis." Center for Asian Law, Georgetown Law, February 2021. https://www.law.georgetown.edu/law-asia/wp-content/uploads/sites/31/2021/02/GT-HK-Report-Accessible.pdf

to pro-democracy sites.[2] Given the wide scope of the National Security Law, its muscular application thus far, and Beijing's long track record on repressing speech and controlling information, it is likely that this is the first of many such actions—which will raise questions about access to information and access to data in Hong Kong.

Across China, in Xinjiang, the continued repression and genocide of the Uighur people continues, with technological tools playing a key role in monitoring, repressing, and imprisoning Uighurs. While accounts about the degradation and abuses of the Uighur people have grown in western media, no account is more harrowing, and disgusting, than that released by the BBC of the systematic torture, sexual abuse, and sterilization inflicted upon Uighurs.[3] One important latest account of how China's technology companies play a key role in this human rights nightmare comes from an example about the use of facial recognition and artificial intelligence. Dahua, a Chinese company specializing in video surveillance, showcased software that could identify faces by race, including materials that suggested that it could identify Uighurs and other ethnic minorities simply by images.[4]

The examples of Hong Kong and Xinjiang lay bare the approach by Xi Jinping and the Chinese Communist Party to human rights—and the role of Chinese technology companies in furthering repression. At the same time, efforts to confront Uighur forced labor in textiles and other basic industries demonstrate the challenges of fully extricating from the abuses underpinning Chinese supply chains. Companies outside China will face increasing pressure—both from governments and customers—as awareness of the CCP's genocide grows. Measures like the Uighur Forced Labor Prevention Act,[5] first introduced in 2020, are likely to be reconsidered in the 117th Congress.

Cracking Down on Internet Dissent, Including Overseas

That the Chinese authorities seek to crackdown on internet dissent is nothing new. Censorship is ingrained into Chinese internet protocols and social media architectures. A recent analysis of the whistleblowers at the early stages of the COVID-19 pandemic in Wuhan—and the resulting crackdown on those who did not toe the line of Beijing's "truth" about the pandemic—reveals how the Chinese regime manages information on the internet and the consequences faced by those who fall afoul of the party's information regime.[6]

One development of note comes from a recent case following online dissent over the recent Sino-Indian border clashes. Using a new law that bans "insulting or slandering heroes and martyrs" to quash

---

[2] Zen Soo, "Hong Kong internet firm blocked website over security law." *Associated Press*, January 14, 2021. https://apnews.com/article/technology-beijing-internet-service-providers-democracy-hong-kong-9b004df447df043ecc7abc044edb2d15

[3] Matthew Hill, David Campanale, and Joel Gunter, "'Their goal is to destroy everyone': Uighur camp detainees allege systemic rape." *BBC News*, February 2, 2021. https://www.bbc.co.uk/news/world-asia-china-55794071

[4] Johana Bhuiyan, "Major camera company can sort people by race, alert police when it spots Uighurs." *Los Angeles Times*, February 9, 2021. https://www.latimes.com/business/technology/story/2021-02-09/dahua-facial-recognition-china-surveillance-uighur

[5] "H.R. 6210 – Uyghur Forced Labor Prevention Act." https://www.congress.gov/bill/116th-congress/house-bill/6210/related-bills

[6] Julia Hollingsworth and Yong Xiong, "The truthtellers: China created a story of the pandemic. These people revealed details Beijing left out." *CNN*, February, 15, 2021. https://edition.cnn.com/interactive/2021/02/asia/china-wuhan-covid-truthtellers-intl-hnk-dst/

critiques of the Chinese military, Chongqing police have arrested seven. While the new law brooking criticism of the national security establishment, with penalties of up to three years' imprisonment, is a new development, the statement from Chongqing police also indicated that they had undertaken an "online pursuit" of one of the suspects—who is a 19-year old Chinese émigré living abroad in Europe.[7]

That the Chinese authorities have sought to quash dissent overseas among Chinese abroad is also not a new development. However, this "online pursuit" and statements about the application of Chinese law to cyberspace suggest that Chinese security officials are establishing extraterritorial enforcement of China's restrictions on online expression—enforcement backed by harassment of family and friends still in China. Yaqui Yang, China researcher for Human Rights Watch, noted:

> Authorities used to harass overseas-based critics or their China-based families without resorting to formal prosecution mechanism or leaving a paper trail…Now they don't feel they need to be discreet about it, or maybe they even want to be conspicuous about it.[8]

Threats Regarding Rare Earths

Concerns about reliance on China for the processing and supply of rare earth materials are not novel. More explicit discussion from Beijing about using rare earths as leverage against Washington, however, has grown in early 2021.[9] While state-affiliated media and other "wolf warriors" were largely the source of previous chatter about rare earths in past years, the increased proximity of these discussions to Beijing foreign policy officials and economic planners suggests intense exploration of this potential leverage.

The Trump administration Department of Defense had undertaken review of rare earth supplies, and President Biden's Executive Order on supply chain resilience—covered in greater detail later in this report—specifically highlights the supply chain for rare earths as an issue of specific concern.

As previous Geotech reports have also highlighted, Japan experienced such an embargo from China in 2011, and responded with a series of state and private sector actions coordinated to find alternative sources. Rare earths are an area that can serve as an opportunity to work with allies to reduce dependence on China based on shared economic interests, security concerns, and environmental values.

