CSPC

CENTER FOR THE STUDY OF THE PRESIDENCY & CONGRESS

GEOTECH

Accelerating the Race for Innovation Leadership

January 2022

CENTER FOR THE STUDY OF THE PRESIDENCY & CONGRESS

GEOTECH: ACCELERATING THE RACE FOR INNOVATION LEADERSHIP

JANUARY 2022

The Hon. Glenn Nye
President & CEO

The Hon. Mike Rogers
David M. Abshire Chairholder

Dan Mahaffee
Senior Vice President, Director of Policy

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

Erica Ngoenha
Vice President for Programs & External Affairs

Hidetoshi Azuma
Ethan Brown
Samantha Clark
Rob Gerber
Andy Keiser
James Kitfield
Zaid Zaid
CSPC Senior Advisors & Fellows

Wes Culp
Manuka Stratta
Research Contributors

Tania Vazquez
Design & Coordination

Brian Byrne
Stella Delgado
Miles Esters
Arik Gulati
Evelyn Jimenez
Liam Miller
Sarah Naiman
Jacqueline Ruiz
Maria Ruiz del Monte
Annmarie Youtt
Researchers

Table of Contents

Executive Summary

Introduction

Throughout 2021, the first year of the Biden administration has been marked by a continued recognition of the Geotech challenge. Both in the administration and Congress, there is recognition that China is the pacing threat for national security and the main competitor in the Geotech challenge. Our understanding and realization of Russia's technological model has also grown deeper and more nuanced. As the United States and other key allies share in a greater understanding of this Geotech challenge and the impact on economic and national security, we have seen greater agreement on multilateral approaches to Geotech—and, if not agreement, at least a willingness to engage on Geotech cooperation and oppose digital authoritarianism.

This race for technology leadership is as much determined in corporate boardrooms and research laboratories as it is the chambers of Congress or the halls of the Pentagon. We have seen this reflected in policies aimed to bolster U.S. research and development and competitiveness. Policymakers' have demonstrated their leadership and support for critical technologies and crucial supply chains, while also moving to block investments and exports that serve to bolster our competitors' technological aims. Having recognized the international challenge, the strategically critical technologies, the needed investments, and what is at stake, it is now time to move rapidly to ensure continued innovation leadership.

China: The Pacing Competitor

- China's economic and Geotech model is increasingly clear. As Xi Jinping was elevated to the same level as Mao and Deng in the Chinese Communist Party's historical pantheon, his policies aim to create a China-driven, digital authoritarian model for not only Geotech but also the other various tools of national power at Beijing's disposal.

- As U.S.-China competition has intensified, the Biden administration has continued the path set by the Trump administration in further tightening export controls and investment restrictions for companies with ties to the Chinese military or intelligence services. While these export controls and other measures should be carefully applied given the complexities of the current U.S.-China economic relationship, when applied, they should be focused on key nodes of civil-military fusion for fields like artificial intelligence (AI) and 5G, as well as the critical supply chains such as semiconductors, rare earths, and biotechnology.

- When it comes to human rights abuses including the Xinjiang Uyghur genocide, the repression of Tibet, and the continued crackdown on Hong Kong, U.S. and allied

policymakers are increasingly sanctioning involved entities and pursuing measures to crackdown on goods produced by forced labor.

- The leeway once given to Hong Kong and the private sector for the sake of engagement with the global economy and China's economic development has been replaced by the greater emphasis on the state-controlled economy. What this means for policymakers and private sector leaders is a need to increasingly rethink doing business with China and the nature of the competition with China.

- Xi Jinping's goals for consolidating power are to address the economic and geopolitical challenges Beijing sees ahead. These include matters such as data management, the role of big tech, technology in society, and the civil-military fusion of strategically critical technologies' R&D and deployment.

- China is moving rapidly to create its own frameworks for data locality and security, with a focus on protecting Chinese data from foreigners while ensuring continued CCP control. For the Chinese Communist Party, the concern is not so much the gathering of the data, but who controls and sees the "data dashboards."

- Business leaders will also find themselves in the crosscurrents of their business interests in China and growing public and political pressure to respond to China's human rights abuses, provocative policies, and increasingly statist economic model.

- As China confronts Geotech policy challenges and the race for innovation leadership—as well as broader societal and global challenges—the gauntlet is thrown down for democracies to bring forth their solutions. China offers up its authoritarian answers, while pointing to deadlock and dysfunction in democracies.

Russia: Digital Sovereignty

- The Russian government approaches the world's internet with a strong instinct of apprehension and has prioritized the development of a domestic technology industry to give itself a measure of control over its segment of the internet under the guise of "digital sovereignty." Russian leadership envisions "digital sovereignty" to be the imposition of significant control over the routing of Russia's internet (Runet) to give Moscow the option of restricting the flow of information on the internet from abroad into Russia (whether that be a passive flow of information or through what Moscow sees as "massive foreign influence").

- The legal foundation of these efforts was solidified through the 2019 Sovereign Internet Law, which introduced the legal concepts of "traffic exchange points," a concept that

refers to points in physical or digital infrastructure that facilitate Runet's connection with networks beyond Russia in order to regulate them.

- Russia has been active in multilateral institutions in promoting the acceptance of its vision of an internet which can be segmented from the rest of the world by national governments as desired.

- Russia itself is increasingly reliant on the Chinese tech sector, a result of its isolation from western technology following international sanctions for Russian cyberattacks against western targets. Indeed, the invasion of Ukraine's Crimea and Donbas, precipitated by Russian cyber operations, exhibit the very behavior which substantiated the sanctions. Moscow does pursue an international policy that would foster an environment where such digital segmentation is viable.

- While Kremlin goals such as its target of 70% of government technology purchases being based on Russian-made processors by 2023 are ambitious, the Russian tech industry still struggles to achieve the requisite production scales to support such aims. The Russian technology sector itself benefits from significant support from the Russian state and state-affiliated organizations but has struggled to stand on its own internationally.

- Russia is home to several large technology companies such as Yandex and Vkontakte with services akin to Google or Facebook, but these companies have struggled to penetrate markets beyond the former Soviet Union. Others such as cybersecurity company Kaspersky Lab have been ejected from Western countries as government and corporate vendors on concerns that Kaspersky products could be used by Russian government entities for purposes of espionage.

Japan: An Ally (Re) Focusing on Geotech

- Japanese Prime Minister Fumio Kishida convened his administration's first cabinet meeting on economic security, the Economic Security Promotion Conference, on November 19, 2021. The event essentially marks the official start of Kishida's signature economic security policy which he and his party allies from Japan's ruling Liberal Democratic Party (LDP) crafted. While Kishida's economic security agenda is steadily showing tangible progress, it will be important to see how it fits into a comprehensive strategy.

- Kishida's policies build on the leadership of former LDP Secretary-General Akira Amari, who had displayed proactive leadership in charting Japan's nascent policy discourse on economic security toward targeted decoupling from China and a more resilient national economy based on strategic autonomy and strategic indispensability. Kishida inherited Amari's vision and continued to pursue his economic security policy in earnest, even expanding its scope to include human rights by appointing the former two-time defense

minister and Japan's top human rights hand, Representative Gen Nakatani as the prime minister's special adviser on human rights issues.

- Kishida's three goals for Japan's economic security: 1) improving the autonomy of Japan's economic structure, 2) securing competitive advantages of Japanese technologies with an eye toward their indispensability, and 3) maintenance and enhancement of fundamental values and a rules-based international order.

- The first reality check of Kishida's economic security agenda will likely occur at the upcoming virtual summit with the US president Joe Biden on January 21, 2022, where the two leaders could further align their respective countries' policies—either bilaterally or through a commitment via the Quad framework.

- While Tokyo's renewed commitment to revitalizing its indigenous semiconductor industry is a welcome move, its role in driving the country's overall economic security policy is still in flux.

- Emerging political undercurrents are promoting the revitalization of the Japanese semiconductor industry. The Japanese semiconductor industry once dominated 51% of the global market in the late 1980s, but it gradually fell in market share, achieving only 6% in 2020. Former U.S. president Donald Trump's trade war with China, beginning in 2017, coincided with the Japanese government paying renewed attention to the industry, laying the foundation for Tokyo's current policy focus on reviving Japan's place in the global semiconductor market.

  In June 2021, the Ministry of Economy of Economy, Trade, and Industry (METI) unveiled its Semiconductor Strategy consisting of the following: 1) Jointly developing cutting-edge semiconductor manufacturing technology and securing sufficient production capability; 2) Accelerating digital investment and strengthening the design and development of cutting-edge logic semiconductors; 3) Promoting green innovation; 4) Strengthening the portfolio of the domestic semiconductor industry and enhancing its resilience.

Democracies' Cooperation & Global Tech Coalitions

- The inaugural meeting of the U.S.-EU Trade and Technology Council (TTC) took place in Pittsburgh on September 29, 2021. The Council's mandate, established at the June 2021 U.S.-EU Summit in Brussels, addresses some of the most pressing topics facing the digital economy, including semiconductor supply chains, standards governing artificial intelligence technology, climate and environmental initiatives, and cyber security threats. The meeting established working groups tasked with continuing the dialogue until TTC's next meeting scheduled for the spring of 2022.

- The United States and the European Union share the world's largest trade relationship in digital services. And yet the U.S. and EU have been unable to agree on a lasting framework governing the transfer of user data from the EU to the United States. This places a burden on companies with customers on either side of the Atlantic, impedes the growth of the trade relationship, has implications for the competitiveness of both the United States and Europe.

- An additional point of contention between the United States and the European Union is their approach to antitrust concerns. The European Union, has led the charge in antitrust lawsuits against major U.S. tech companies. Google, Facebook, Apple and Microsoft have collectively been fined billions of dollars.

- The European Commission has proposed the Digital Services Act and the Digital Markets Act, which will set even tougher standards for tech companies doing business in EU countries when passed. The bills are designed to simultaneously expand and protect the rights of consumers while curbing the anticompetitive practices undertaken by many tech companies. The EU has largely not welcomed private sector input in these legislative initiatives. The Office of the U.S. Trade Representative and the U.S. Department of Commerce have expressed U.S. concerns about the process and potential impact of these measures.

- Solving U.S. and EU differences on data privacy and digital competition could pave the way for a Transatlantic digital trade zone that would strengthen the economic competitiveness of both the U.S. and the EU, and would help the U.S. and EU pose a united front against the digital authoritarianism that China seeks to export.

- The broad scope of subjects addressed in the latest Quad meeting indicates an interest in tightening their relationship to a level never before seen. The group is not technically an alliance, and its messages are not necessarily binding, but the released statement suggests a desire to collaborate in areas that affect geopolitical positioning in the Indo-Pacific. While the Quad never explicitly addresses China in its statements or press releases, it remains clear that countering Chinese influence in the Indo-Pacific remains a priority.

- AUKUS is a security arrangement between Australia, the United Kingdom and the United States. While the submarine aspect of the deal has received the most press coverage, AUKUS aligns Australia, the United Kingdom and the United States on a variety of technological objectives. The agreement designates long-range missiles, artificial intelligence, quantum computing and cyber technology as priorities for the three nations. The trilateral collaboration of the military industrial complexes of these countries signals a repositioning in the Indo-Pacific. As competition moves to the region, the United States is working with historical allies to make a concerted effort to meet

Chinese influence head on.