Military-Civil Fusion

The CCP's efforts toward Military-Civil Fusion (MCF) are policies aimed at economic expansion, industrial base development, and technological innovation. MCF should continue to be an area of particular concern for policymakers. However, that concern should be accompanied with a thorough

---

[7] Joseph Brouwer, "Police Arrest Seven, Engage in 'Online Pursuit' to Crack Down on Online Speech." *China Digital Times*, February 25, 2021. https://chinadigitaltimes.net/2021/02/police-arrest-seven-engage-in-online-pursuit-to-crackdown-on-online-speech/

[8] Helen Davidson, "China arrests six for 'causing negative social impact' online over India border clashes." *The Guardian,* February 23, 2021. https://www.theguardian.com/world/2021/feb/23/china-arrests-six-for-causing-negative-social-impact-online-over-india-border-clashes

[9] Dan Mahaffee, "Rare Earth Saber Rattling." CSPC Friday News Roundup, February 19, 2021. https://link.medium.com/Hv5Dj10Efeb

understanding of the realities of MCF. Research by Elsa B. Kania and Lorand Laskai at the Center for a New American Security provides a through analysis of MCF.[10] A key point they note for policymakers is that while the MCF is expansive, much of it remains aspirational or just underway. Furthermore, while the policies of MCF and the rhetoric around it can appear monolithic, there are differing incentives for the various firms, actors, and officials involved. Kania and Laskai note that many Chinese companies' global ambitions could come into conflict with MCF should international perceptions shift or brand damage occur. Finally, misperceptions about the MCF may lead U.S. policymakers to emulate Beijing's policies—which may ultimately be counterproductive by limiting enterprise and innovation—while the best lesson to take from the rhetoric and emphasis on MCF Is the scope of the challenge, but the need to respond in terms of our interests and values.

Geotech and the 2022 Beijing Winter Olympics

The upcoming 2022 Beijing Winter Olympic Games loom as a likely diplomatic flashpoint given the international attention to the quadrennial international winter sports event, Beijing's emphasis on events of international prestige, and the genocide and human rights abuses perpetrated by the host nation government. Such an international stage is used for pomp and pageantry, as well as the display of new technologies, commercial tools, and sponsored products. Security and communications technologies are often showcased at Olympic events. Many Chinese telecom and technology firms are already partners for the upcoming Winter Olympics, yet have strong ties to the Chinese government and have supplied repressive technologies and tools to the regime.

Policymakers in liberal democracies should carefully consider what official recognition is provided to the games, given the genocide and human rights abuses and the likely showcasing of repressive tools and technologies.

[10] Elsa B. Kania and Lorand Lasai, "Myths and Realities of China's Military-Civil Fusion Strategy." Center for a New American Security, January 28, 2021. https://www.cnas.org/publications/reports/myths-and-realities-of-chinas-military-civil-fusion-strategy

RUSSIA: "POST-SOLARWINDS" & CYBER THREATS

While previous Geotech reports have covered China in greater detail than Russia, the current cybersecurity challenge posed by Russia—revealed by the recent SolarWinds hack—is a key Geotech concern for the Biden administration. Beyond the cybersecurity implications, SolarWinds demonstrates that supply chains for software and coding are also vulnerable, not just physical supply chains. It also is a manifestation of how Russia approaches Geotech, as well as the ramifications for U.S. and allied policy makers. Joshua Huminski, Director of the CSPC Mike Rogers Center for Intelligence and Global Affairs, provides the in-depth analysis that follows:

The Biden Administration & Russia

After four years of what could best be described as a curious public policy towards Russia under the Trump administration, it appears that the newly elected Biden administration aims for a "return to normal" in style. What the substance is in practice is unclear. Thus far, the White House has indicated an intention to re-prioritize China and Russia as the top priorities, and continue a shift begun under the Obama administration away from the Middle East. President Biden indicated as much warning, "the days of the United States rolling over in the face of Russia's aggressive actions — interfering with our election, cyber-attacks, poisoning its citizens— are over." He added, "We will not hesitate to raise the cost on Russia and defend our vital interests and our people."[11]

What this "return to normal" means in practice very much remains to be seen. For one, it should be noted that on-the-ground, the Trump administration's policies towards Russia were considerably more aggressive than that of the Obama presidency and well beyond that which was appreciated by the public or Congress at the time. The imposition of sanctions and the delivery of offensive weapons to Ukraine are two areas in which the Trump administration went beyond that of his predecessor, and are in contrast with the public narrative of an administration kowtowing to Moscow.

As for the Biden administration, his appointees, thus far, are believers in multilateralism and engagement, both of which could potent well for the future of U.S.-Russia relations. In the case of the former, President Trump's antagonism of NATO allies undermined a key tool in confronting Russia, playing into Moscow's hands. In the case of the latter, smart engagement is critical—isolation and refusing to talk is not a strategy. Even during the Cold War, the United States engaged with the Soviet Union while competing globally with Moscow.

There are, however, risks in both. NATO partners such as Germany, have their own interests and relationships with Moscow, particularly on energy, which could and have been exploited by Moscow in the past. Engagement must not be an end in and of itself—as Winston Churchill said, "meeting jaw to jaw is better than war", but without a coherent arsenal of carrots and sticks, negotiations and engagement will be little more than a diplomatic salon session.

[11] "Biden strikes tough tone on Russia in diplomatic push." *AP*, February 4, 2021. https://apnews.com/article/joe-biden-foreign-policy-jen-psaki-united-nations-101d7778c61465a279495f9c419c9a32

The Russian Geo-Technological Challenge

The ultimate threat Russia presents in terms of Geotech is not in that it offers a competing model for governance as China does. While it is true that Russia has a form of authoritarian capitalism, perhaps better described as a kleptocracy more than anything else, it is not in the business of exporting that model as Beijing seeks to do. True, Putin is motivated by a set of "orthodox, illiberal, antidemocratic, anti-Western"[12] ideas, in the words of former Ambassador Michael McFaul, and both gravitated towards and drew in supporters of this worldview, it is less a model for governance or geo-technology than an ideological motivation.

Russia does not aim to define a new international order so much as it seeks to reclaim its great power status and undermine the western liberal order led by or embodied by the United States. The more it can split Washington from its European allies, sow discord within the American democratic republic, and pursue its own interests in Europe and further afield, the better.

Moreover, the international adventurism serves two concurrent purposes for President Putin and the Kremlin. First, there is the obvious direct benefit to Russia's national security and foreign policy. A weakened and divided West is less a threat to Russia's interest than a unified, coordinated NATO or European Union. Propping up Bashar al-Assad in Syria ensures that Moscow maintains its Mediterranean port at Tartus, allows Moscow to raise the temperature and drive refugees into southern Europe, and provides a proving and training ground for Russia's military that it otherwise would not enjoy. Addressing the Munich Security Conference, President Biden rightly said, "Putin seeks to weaken European — the European project and our NATO Alliance. He wants to undermine the transatlantic unity and our resolve, because it's so much easier for the Kremlin to bully and threaten individual states than it is to negotiate with a strong and closely united transatlantic community."[13]

Second, the foreign adventurism provides the Kremlin with a means to mobilize domestic support and undermine domestic opposition. By acting aggressively internationally, it provides President Putin and the Kremlin a reason for its domestic behavior and continuation of the regime. Whereas the original social contract between Putin and the Russian public was based upon improvements in living conditions, a growing economy[14], and certainly—but to a lesser degree—external threats, the current contract is all but wholly reliant on some foreign adventurism. Again, speaking virtually to the Munich Security Conference, President Biden said as much: "the Kremlin attacks our democracies and weaponizes corruption to try to undermine our system of governance. Russian leaders want people to think that our system is more corrupt or as corrupt as theirs."[15]

---

[12] Amb. Michael McFaul, "How to Contain Putin's Russia." *Foreign Affairs*, January 19, 2021 https://www.foreignaffairs.com/articles/ukraine/2021-01-19/how-contain-putins-russia

[13] Remarks by President Biden at the 2021 Virtual Munich Security Conference, White House, February 19, 2021. https://www.whitehouse.gov/briefing-room/speeches-remarks/2021/02/19/remarks-by-president-biden-at-the-2021-virtual-munich-security-conference/

[14] Tony Barber, "Putin revamp hinges on the illusion behind Russia's social contract", *FT*, January 16, 2020. https://www.ft.com/content/eaa23f78-383c-11ea-a6d3-9a26f8c3cba4

[15] Remarks by President Biden at the 2021 Virtual Munich Security Conference

Real wages are declining as a result of Covid[16], investment in domestic infrastructure has not yet materialized or provided the expected benefits, and the population is increasingly unhappy with the Putin regime. This was very much on display with the protests following the arrest and imprisonment of Alexei Navalny, the opposition figure poisoned with Novichok by the regime. The protests were less about Navalny and more about overall dissatisfaction with the state of affairs, the economy, and the Putin government.

Hacking, Disruption, and Geotech

Given the aforementioned interests and societal conditions, cyber warfare and cyber conflict represent, perhaps, the greatest tool for Moscow—comparably cheap (when set against conventional and nuclear forces), deniable (to a degree), and hugely impactful. The structure of Russia's security services also encourages competition and infighting, which all but guarantees that each service is working to one-up the other, achieve a bigger and better breach, or demonstrate some success to appease Putin and undermine the Main Enemy (the United States and the West).

The last five years alone are replete with examples of Russia's hacking efforts in terms of preparation of the battlefield, intelligence collection, mis- and dis-information, and more. From the hack of the Democratic National Committee emails, to the Internet Research Agency's information operations against the United States (the success of which is debatable), to attempts to influence the UK's 2019 general election, to cyber-attacks against Georgia, to the successful hack of Ukraine's power grid, Russia has demonstrated a propensity and talent for cyber operations; a propensity for which was vividly on display with the SolarWinds breach, about which more follows.

The Lexicon of a Cyber Incident

It is important to recognize that the SolarWinds breach was not an attack per se. Rather, it was an intelligence-gathering effort, and a spectacularly successful one at that. Getting the lexicon correct is important if one is to understand what happened, why it matters, and what it means going forward. To confuse the incident with an act of "cyber warfare" as some have suggested, is to imply that the attack crossed some as of yet undefined threshold and, therefore, necessitates some form of kinetic or destructive attack.

Could SolarWinds have led to a destructive attack? Based on available evidence it is certainly possible. Had the hackers wished to do so they could have left behind (and indeed may well have) destructive malware that could destroy data, change information, or attack key services. That they did not is likely indicative of the nature of the breach—intelligence collection vice destructive attack. Why did they not do so? For one, it was certainly restraint on the part of the hacker and the nature of the mission itself.

[16] "Russia's Putin says real incomes to fall around 3% in 2020.", Reuters, December 17, 2020. https://www.reuters.com/article/russia-putin-wages/update-1-russias-putin-says-real-incomes-to-fall-around-3-in-2020-idUSL8N2IX2HX

Equally too, however, the ability of the United States to retaliate offered a measure of deterrence, encouraging the adversary to restrain their own behavior.

What would a destructive attack have looked like? For one, the Russians could have easily destroyed data, changed information in key databases, deleted emails, and generally sown chaos within the networks of the federal government. At a time when the government is responding to a global pandemic, the immediate confusion would have been immeasurably damaging and the long-term remediation would have consumed vast amounts of time and resources. Simply locking down the federal government's networks in a ransomware attack, given how deeply they burrowed, would have effectively paralyzed the federal government leading to immeasurable second- and third-order effects. This is well before actual destructive attacks such as that which was launched against Saudi Aramco by Iran.[17]

Commenting on the SolarWinds breach, Anne Neuberger, the Deputy National Security Adviser said, "when there is a compromise of this scope and scale, both across government and across the U.S. technology sector… It's more than a single incident of espionage. It's fundamentally of concern for the ability for this to become disruptive."[18]

At its core, this was a supply chain penetration that leveraged third-party service suppliers as opposed to a brute force penetration. Here, it is also important to note that SolarWinds was not the only vehicle for the breach. The Russians also compromised the email security firm[19], Mimecast, and a Microsoft corporate partner[20] that provided cloud-management service for multiple firms.

In the end, the Russians achieved a significant success, collecting information and data for nearly a year before being detected and exposed. The investigation and remediation of this breach will take a considerable amount of time. Nearly three-months-on from the attack and the federal government is still unsure of just how widespread the breach was and how many users were affected.

How SolarWinds Happened

How did the Russians achieve such a spectacular intelligence success? There are three key components to this attack that are worth noting. First, the Russians piggy-backed on the SolarWinds regular network update software to get behind the security measures of the agencies and companies they targeted. This use of the supply chain as a trusted vector proved to be a novel mechanism to circumvent security protocols.