- In December 2021, the Biden administration convened a virtual Summit for Democracy. The goal of the event was to "galvanize commitments and initiatives across three principal themes: defending against authoritarianism, fighting corruption, and promoting respect for human rights." The meeting sought to synthesize a coordinated response on behalf of the democratic countries invited. Ideally, from this two-day summit future dialogues will materialize into concrete initiatives.

- During the virtual East Asia Summit in October 2021, President Biden announced that the United States would aim to develop "an Indo-Pacific economic framework." In meetings in the region in November, Secretary of Commerce Gina Raimondo indicated that the United States would seek to develop such a framework in 2022. While past and current political dynamics prevent participation in existing regional trade arrangements, how the administration approaches the Indo-Pacific Economic Framework will require a careful balancing of emphasizing the importance of competition with China and engagement with partners alongside the thorny issues of trade in U.S. domestic politics.

U.S. Efforts

- The Biden administration has continued to address supply chains, both ones related to critical technologies and broader supply chain concerns. In June of 2021, following Executive Order 14017, the Biden Administration released a report on "Building Resilient Supply Chains, Revitalizing American Manufacturing, and Fostering Broad-Based Growth." The report includes analysis from the Departments of Commerce, Energy, Defense, and Health and Human Services. Along with the executive order that established this report, it also created the Supply Chain Disruptions Task Force, which works in conjunction with the Covid Relief Task Force and industry leaders to help secure the supply chain issues that arose over the past 18 months.

- The passage of the FY21 NDAA retains Senate provisions to authorize, but not fund, $52 billion for U.S. semiconductor manufacturing. Of additional note in the bill's language, is a provision to strengthen the U.S. semiconductor supply chain by "requiring the DoD to establish a national network for microelectronics research and development, further requiring the defense department to brief congress at interval on the establishment of such a safeguard". Further, a panoply of cyber initiatives are expanded.

- In June of 2021, the Senate passed the United States Innovation and Competition Act (USICA), which "establishes a Directorate for Technology and Innovation in the National Science Foundation (NSF) and establishes various programs and activities." This would involve investing in research into artificial intelligence, computing, manufacturing, and the commercialization of tech.

- As of this report's writing, we await details on the status of that legislation and a proposed conference to reconcile differences between the House and Senate approaches. Speaker Pelosi has indicated that the House will introduce its own version of USICA. Other measures in the House of note for this conference process include: The EAGLE Act, introduced by Chairman Gregory Meeks (D-NY) of the House Foreign Affairs Committee, provided frameworks for investments in U.S. competition with China, a focus on diplomatic efforts to counter Chinese influence in regions around the world, and further measures to counter China's Belt and Road Initiative with particular focus on green technologies and the House includes H.R.2225, the National Science Foundation for the Future Act, which would focus on increasing investments into STEM research and education. If signed into law, the bill would also fund research grants and create a Research Security and Policy office to coordinate initiatives across the NSF.

5G Deployment & the Road to 6G

- 5G is a field where this challenge was recognized in the early stages of Geotech competition, yet one where important decisions still remain for the future of 5G and the path towards leadership in 6G technologies.

- On November 11, 2021, President Biden signed the bipartisan Secure Equipment Act, which bans the Federal Communications Commission (FCC) from considering products from companies, such as Huawei and ZTE, that are considered national security threats.

- Following up on the proposals and activities of the 2019 and 2020 conferences, the 2021 Prague 5G Security Conference continued discussions amongst government officials, private sector leaders, and academic experts to discuss the security of critical 5G infrastructure and its relationship to other strategically critical technologies. The conference introduced both the "Prague Proposals on Cyber Security of Emerging and Disruptive Technologies (EDT)" and the "Prague Proposals on Telecommunications Supplier Diversity". These efforts were welcomed by the Biden administration.

- While policymakers have continued to support the development and deployment of Open RAN, now is the time to accelerate efforts to test integrated Open RAN systems—where the equipment and software of different vendors can be tested in the same environment. This will further efforts to promote interoperability and vendor diversification. Vendor diversification empowers the network operators, where the leaders are in the United States, Europe, South Korea, and Japan.

- As next steps in 5G help to lay the road to 6G, it is important for U.S. policymakers to begin public-private efforts to foster and sustain U.S. 6G leadership. These efforts can also be coordinated with allies, as demonstrated by the April 2021 announcement of joint $4.5 billion investment in 6G and 5G Open RAN research, development, and testing

by President Biden and former Japanese Prime Minister Suga.

- Where Chinese Geotech firms enjoy an advantage in the developing world, a "leapfrogging" approach focused on future technologies is required to compete. The challenge is to again lead in the next generation of technologies to leapfrog the current advantage of Chinese firms. Geotech diplomacy and Geotech development assistance efforts are in their nascent stages, and will require greater engagement, resourcing, and leveraging of public-private partnerships. Multilateral efforts working with allies and partners can also provide opportunities for greater resource and burden-sharing, as well as avoiding perceptions of American domineering in regions with sensitive historical memories.

Innovation Leadership & Strengthening the Value of U.S. Intellectual Property

- In terms of the relationship between innovation leadership, economic prosperity, and national security, intellectual property protections and policies play a key role in incentivizing the next generation of strategically critical technologies by rewarding the innovators who make breakthrough advancements. As part of the Geotech competition, it is important to understand the nexus of intellectual property, innovation leadership, and national security.