---

[17] Nicole Perlroth & Clifford Krauss, "A Cyberattack in Saudi Arabia Had a Deadly Goal. Experts Fear Another Try.", New York Times, March 15, 2018. https://www.nytimes.com/2018/03/15/technology/saudi-arabia-hacks-cyberattacks.html

[18] Ellen Nakashima, "Biden administration preparing to sanction Russia for SolarWinds hacks and the poisoning of an opposition leader.", *Washington Post*, February 23, 2021. https://www.washingtonpost.com/national-security/biden-russia-sanctions-solarwinds-hacks/2021/02/23/b77039d6-71fa-11eb-85fa-e0ccb3660358_story.html

[19] Ibid

[20] Ellen Nakashima, "Russian hackers compromised Microsoft cloud customers through third party, putting emails and other data at risk.", *Washington Post*, December 24, 2020. https://www.washingtonpost.com/national-security/russia-hack-microsoft-cloud/2020/12/24/dbfaa9c6-4590-11eb-975c-d17b8815a66d_story.html

Such supply chain attacks are not a new threat. Previous hackers have attempted to make their malware appear[21] as if it were legitimately originating from Microsoft, in one case, and mimic NetSarang, a company that makes server management software, in another. The management software may well originate from a trusted vendor or supplier, but the updates pushed by that vendor could be compromised as evidenced by the SolarWinds breach.

Second, the breach used domestic, U.S. servers allowing the hackers to not only mask the hack's origin, but to use U.S.-law against itself. Whereas an attack originating from a foreign source could be detected by U.S. Cyber Command or the National Security Agency, the remit stops at the water's edge, becoming a Department of Homeland Security challenge. Given the size, scope, breadth, and depth of the attack surface, ensuring constant protection, even of the .gov domains from within the United States proved to be too significant of a challenge. Homeland Security invested billions of dollars into "Einstein" a cyber security surveillance tool for government networks, around which the Russians simply went.[22]

Finally, once onto the networks, the Russians waited, watching first to see if their penetration had been detected, but then, and more importantly, to learn what the cybersecurity protections were and what protocols existed. With this data, Moscow was able to devise follow-on measures, crafting bespoke software and exploits to ensure that they would be able to reside on the servers, hoovering up as much data and information as possible without being exposed.

The Cyber Exploit Ecosystem & Supply Chain Attacks

This breach, a spectacular success from Moscow's point of view, undoubtedly provided them with massive amounts of emails, documents, and other U.S. government information and data, with which Moscow would be better equipped to understand Washington's intentions and policies. More importantly than just that information is user credentials and passwords. With that information, Moscow would be able to access additional systems, spreading their reach, and thereby repeating the cycle. While it does not appear that the Russians were able to penetrate classified or secured networks, the damage done is nonetheless significant.

The mechanism and process by which the SolarWinds breach occurred is unlikely to stay in the proverbial box. Given the previous attempts at mimicking trusted vendors and supply chain attacks, and the success of the SolarWinds breach, this type of hack is likely to be replicated by other actors—Russian or otherwise. Indeed, this was the case with ransomware and other malware that may have started at the nation-state level, but spread to criminal enterprises and vice-versa. The ecosystem of zero-days, malware, and breaches is constantly evolving and where success is found, it is quickly replicated by other actors.

Supply chain attacks are not restricted to just regular update mechanisms and it is here that the positive effects of globalization are proving to be a vulnerability. Given the decrease in economic barriers to

---

[21] Lucian Constantin, "SolarWinds attack explained: And why it was so hard to detect", *CSO Online*, December 15, 2020. https://www.csoonline.com/article/3601508/solarwinds-supply-chain-attack-explained-why-organizations-were-not-prepared.amp.html

[22] "SolarWinds: How Russian spies hacked the Justice, State, Treasury, Energy and Commerce Departments." *CBS News: 60 Minutes*, February 14, 2021.https://www.cbsnews.com/news/solarwinds-hack-russia-cyberattack-60-minutes-2021-02-14/

entry and the resulting increase in global competitiveness, software and coding can be done from virtually anywhere with an Internet connection. While this may prove to be a boon for the bottom-line of any company, it concomitantly increases the risk that a nation-state or criminal enterprise could penetrate the software supply chain. With sub-contracting and outsourcing, the true provenance of any code becomes increasingly difficult to guarantee.

Moreover, given the linkages and connections between varying software systems, and often unforeseen interactions, just because one system is fully vetted does not mean it could not be corrupted or coopted by another. This was graphically illustrated by the 2014 Target breach[23] in which hackers managed to get into the company's payment system via a HVAC subcontractor. In that incident alone, nearly 110 million customers' credit card and personal data information was stolen, resulting in an $18.5 million settlement with 47 states and the District of Columbia (the incident cost Target at least $202 million in legal fees and other costs).[24]

The U.S. Response to SolarWinds

While the investigation remains underway, it appears that the federal government may be showing signs of a response. While the initial discovery of the breach occurred at the end of 2020, the Trump administration did not take any public action in response, something for which it was roundly criticized.

At the end of February, the Washington Post reported that the Biden administration was preparing sanctions in response to the SolarWinds breach, but also the poisoning of Russian opposition figure, Alexei Navalny. Additional measures are expected. The National Security Adviser, Jake Sullivan, said that the response "will include a mix of tools seen and unseen, and it will not simply be sanctions." He added, "we will ensure that Russia understands where the United States draws the line on this kind of activity."

While sanctions are a good way of signaling displeasure with Moscow's actions, they have resulted in very little change in Russia's behavior. Sanctions failed to evict Russia from Crimea or stanch the violence in Ukraine. Indictments and sanctions resulting from previous cyber incidents and Russia's disinformation campaign yielded no significant results. Sanctions are certainly a tool when properly applied, but they are neither a panacea for an absence of strategy, nor sufficient in their own right. Indeed, the performance of Russia's economy continued to improve (pre-Covid) even under a sanctions' regime.

[23] Chris Krebs, "Target Hackers Broke in Via HVAC Company", *Krebs on Security*, February 5, 2014. https://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/

[24] Rachel Abrams, "Target to Pay $18.5 Million to 47 States in Security Breach Settlement." New York Times, March 23, 2017. https://www.nytimes.com/2017/05/23/business/target-security-breach-settlement.html

EARLY BIDEN ADMINISTRATION APPOINTMENTS & THE GEOTECH CHALLENGE

President Biden enters office with a well-established cadre of advisors across a variety of policy areas, but in foreign policy, especially with regards to China, the initial group of advisors in the White House, State Department, and Defense Department come to office as a preexisting network. Several of them worked together in the Obama administration; many co-authored essays on Geotech themes in important publications; and they often referred to each other's' works in public statements. In the following section, CSPC Senior Advisor Michael Stecher analyzes the intellectual connections between these advisors for the best early insights into the direction that the Biden administration will pursue in Geotech. This collection of ideas can best be described as U.S. leadership of a global coalition of states that are concerned about the rise of techno-authoritarianism and can collaborate to promote free and open digital and economic realms.

In the White House, the development of a strategy on Geotech themes and the overall approach to China will largely fall on two senior advisors: Assistant to the President for National Security Affairs Jake Sullivan and Deputy Assistant to the President and Coordinator for Indo-Pacific Affairs Kurt Campbell. Both are well-known from the Obama administration, where Sullivan was Director of Policy Planning at the State Department and later National Security Advisor to Vice President Biden, and Campbell was Assistant Secretary of State for East Asian and Pacific Affairs.

These two men co-authored a long essay in *Foreign Affairs* in the September/October 2019 issue entitled "Competition Without Catastrophe: How America Can Both Challenge and Coexist with China".[25] In this essay, Sullivan and Campbell lay out their vision for a US strategy towards China that moves beyond Cold War analogies. They identify China's "fusion of mass surveillance and artificial intelligence" as a key challenge, as well as the "economic, people-to-people, and technological linkages" that connect both countries and others that "might look to Beijing for investments or for surveillance technologies, but hardly see these purchases as part of a conscious turn away from the United States."

Sullivan and Campbell advocate developing a "united front of like-minded partners" to utilize their combined market and technological power to push China towards adopting reforms that allow reciprocal treatment of firms from other countries in areas like "artificial intelligence, robotics, advanced manufacturing, and biotechnology." They also recommend using a coalition of "market democracies" to build standards "that connect Asia to Europe" in areas that are not already covered by the World Trade Organization, including state-owned enterprises and digital trade. They contrast their proposals with the way that the Trump administration was implementing its efforts against Huawei-built 5G infrastructure, noting that they were hampered by a lack of creativity and an unwillingness to coordinate with allies.

Campbell and Rush Doshi, a Director for China on the National Security Council, co-authored a post on Foreign Affairs online the week before President Biden took office entitled "How America Can Shore Up Asian Order: A Strategy for Restoring Balance and Legitimacy".[26] While framed as an application of Henry Kissinger's doctoral thesis—*A World Restored: Metternich, Castlereagh and the Problems of*

[25] https://www.foreignaffairs.com/articles/china/competition-with-china-without-catastrophe
[26] https://www.foreignaffairs.com/articles/united-states/2021-01-12/how-america-can-shore-asian-order

Peace, 1812-22—the two men identify China's threat to the economic and security order in the Indo-Pacific and the need for the United States to build a security architecture "characterized by balance [in the security realm] and openness [in the economic realm]." They propose working within existing structures like the Quad, building new ones like the United Kingdom's D-10 proposal, and not forcing countries in the region to "choose" between the United States and China. Diplomatic engagement in the Indo-Pacific will "revolve around supply chains, standards, investment regimes, and trade agreements", rather than "borders and political recognition".

Doshi expanded further on ideas for a U.S. high-tech industrial policy in his July 31, 2020 testimony before the U.S. Senate Committee on Commerce, Science, and Transportation, "The United States, China, and the Contest for the Fourth Industrial Revolution."[27] Senior Director for Technology and National Security at the National Security Council Tarun Chhabra (also an alumnus of the CSPC Presidential Fellows Program) has also contributed important works to the intellectual framework of the Biden administration. In "The China Challenge, Democracy, and U.S. Grand Strategy", a policy brief published by the Brookings Institution in February 2019, he identified a unified motivating impulse for China strategy in "China's economic statecraft, industrial planning, technology partnerships, and currency strategies: reducing dependence on the United States while maintaining others' reliance on China." This idea draws on work by Henry Farrell and Abraham Newman on "Weaponized Interdependence".[28]

In response to this, Chhabra argues, the United States must focus on protecting freedom and democracy and work both internationally and domestically to restore faith in democratic capitalism as a form of social organization. Working with partners that are also committed to those goals will allow for a broader coalition that is able to mobilize resources in infrastructure, research and development, education, development assistance, intelligence, alliances, and defense." NSC China Director Julian Gerwitz also quoted Chhabra in an edition of *Politico's* "China Watcher" newsletter on July 22, 2020 saying that "We need a technology alliance agenda [including] pooled R&D investments (such as an 'allied In-Q-Tel' focused on emerging technology that advances liberal democratic values); better coordinated industrial policy and antitrust regulation; privacy-preserving data-sharing; energetic norm-building and technological standard-setting; and tailored, coordinated technology transfer restrictions, investment controls and export controls."[29]

With regards to export controls, it is important to note that Peter Harrell[30] has assumed a key post at the National Security Council as Senior Director for International Economics and Competitiveness. As an Adjunct Senior Fellow at the Center for a New American Security, he wrote "Export Controls Are Bigger and Broader. But Are We Safer?" In this briefing, he raises questions about how export controls are targeted and whether the right questions are asked about unintended consequences:

> As the U.S. government expands its use of export controls, American policymakers must grapple with key questions about their use. Should export controls be limited to promoting national security and foreign policy objectives, or should they be a tool to

[27] https://www.brookings.edu/testimonies/the-united-states-china-and-the-contest-for-the-fourth-industrial-revolution/
[28] https://www.brookings.edu/research/the-china-challenge-democracy-and-u-s-grand-strategy/
[29] https://www.politico.com/newsletters/politico-china-watcher/2020/07/22/how-us-allies-can-confront-the-china-challenge-489863

> maintain economic preeminence? Does the growing use of export controls actually undercut U.S. competitiveness by encouraging research and development outside the United States? Are unilateral controls effective, and how can the United States engage allies to support multilateral controls? Export controls are likely to be effective only if there are clear answers to these questions to guide their use.[31]

It is also possible to see how this intellectual network is being built in the State and Defense Departments. Secretary of State Anthony Blinken is a long-time associate of President Biden and, in his confirmation hearing on January 19, Blinken described the competition "between techno-democracies and techno-autocracies" as one of the most pressing challenges facing the new administration.[32] At the time of this report writing, most other senior positions at the State Department in policymaking roles are not yet filled, though that process is underway.