- Given that revenue from intellectual property feeds R&D—and since R&D decisions are made by corporate leaders years, if not a decade, in advance—strategic, long-term, and consistent approaches to IP policy are needed.

- U.S. IP policy suffers from what former USPTO Director David Kappos describes as "cognitive dissonance", where U.S. innovation leadership in global standards is discouraged; U.S. IP is devalued; and a negative example is set for global partners and competitors. Addressing these issues, incorporating national security stakeholders in IP policy decision-making, and addressing shortcomings in the patent system related to strategic critical technologies will ensure that our IP system helps to protect our national security and economic prosperity.

- Weakening standards to which U.S. patents are held, including SEPs, encourages other countries to weaken their IP enforcement and their respect for U.S. patentholders' rights. Policies that devalue or lessen the standard to which SEPs are held discourage American innovators from participating in international standards bodies in which they are encouraged to participate for the sake of innovation leadership and national security. a holistic approach to IP policymaking—especially in strategically critical technologies—requires input from stakeholders focused on innovation leadership and national security.

- The U.S. patent system needs reforms to encourage innovation and patent making in strategically critical technologies. as China has consolidated and modified its patent policies, a resultant void in U.S. patent policymaking has allowed China to move ahead in incentives for innovation and the pool of patents for strategically critical technologies.

Recommendations:

- **Continue to Protect U.S. Innovation & Technology with Targeted Export Controls:** Cutting-edge U.S. technology should not be in the hands of the Chinese government and government-affiliated entities. That said, the continued interdependence of many supply chains at lower levels of technological sophistication requires careful application of export controls and investment restrictions.

- **Set U.S. Standards for Key Geotech Policies & Data Cooperation with Allies & Partners:** U.S. Geotech interests and national security benefit when the United States can set the standards for international Geotech policy and strategically critical technologies, but such efforts are hampered by a lack of policy or policies that disincentivize international digital commerce or standards-setting. Toward this end, 1) the adoption U.S. national data privacy legislation can replace what is currently a disjointed patchwork of state and federal laws and be paired with a creative solution to circumvent EU court objections on national security access to data; 2) policymakers should avoid any interpretations of export controls that would lead U.S. companies to believe that they cannot participate in widely-attended, transparent international forums that also include companies on the U.S. government entity list or other restrictions.

- **Better Coordinate Cooperation with Europe:** Further coordination between the U.S. Federal Trade Commission, which is responsible for anti-trust enforcement, and the European Commissioner for Competition can ensure a joint approach to modernizing regulations for digital platforms in a way that benefits citizens and the digital market on both sides of the Atlantic.

- **Build on Cooperative Agreements with Geotech Allies with Active Cooperation & Real-World Testing:** As agreements are made with partners regarding Geotech standards, investments, and broader joint approaches to Geotech competition, policymakers should support efforts to stand up real-world opportunities for cooperative technology testing and deployment. The AUKUS deal is an example of this, where immediate successes can deepen long-term defense and technology cooperation.

- **Embrace Opportunities when Allies & Partners Adjust Geotech Policies:** The examples of Australia and Japan show how allies and partners can align themselves closer to the United States when faced with China's aggressive behavior. As Japan re-emphasizes Geotech concerns under the framework of overall economic security, this is an

opportunity for the United States to engage with a key ally and deepen Geotech cooperation.

- **Craft Policies Focused on Geotech Competition in the Developing World:** As China continues to build out Geotech infrastructure and ties in the developing world, it is important for the United States and allies to provide near-term and long-term alternatives that include financing and development assistance in this area. Given the advantages already enjoyed by Chinese providers, an emphasis on leapfrogging existing Chinese tech infrastructure is necessary.

- **Accelerate efforts to promote and support interoperability testing of Open RAN technologies:** To speed the deployment of Open RAN 5G systems, interoperability testing can ensure that the software and hardware of diversified vendors work together to provide 5G network service. Where possible, policymakers should support these interoperability test beds and foster opportunities to test interoperability with allied and partner countries' companies.

- **Develop Strategies for Next Generation Technologies Such as 6G:** As both partner countries and competitors push ahead with 6G strategies and efforts to coordinate 6G research and development, the United States should develop its own similar strategies focused on 6G, as the race for leadership in that technology is already underway. These strategies can benefit from coordination with allied and partner governments and innovation leaders.

- **Apply Next Generation Technology Strategies towards Competition in Developing Countries:** Approaches focused on security and espionage concerns cannot compete with the bottom-line value of Chinese telecom build outs in the developing world. The race to provide the next generation of technologies will determine the leader in connecting the developing world and bringing even more of humanity into the digital world.

- **Avoid Weakening Standards-Essential Patents (SEPs):** Any measures that weaken the standard to which SEPs are held devalue U.S. intellectual property and discourage American innovation leaders from establishing leadership in international standards-setting bodies. Such measures disrupt the R&D ecosystem that underpins U.S. innovation leadership, while ceding leadership in international standards to competitors—harming economic and national security interests.

- **Include National Security Stakeholders in IP Policymaking:** Given that leadership in strategically critical technologies is a matter of national security, national security stakeholders from the Department of Defense, Intelligence Community, and other related entities should be included in policymaking regarding IP policy. Congressional bodies responsible for oversight of national security matters and their counterparts

overseeing intellectual property laws should also consider opportunities for joint hearings or action.

- **Reform IP Policies for Leadership in Strategically Critical Technologies:** As China has moved ahead to strengthen its patent system and align it with national goals related to strategically critical technologies, U.S. IP policy has failed to keep up with this challenge. Following the recommendation of entities including the National Security Commission on Artificial Intelligence, IP reforms should aim to encourage U.S. innovation leadership in fields such as artificial intelligence, 5G and 6G networks, and quantum computing.

Introduction

Throughout 2021, the first year of the Biden administration has been marked by a continued recognition of the Geotech challenge. The race for innovation leadership is critical to our economic prosperity and national security—and breakthroughs in strategically critical technologies such as 5G and 6G networks, artificial intelligence, and quantum computing could determine the future technological balance of power.

Both in the administration and Congress, there is recognition that China is the pacing threat for national security and the main competitor in the Geotech challenge. Our understanding and realization of Russia's technological model has also grown deeper and more nuanced. Furthermore, as the United States and other key allies share in a greater understanding of this Geotech challenge and the impact on economic and national security, we have seen greater agreement on multilateral approaches to Geotech—and, if not agreement, at least a willingness to engage on Geotech cooperation and oppose digital authoritarianism.

This race for technology leadership is as much determined in corporate boardrooms and research laboratories as it is the chambers of Congress or the halls of the Pentagon. We have seen this reflected in policies aimed to bolster U.S. research and development (R&D) and competitiveness, while also seeking to protect innovators and researchers' intellectual property from piracy or espionage. Policymakers' have demonstrated their leadership and support for critical technologies and crucial supply chains, while also moving to block investments and exports that serve to bolster our competitors' technological aims.

Having recognized the international challenge, the critical technologies, the needed investments, and what is at stake, it is now time to move rapidly to ensure continued innovation leadership. Where discussions with allies have begun, it is now time to deepen cooperation and build Geotech coalitions where possible. As key Geotech allies like Australia, Japan, the United Kingdom, and others enhance their Geotech and economic security approaches, U.S. policymakers can share best practices and coordinate measures for greater impact. Shared and multilateral approaches to Geotech must also recognize, and increasingly focus on, the competition for being the technology vendor of choice in the developing world.

With regards to strategically critical technologies themselves, simply identifying and promoting them will not win the race. With the 5G rollout and the race to 6G already underway, hastening Open RAN testing and establishing centers of gravity for U.S. 6G research and public-private partnerships are important next steps. Leadership in next generation breakthroughs will be a determinant factor in outpacing our competitors and setting future international technology standards. Here, our policies need to move with alacrity, while we need to make sure that other policies do not slow or disincentivize innovation leadership. Intellectual property policies that devalue American innovation—especially in strategically critical technologies for our national security—and discourage leadership in international standards bodies are an example of counterproductive policies that can be reversed.

The Geotech race is well underway. In some aspects of this race, we enjoy a tenuous lead, and in others, we must acknowledge the need to catch up to, or better yet, leapfrog our competitors. As our policies increasingly acknowledge the scope of the Geotech competition, they must also match its pace.

Throughout 2021, CSPC engaged with policymakers, private sector leaders, and academic experts regarding strategically critical technologies, policies to promote innovation leadership, geopolitical and strategic competition, and trends in commerce, trade, and technology. This report reflects, and respects, the off-the-record nature of these discussions, combined with open-source research and the analysis of CSPC staff, advisors, and fellows. In the updates on Geotech policy in competitors China and Russia and ally Japan, CSPC staff and fellows have lent their expertise and analysis to the work of our research team. Our analysis of legislation is not meant to be exhaustive—nor endorse legislation—but to track the progress of substantive, and likely, Geotech policymaking.

In 2021, following our March Geotech report on the early actions of the Biden administration, CSPC released two sector-specific Geotech reports. The first, in July, focused on the future of 5G technologies and the race towards 6G. In this report, we provide some further updates and recommendations regarding Open RAN testing and organizing for the already underway race for 6G leadership. The other, in October 2021, looked at the global competition for leadership in semiconductors and their manufacture. This report complements those recommendations to secure U.S. and allied cutting-edge semiconductor research and capabilities from entities affiliated with the Chinese government and military.

China: The Pacing Competitor

Through 2021, the shape of China's economic and Geotech model became increasingly clear. As Xi Jinping was elevated to the same level as Mao and Deng in the Chinese Communist Party's historical pantheon, his policies aim to create a China-driven, digital authoritarian model for not only Geotech but also the other various tools of national power at Beijing's disposal.

In many critical technologies, the policies of civil-military fusion, outlined in our previous reports, wholly dissolve the lines—which were tenuous at best—between military, intelligence agencies, the private sector, and academia. This presents challenges for U.S. and allied entities seeking to balance legitimate business and engagement with their Chinese counterparts with compliance with laws and regulations designed to protect U.S. national security and innovation leadership. At the same time, policymakers must balance these security concerns with China's deep integration into many companies' and organizations' supply chains, revenue streams, and business models.

The October 2021 report from the Georgetown University Center for Security and Emerging Technology entitled "Harnessed Lightning: How the Chinese Military is Adopting Artificial Intelligence," by Ryan Fedasiuk, Jennifer Melot, and Ben Murphy, provides an excellent analysis, via the field of artificial intelligence, to examine how the Chinese military is integrating this strategically-critical technology, how it is aided by a web of suppliers and domestic and international investments, and the gaps in U.S. export control.[1] The model identified by the Georgetown researchers is one that China applies to a range of other critical technologies.