Secretary Blinken has placed two notable staffers in the State Department's Policy Planning Staff. Julianne Smith was a top foreign policy advisor for President Biden during the presidential campaign. She is a noted transatlanticist with close relationships in Europe. Recently, she was the Director of the Asia Program at the German Marshall Fund. She has written on how to work with Europe on coordinated strategies on Geotech issues, including technology, trade, investment, and global governance, culminating in a report published jointly by the German Marshall Fund and the Center for a New American Security in October 2020 entitled "Charting a Transatlantic Course to Address China".[33] One of Smith's co-authors on that report, Ellison Laskowski has also accepted a position on the Policy Planning Staff.

The other notable Policy Planning Staff appointee is Mira Rapp-Hooper. Rapp-Hooper collaborated with Campbell on a piece for Foreign Affairs online in July 2020 entitled "China is Done Biding Its Time: The End of Beijing's Foreign Policy Restraint".[34] They identify how changes in the internal leadership structure of the Chinese Communist Party, combined with China's position as a major global power, have made the country more risk-acceptant and willing to use coercive tools to accomplish political goals. In response, they suggest working with allies and reengaging in international organizations as a counterbalance.

She built on this framework in a book, co-authored with Rebecca Lissner, a professor at the Naval War College, entitled *An Open World: How America Can Win the Contest for Twenty-First-Century Order*.[35] They argue that Russia and China are trying to build spheres of influence that can be closed off other powers. In order to prevent this, the United States needs to take a leadership position working with countries that are committed to openness: economic interdependence, liberal democratic political systems, and accessible global commons. This will necessarily be an effort based on partnerships—most notably with Germany and Japan—and the United States will need to incorporate non-military areas into its conception of collective security, including "technological expertise, intelligence sharing, resilience planning, and economic statecraft."

---

[31] https://www.cnas.org/publications/commentary/export-controls-are-bigger-and-broader-but-are-we-safer
[32] https://www.foreign.senate.gov/hearings/nominations-011921
[33] https://www.gmfus.org/publications/charting-transatlantic-course-address-china
[34] https://www.foreignaffairs.com/articles/china/2020-07-15/china-done-biding-its-time
[35] https://yalebooks.yale.edu/book/9780300250329/open-world

The leadership at the Department of Defense is also coming into focus. Ely Ratner was Deputy National Security Advisor to Vice President Biden during the Obama administration and is now Special Assistant to the Secretary of Defense. He co-authored an essay with Campbell that analyzed the misapprehensions under which prior policies towards China had been developed. [36] Their conclusion was that, rather than pursuing a strategy to try and contain or isolate China, the United States needs to work with allies on a positive strategy to advance shared goals in the region.

Ratner was also the lead author of a report mandated by Congress in the National Defense Authorization Act of 2019 entitled "Rising to the China Challenge: Renewing American Competitiveness in the Indo-Pacific".[37] Their recommendations fit neatly into this framework, including developing closer cooperation with like-minded partners and developing an "alliance innovation base" and enhancing U.S. diplomacy in commerce, trade, and finance. Ratner's co-authors on this report include Rush Doshi; Peter Harrell; Susanna Blume, a Defense Department appointee; and Elizabeth Rosenberg, who is currently Counselor to the Deputy Treasury Secretary.

President Biden comes to office with a group of advisors and senior officials who already have his trust and have collaborated publicly for several years to develop a Geotech strategy nested within a China strategy. This group has identified that China is a strategic rival that is trying to set the rules of the road in high technology, establish at least regional economic and military preeminence, and close off the global commons to create a sphere of influence. Countering that will require an effort by the United States that invests in domestic high-tech industry, leverages relationships with allies and like-minded states around the world, and breaks out of narrow silos of thought around containment.

[36] Kurt Campbell and Ely Ratner, "The China Reckoning: How Beijing Defied American Expectations." *Foreign Affairs,* March/April 2018. https://www.foreignaffairs.com/articles/china/2018-02-13/china-reckoning

[37] https://www.cnas.org/publications/reports/rising-to-the-china-challenge

EARLY BIDEN ADMINISTRATION ACTIONS

As its personnel have taken their places, the Biden administration has also moved quickly on Geotech issues, especially in setting their mark on U.S.-China policy and cooperation with allies and partners. The tone has been set directly from the top, as President Biden has said that China should expect "extreme competition."[38] Before taking office, the Biden administration indicated that it concurred with the outgoing Trump administration's finding of a genocide in Xinjiang, and President Biden raised Hong Kong and Xinjiang in his first call with Xi Jinping.

The most impactful early action by the Biden administration, thus far, is the February 24, 2021, Executive Order on America's Supply Chains. This will launch a review of supply chain security in semiconductors, batteries, rare earths, and pharmaceuticals. This has largely been supported by the included industries. What remains unknown is how the administration will pursue rules put in place by the Trump administration to restrict trade with China in some advanced technologies.

Finally, as the Biden administration speaks of a summit of democracies and cooperation with allies on Geotech, this analysis looks at the prospects for such cooperation and how the administration can approach allies. Outreach and partnerships with European and Indo-Pacific allies are key. The supply chain review provides an opportunity to engage allies on security these global supply chains—and build on shared experiences and interests on these economic and technological concerns. Concluding this analysis, in both traditional geopolitics and the Geotech context, the Biden administration's initial outreach to Taiwan is also of interest.

Supply Chain Executive Order

On February 24, 2021, the Biden administration issued its "Executive Order on America's Supply Chains."[39] Of immediate importance is the 100-day review launched in the key areas of semiconductors, batteries, rare earths, and pharmaceuticals. The attention to semiconductors is grounded in their strategic importance, as well as the current semiconductor shortage that has slowed goods ranging from Ford F-150s to PlayStation 5s. A range of issues has resulted in this shortage, and many have converged due to the pandemic, disruptions to trade, and various accidents and incidents.[40] Still, as CSPC Geotech reports, research, and discussions on semiconductors previously noted, the lead time for new semiconductor fabs takes years. Similarly, the attention to batteries and rare earths reflects both the strategic importance of certain minerals—lithium for batteries in addition to the other rare earths—and how China has a powerful position in those supply chains. Finally, following the COVID-19 pandemic, the attention to pharmaceuticals comes at a time when concerns have been raised about reliance on foreign suppliers for key chemicals and compounds, as well as basic medical equipment.