As U.S.-China competition has intensified, the Biden administration has continued the path set by the Trump administration in further tightening export controls and investment restrictions for companies with ties to the Chinese military or intelligence services. Most recent steps have included further restrictions on major Chinese companies in the Geotech field, including: SMIC, a major Chinese semiconductor manufacturer, DJI, a drone maker, and Megvii, an AI vendor.[2]

While these export controls and other measures should be carefully applied given the complexities of the current U.S.-China economic relationship, when applied, they should be focused on key nodes of civil-military fusion for fields like artificial intelligence(AI) and 5G, as well as the critical supply chains such as semiconductors, rare earths, and biotechnology. Furthermore, when it comes to human rights abuses including the Xinjiang Uyghur genocide, the repression of Tibet, and the continued crackdown on Hong Kong, U.S. and allied policymakers are increasingly sanctioning involved entities and pursuing measures to crackdown on goods produced by forced labor.

[1] https://cset.georgetown.edu/publication/harnessed-lightning/
[2] https://www.bloomberg.com/news/articles/2021-12-15/u-s-to-add-dji-seven-other-china-firms-to-blacklist-ft-says?sref=iNToYtBt

Clampdowns & a New Economic Model

Focusing more on the economic and tech sectors, the chilling clampdown on Hong Kong and the strictly enforced guardrails for private sector leaders—i.e. where was Jack Ma?—serve as reminders for how China has changed under Xi Jinping and his consolidation of power. The leeway once given to Hong Kong and the private sector for the sake of engagement with the global economy and China's economic development has been replaced by the greater emphasis on the state-controlled economy. What this means for policymakers and private sector leaders is a need to increasingly rethink doing business with China and the nature of the competition with China.

During the heated U.S.-China trade talks during the Trump administration, one of the factors discussed among China hands was that many of the liberalizing reforms favored by Washington were also favored by more liberal, economic-development-minded factions in the Chinese Communist Party, while resisted by those who favored more state-directed models. This reflects the fundamental split within the CCP that has defined its politics — and one where reformers from Deng Xiaoping through Hu Jintao have delivered sustained economic growth (though not without major social, demographic, and environmental flaws).

In *Foreign Affairs*, Jude Blanchette brilliantly sums up the challenge Xi faces in consolidating power and addressing the economic and geopolitical challenges Beijing sees ahead:

> Yet ambition and execution are not the same thing, and Xi has now placed China on a risky trajectory, one that threatens the achievements his predecessors secured in the post-Mao era. His belief that the CCP must guide the economy and that Beijing should rein in the private sector will constrain the country's future economic growth. His demand that party cadres adhere to ideological orthodoxy and demonstrate personal loyalty to him will undermine the governance system's flexibility and competency. His emphasis on an expansive definition of national security will steer the country in a more inward and paranoid direction. His unleashing of "Wolf Warrior" nationalism will produce a more aggressive and isolated China. Finally, Xi's increasingly singular position within China's political system will forestall policy alternatives and course corrections, a problem made worse by his removal of term limits and the prospect of his indefinite rule.[3]

Understanding this dynamic in China is key to our competition with China and understanding doing business with China as the slow decoupling continues. All of our notions that Hong Kong was somehow protected because of its economic importance rest on an outdated concept of how Beijing views its interests and its exercise of power. Similarly, as it reshapes once-innovative tech and finance companies for purposes of the state, their competitive edge is blunted. As policymakers take note, and alarm, of programs like Made in China 2025 and the ties between state-owned enterprises, the Chinese military, and key research institutions. At

[3] https://www.foreignaffairs.com/articles/china/2021-06-22/xis-gamble

the same time, do not interrupt an adversary when they are in the process of making a mistake—if Beijing intends to shackle its most dynamic industries and entrepots while boosting sclerotic state-owned industries, then let them. Where this affects the competitive balance, work to achieve multilateral responses with the other industrialized economies.

Data & Capital

"A big F-U to the United States" is how one hedge fund manager described Chinese regulators' crackdown on Didi Chuxing, the "Uber of China", just days after its summer 2021 Wall Street IPO.[4] This IPO had been highly anticipated by U.S. investors eager to invest in China's tech giants—firms eager to seek capital abroad, but increasingly under stricter and stricter regulation by Beijing. Four days after Didi went public and raised $4.4 billion in the second-largest U.S. IPO by a Chinese firm, the Cyberspace Administration of China (CAC) announced an investigation into Didi's data management practices, banning the app from app stores and prohibiting new users—wiping out about $15 billion in market value from Didi's American depositary shares.

While Beijing announced plans[5] to address the loophole by which Chinese companies listed onshore could also sell shares of units incorporated overseas, the main focus of the announcements by Chinese authorities were focused on investigations related to users' data and what access to that data is given to overseas investors and regulators when listing overseas. While U.S. lawmakers talk about toughening standards on Chinese firms on U.S. exchanges, Beijing cracks down on firms looking to list abroad. Here, Beijing can hope that Hong Kong, stripped of free expression and civil liberties, can serve as the revolving door for international capital for Chinese companies—always on CCP terms.

Most attention in the United States was paid to the financial ramifications, yet the focus in Beijing is on data. These regulatory measures have come under strengthened authorities for the CAC to address privacy and national security concerns related to foreign access to Chinese data. Dave Wertime and Shen Lu at *protocol*, a China-focused tech newsletter, broke it down:[6]

> Powerful Chinese tech firms like Alibaba, Tencent and DiDi own detailed, real-time dashboards into major portions of Chinese life—from what people want and buy to what they tell their friends in private to where they're going each day. The Party wants to be sure it can see those dashboards—and that no one else outside the companies can. As Eurasia Group tech expert Xiaomeng Lu told us: "It sends a signal that Beijing is uncomfortable with Chinese tech companies' overseas

[4] https://www.cnn.com/2021/07/07/investing/china-didi-kyle-bass/index.html
[5] https://www.bloomberg.com/news/articles/2021-07-07/china-mulls-closing-loophole-used-by-tech-giants-for-u-s-ipos?sref=iNToYtBt
[6] https://www.protocol.com/newsletters/protocol-china/didi-china-tech-ipos?rebelltitem=1#rebelltitem1

> listings, particularly those that may involve data-related national security implications."

China is moving rapidly to create its own frameworks for data management and security, with a focus on protecting Chinese data from foreigners while ensuring continued CCP control. Foreign companies should expect further attention as well, as Tesla provided an example[7] of facing the ire of Beijing and state-managed Chinese social media over the data collected by its cars—and complied with data localization regulations.

For the Chinese Communist Party, the concern is not so much the gathering of the data, but who controls and sees the "data dashboards". Didi can tell Beijing much about how its citizens are traveling, while AntPay can deliver the details on their financial health. Combined with facial recognition technologies, tracking of telecom and social media communications, and other tools, Beijing is building its data-driven panopticon. Companies from overseas must meet its standards to do business in the Chinese market, while it exports the technical foundation of this to other despots, and hacks foreign networks for the other data needed to learn about overseas individuals—e.g. how the hacking of the U.S. government Office of Personnel Management and the user records of hotels and airlines can help to penetrate potential U.S. intelligence cover identities or identify other targets for Chinese espionage.

Interdependence & Decoupling

Throughout the course of CSPC's Geotech project, we have continually acknowledged the complexity of this competition, marked by deep economic interdependence with growing geopolitical and technical rivalry. The past two years have demonstrated the reliance on China for critical supply chains as many in Wall Street, Silicon Valley, and Hollywood continue to see current and future opportunity in China. While this economic interdependence may yet continue to arrest some tensions, policymakers and business leaders must also be clear eyed about the path upon which Xi Jinping and the Chinese Communist Party seek to do business and achieve dominance in critical technologies and key fields for innovation leadership.

Business leaders will also find themselves in the crosscurrents of their business interests in China and growing public and political pressure to respond to China's human rights abuses, provocative policies, and increasingly statist economic model.

Beijing's policies are reshaping how business is done with and in China, and the "China, Inc." model is being applied to strategically critical technologies, big tech companies, traditional finance and fintech, and other cutting-edge arenas ranging from green technologies—electric vehicles, wind turbines, solar—to advanced biotech and pharmaceuticals. Just as we learned with 5G networks, and understand now with other critical technologies and supply chains, the race is on, and China's Geotech paradigm and that of the United States and its allies will

[7] https://fortune.com/2021/05/26/tesla-china-data-policy-storage-sharing/

increasingly diverge—even as a range of shared commercial interests remain. Our military leadership repeatedly describes China as our pacing competitor, while our diplomats also acknowledge Beijing's seat at the table in discussions to solve many of the world's ills.

Therefore, the United States must continue to work with its allies to create policies and paradigms, for Geotech and other fields, that are shaped to out-compete the China model, rather than emulate it—or accept its rise and our decline.

Beijing's Model & the Challenge for Democracy

While there had been little doubt, in November 2021, it was made official that Xi Jinping would remain in office for a third term. Elevated to a level on par with Mao Zedong and Deng Xiaoping, the party declared under Xi's leadership, "the great rejuvenation of the Chinese nation has entered an irreversible historical process." In a dig at his predecessors, the party plenum also stated that Xi had "resolved many problems that [the party] failed to address for a long time despite intending to do so."[8]

It is important not to build China into an unstoppable giant in our imaginations, resigning ourselves to defeat by their techno-authoritarian expertise. The problems that China faces are myriad. The business headlines about the collapse of Evergrande and the slow-motion insolvency of that company are a highly visible example of the deep indebtedness of China's economy and the challenges of reorienting that nation's economy and allocation of capital. Real estate markets, economic indicators, and continuing COVID crackdowns reflect instability and uncertainty. China also faces an aging and shrinking population, and measures from the relaxation of the "one child policy" to those aimed at curbing the cost of education and childcare also reflect a desire to encourage Chinese couples to have children. At the same time, the restrictions on the education and tutoring industry have the shared goal of reducing foreign influence over Chinese students—via restrictions on foreign curricula and instructors—and the economic crackdown on the tech sector and companies listing overseas shows how Beijing is seeking to consolidate its control over corporate data, financial information, capital flows, and other arenas that we would see as traditionally commercial and business-related, yet the party increasingly sees as a matter of national security and data sovereignty.

It is not solely a matter of doing business. Social credit scores and crackdowns on video gaming by youths demonstrate how the party seeks to shape individual behavior to address perceived societal ills. Rhetoric about "common prosperity" belies a complicated mixture of the aforementioned factors, income inequality, and the transition of the Chinese economy beyond export-led growth and middle-income GDP per capita. Nationalist rhetoric and wolf warrior diplomacy about Taiwan, regional rivalries, and competition with the United States and allies reflects a desire to both distract from domestic ills, while also reflecting China's concerns about

[8] https://www.ft.com/content/77f8dd89-fd16-42f9-b2a5-0f5e9ee93ace

its influence and security. The crackdown on Hong Kong and the genocide of the Uyghurs show a party willing to do anything to stay in power.

While some of these problems and their interaction are distinctly Chinese, the fundamental challenges are not unique to China. The whole developed world faces the challenge of shrinking and aging populations, growing income inequality, and the impact of technology on the economy and society. On the global stage, insecurity and instability, the impact of climate change, the current and future pandemics, and sustainable and equitable economic development also remain shared challenges.