---

[38] "Biden: China should expect `extreme competition' from US." *AP,* February 7, 2021. https://apnews.com/article/joe-biden-xi-jinping-china-8f5158c12eed14e002bb1c094f3a048a

[39] "Executive Order on America's Supply Chains." The White House, February 24, 2021. https://www.whitehouse.gov/briefing-room/presidential-actions/2021/02/24/executive-order-on-americas-supply-chains/

[40] Bindiya Vakil and Tom Linton, "Why We're in the Midst of a Global Semiconductor Shortage." *Harvard Business Review*, February 26, 2021. https://hbr.org/2021/02/why-were-in-the-midst-of-a-global-semiconductor-shortage

While those key sectors are the most immediate concern, the Executive Order also lays the groundwork for longer-term one-year examination of America's key supply chains across a wide range of sectors: from defense to agriculture, information technology to transportation infrastructure.

The National Security Advisor and Director of the National Economic Council are the lead coordinators of this effort, reflecting the importance of this review and the longer-term institutionalization of reviewing and examining the U.S. supply chain. As these reviews are ongoing, these coordinators also have the authority to expand the supply chain reviews to cover digital technologies that might apply across the other sectors and infrastructures. Finally, looking beyond this administration and towards the further institutionalization of supply chain security review, the Executive Order lays the groundwork for future reviews, including a process for a "Quadrennial Supply Chain Review."

Indications are that key industry groups are welcoming this review, and government and private sector cooperation will be key to ensuring that this is an effective exercise to secure vital supply chains. What remains to be seen is how the administration and private sector cooperate when this supply chain review finds security concerns that may affect company bottom lines and shareholder value.

Potential Technology Restrictions

While the private sector has been complementary regarding the Executive Order on the supply chain, they are more concerned about rules that remain from the Trump administration that would give the Department of Commerce authority to restrict trade and commerce with China related to advanced technologies and information technology that is a threat to U.S. national security.[41]

Where industry objects are in terms of the broad scope of the measures, and the impact that it may have on industries that are particularly reliant on information technology supply chains that have yet to readjust to Geotech concerns. Policymakers should also be aware of the likelihood of Chinese retaliation, which, as we have seen, can include detention of executives.

Government and private sector cooperation are key to the Geotech challenge, and the application and implementation of such rules requires careful coordination to balance security and commercial interests. Thus far, the example of semiconductors—where the rules delineated between trade in largely commoditized components versus cutting-edge advanced technologies—demonstrates a model for carefully crafting trade restrictions.

Cooperation with Allies

While continuing approaches towards Beijing similar to the Trump administration, the Biden administration has placed a greater emphasis on the role that U.S. allies and partners can have in the Geotech competition. As past Geotech reports have noted, allies and partners are an advantage that the United States enjoys compared to China. That said, those allies and partners cannot be taken for

[41] John D. McKinnon, "U.S. to Impose Sweeping Rule Aimed at China Technology Threats." *The Wall Street Journal*, February 26, 2021. https://www.wsj.com/articles/u-s-to-impose-sweeping-rule-aimed-at-china-technology-threats-11614362435

granted, nor can we automatically assume that their Geotech interests will automatically align with the United States.[42]

The Biden administration has spoken of a summit of democracies, a concept designed to bring together nations beyond the traditional G-7 to discuss democratic values and shared challenges. This has been seen by many as an opportunity to further Geotech cooperation, as the idea of a "Democratic 10" or "Tech 10" grouping of nations has been bandied about. That said, a major challenge continues to be what nations would be included in such a grouping, depending on how matters of security, commercial interests, and shared values are weighed. How the group orients itself is also an outstanding question, as are matters of prioritizing securing vital networks, building resilient supply chains, protecting commercial interests, competing with Chinese firms and diplomats in the Global South, and/or advocating for human rights and shared values. At its most basic level, whether this is a one-off or the start of a new series of summits is unclear.

Where these summits might prove to be of the most utility is not at the summit itself, but in the groundwork laid before and after for continued dialogues on a range of technology policies and issues. Not every nation may want to participate in a certain aspect of this approach, or be seen to openly participate, as they risk retaliation from China. Still, despite these headwinds, there is an opportunity for the Biden administration to ensure that the United States can play a key role in leading democracies on technology issues and serving as a bridge between the transatlantic and Indo-Pacific communities.

While most attention on matters of Geotech diplomacy first looks abroad, measures at home are what will put the United States in the strongest position for both the competition with adversaries and cooperation with allies. As has been previously noted in Geotech reports, the lack of a nationwide data privacy standard means that the European Union's GDPR, as well as various state measures, become the de facto lead in terms of these important regulations and standards. While a Federal standard may draw on some of these European and state-level measures, it is important for the United States to establish its own standards reflecting our interest and values for data management and privacy. This can serve as the framework to build harmonization, compatibility, and adequacy with foreign partners—rather than leaving U.S. companies and consumers to deal with a patchwork of foreign rules and state laws.

Additionally, how the administration organizes for the Geotech challenge will be important. Beyond the roles played on domestic Geotech policy—including in each cabinet agency and sector specific agencies for various industrial sectors—these officials will increasingly interface with foreign counterparts. The State Department reorganization of the cybersecurity bureau is one measure that has been designed to address dialogue with foreign partners on these issues, yet also has some on Capitol Hill concerned about whether the reorganization and diplomatic approach to Geotech issues is properly coordinated.

As already laid out in the Supply Chain Executive Order, the National Security Advisor and Director of the National Economic Council will have a key role to play in both domestic policies and coordination with allies. How the State Department is structured and empowered to take the lead, however, in regular coordination with allies, will build on both the Trump administration's past approach, e.g. Clean

[42] On February 25, 2021, CSPC hosted a dialogue with Ambassador Daniel Sepulveda, former Deputy Assistant Secretary of State, and Steven Feldstein, Senior Fellow for Democracy, Conflict and Governance at the Carnegie Endowment, entitled "Building an Alliance of Techno-Democracies." This section is informed by that event, which can be viewed online at https://www.youtube.com/watch?v=2VMUNQ1Y1eo&t=16s

networks, and new authorities and tools to coordinate with key Geotech allies and partners. However, as the executive agencies are reoriented bureaucratically to address this challenge, the signaling from the White House of the urgency of the issues, as well as the designation at each relevant agency of a key leading individual empowered to move policy will be vital as the broader administration comes together.

In terms of direct cooperation with allies and partners, several early actions of the Biden administration are of note. Readouts from both Washington and Tokyo illustrated President Biden and Prime Minister Suga's commitment to strengthening the U.S.-Japan alliance.[43] Secretary of State Blinken's early dialogue with the Quad members was largely focused on traditional security issues and pandemic response, but the economic assault by China on Australia, India's restrictions on Chinese app companies following border clashes, and existing U.S.-Japan Geotech cooperation serve as a regional foundation for Geotech concerns.

As the Biden administration undertakes its supply chain security review, coordination with key allied partners is vital. Japan, South Korea, and the Netherlands, for example, are the technology leaders in semiconductors, while U.S. and Japanese automakers increasingly share supply chains and build partnerships for electric motors and vehicle batteries. Just as U.S. policymakers consult with allies on matters of military exercises and countering China's territorial incursions, these discussions should be accompanied by greater dialogue on supply chain security, resilience, and capacity.

The U.S. administration should look to measures already undertaken by allies as both an example for potential U.S. policies and an expression of their willingness to address the shared Geotech challenge. On rare earths, as already noted, Japan has experience dealing with Chinese embargoes in 2011. More contemporary examples of note include the effort by the Japanese Ministry of Economy, Trade, and Industry (METI) to work with Taiwan Semiconductor Manufacturing Company (TMSC) to build a packaging and testing plant in Japan.[44] Strengthening Geotech cooperation amongst Quad members, Japan's Minister of Internal Affairs and Communications Takeda Ryota signed a January 2021 Memorandum of Understanding with his counterpart in New Delhi promoting Japan-India ICT cooperation. [45]The Japanese government has also pursued policies to diversify supply chains, including ¥222.5 billion in funding for domestic- or ASEAN-based manufacturing.[46]

Of final note, beyond the traditional flashpoint in U.S.-China relations, Taiwan has taken on greater importance in terms of Geotech competition. As Taiwan has grown into one of the major powers in terms of semiconductors, particularly in manufacturing, it has become a vital lynchpin of Geotech supply chains, while its democratic ideals and culture stand in stark contrast to what the Chinese Communist Party seeks to define as Chinese history, culture, and politics.

---

[43] "Suga says he and Biden agree to strengthen U.S.-Japan alliance." *Reuters*, January 27, 2021. https://www.reuters.com/article/us-japan-usa-suga-biden/suga-says-he-and-biden-agree-to-strengthen-u-s-japan-alliance-idUSKBN29W2GL

[44] "TSMC to build advanced IC packaging, testing plant in Japan: report." *Focus Taiwan*, January 5, 2021. https://focustaiwan.tw/business/202101050014

[45] "India and Japan Sign MoU to Enhance Cooperation in the Field of ICT." Ministry of Communications, Repubic of India, January 15, 2021. https://pib.gov.in/PressReleasePage.aspx?PRID=1688812

[46] Yoshiaki Nohara, "Japan Boosts Incentives to Counter China's Factory Dominance." *Bloomberg,* February 3, 2021. https://www.bloomberg.com/news/newsletters/2021-02-03/supply-chains-latest-japan-adds-incentives-to-counter-china-inc?sref=iNToYtBt

Some in Taiwan and the United States speculated that a Biden administration would reverse Trump administration overtures to Taipei. Instead, the Biden administration has continued to strengthen ties with Taiwan while not wholly rupturing "one-China" policy. An early sign was the invitation of Taiwanese delegates to the inauguration of President Biden and Vice President Harris. In the following weeks, Taiwan has also worked with the Biden administration to address the current semiconductor shortages, though those measures have been tempered by drought on the island affecting water supplies.[47]

Taiwan's importance in Geotech supply chains, as well as its democratic example and strategic location, require U.S. and allied policymakers to approach policy to Taiwan in a manner that reflects its importance to both our national security and economic prosperity. This can complicate diplomatic matters, as engagement with Taipei draws Beijing's ire. Furthermore, as evidenced by the impact of a water supply issue, a kinetic Chinese blockade or invasion of Taiwan, or Chinese cyberattack disabling semiconductor manufacturing or supporting infrastructures, could affect supply for the United States and its allies. Policymakers will need to consider how Taiwan's security affects broader security and economic interests.

[47] "Drought hits Taiwan chip supply as Biden asks for more." *BBC News*, February 25, 2021. https://www.bbc.com/news/technology-56198269

CONCLUSION

The Biden administration has approached the Geotech challenge with purpose and alacrity. While this report has largely focused on the administration's approach and the developments in the challenge from key adversaries, there is also an opportunity for bipartisan cooperation with Congress on these issues. From securing vital networks to expanding R&D and manufacturing capacity in key technologies, there are legislative proposals designed to address U.S. Geotech vulnerabilities. At a time when American politics seems intractably divided, this growing consensus should be built upon. It will demonstrate our commitment to our values and continued innovation leadership.

The new administration has the opportunity not only to work with allies, but also with U.S. allies and partners. While the Trump administration years raised questions about U.S. reliability—and allied concerns about that may continue—the Biden administration has the opportunity to not only rededicate, but also realign our partnerships and alliances to reflect new technology challenges. The upcoming review of supply chain security presents an opportunity to not only promote domestic supply chains, but also to work with our close allies and partners who share common values and join us as innovation leaders. This dialogue, along with the extensive outreach needed to the private sector, will also require bipartisan Congressional support. Here as well, Geotech leaders on Capitol Hill have an opportunity to work with the administration and engage allied policymakers.

Many priorities will compete with Geotech for attention, particularly given the magnitude of the many other challenges the administration faces. Still, this is an opportunity to institutionalize and build rules and norms around cutting edge technologies and set the stage for future innovation leadership.