In China, Xi is developing a model for how these problems can be addressed, and, at the same time, this is a challenge for democracy. While China may not seek to export its model as an ideological challenger, there is a competition between these systems to show that they can deliver results and address these challenges. China's model, via Xi and the party, is one that emphasizes the role of the state in tackling these, reining in the free market and free enterprise, while also cracking down on foreign influence and those threatening the party's grip on power. While this is not an authoritarian model Beijing may seek to "export" like our Soviet adversaries in the past, they will happily facilitate and sell the tools needed for its spread. In the battle of ideas, they're happy to compete, as the announcement about Xi's appointment also called U.S. democracy a "game of the rich."

Given these globally ubiquitous challenges, the gauntlet is thrown down for democracies to bring forth their solutions. China offers up its authoritarian answers, while pointing to deadlock and dysfunction in democracies.

Russia: Digital Sovereignty

The Russian government approaches the world's internet with a strong instinct of apprehension and has prioritized the development of a domestic technology industry to give itself a measure of control over its segment of the internet under the guise of "digital sovereignty." While Russia's international export of tech products has seen significant recent growth—up from $1.4 billion of goods in 2014 to $4.5 billion in 2020—the true effort behind the Russian tech industry's growth is the Kremlin's desire to achieve self-reliance in tech production in order to support its pursuit of a sovereign internet model rather than an attempt export a cookie-cutter version of its model abroad.[9]

Russian leadership envisions "digital sovereignty" to be the imposition of significant control over the routing of Russia's internet (Runet) to give Moscow the option of restricting the flow of information on the internet from abroad into Russia (whether that be a passive flow of information or through what Moscow sees as "massive foreign influence"). This could be used in times of conflict or in more mundane cases where the Russian government simply would like to block access to a certain product or service on the internet. Russian attempts to ban (in the case of Telegram in spring 2018) or throttle (in the case of Twitter in spring 2021) were undertaken under the guise national security or crime prevention but in reality represented an attempt by the Russian government to prevent access to widely-used channels of information independent of state control.[10] The Russian government hopes to build its segment of the internet into a structure in which it can maintain a clear measure of control – one in which it can control the flow of information and determine public access to foreign web products in all circumstances.

The legal foundation of these efforts was solidified through the 2019 Sovereign Internet Law, which introduced the legal concepts of "traffic exchange points," a concept that refers to points in physical or digital infrastructure that facilitate Runet's connection with networks beyond Russia in order to regulate them.[11] The Russian government claims to have already tested a disconnected form of Runet in 2019, although the technical specifics of this test were not made publicly available.[12] In addition, a 2014 Data Localization law that prohibits the hosting of the data of Russian users outside the territory of Russia has been used to control or cut off access to websites such as Linkedin, which was prohibited by Roskomnadzor following a Moscow City

9 "Russian Tech Exports Up Threefold Since 2018." 2021. The Moscow Times. September 1, 2021. https://www.themoscowtimes.com/2021/09/01/russian-tech-exports-up-threefold-since-2018-a74950.
10 Myles-Primakoff, Dylan, and Justin Sherman. n.d. "Russia Can't Afford to Block Twitter—Yet." Foreign Policy (blog). Accessed December 16, 2021. https://foreignpolicy.com/2021/04/30/russia-block-twitter-telegram-online-censorship/.
11 О Внесении Изменений в Некоторые Законодательные Акты Российской Федерации (On Amendments to Some Legislative Acts of the Russian Federation). 2019. №608767-7. https://sozd.duma.gov.ru/bill/608767-7.
12 Wakefield, Jane. 2019. "Russia 'successfully Tests' Its Unplugged Internet." BBC News, December 24, 2019, sec. Technology. https://www.bbc.com/news/technology-50902496.

court ruling in 2016.[13] In order to develop the domestic tech industry which would be required to sustain a truly walled-off internet, the Kremlin launched the "Digital Economy" national project to much fanfare in 2017 as a modernization project on par with efforts to electrify Russia in the first half of the 20th century. However, the project has struggled to meet its goals while continuing to see its budgeted funding slashed from year to year.[14] The limits to the Kremlin's efforts to control the flow of information into Russia through the internet additionally saw its limits tested when Russia was forced to lift a multi-year ban on the encrypted messaging app Telegram in 2020.[15]

Russia has been active in multilateral institutions in promoting the acceptance of its vision of an internet which can be segmented by national governments as desired. A 2018 resolution introduced by Russia at the UN General Assembly to create an Open-ended Working Group (OEWG) on cybersecurity with a portfolio mimicking that of the existing UN Group of Governmental Experts (GGE).[16] The OEWG's foundational resolution expressly confirms that the sovereignty of the state correspondingly covers internet and other communications forms within its territory, and raises the question of what influence the Russian-led OEWG will have in shaping international internet norms as the GGE winds down its work.[17] Russia has also expressed interest in exerting influence over the work of the International Telecommunications Union (ITU) through promoting its candidate for Secretary-General and by taking the stance that national governments should take more active roles in the administration of telecommunications, including the internet.[18]

Reliance on China & State Support

Russia itself is increasingly reliant on the Chinese tech sector, a result of its isolation from western technology following international sanctions for Russian cyberattacks against western targets. Indeed, the invasion of Ukraine's Crimea and Donbas, precipitated by Russian cyber operations, exhibit the very behavior which substantiated the sanctions. Moscow does pursue an international policy that would foster an environment where such digital segmentation is viable. Russian attempts to move national governments and international bodies into the driver's seat in the international regulation of information technology and telecommunications

13 Elterman, Maria. 2017. "Why LinkedIn Was Banned in Russia." IAPP. January 23, 2017. https://iapp.org/news/a/why-linkedin-was-banned-in-russia/.
14 "Дорогая Цифровая Экономика: Триллионы На Технологическое Лидерство (An Expensive Digital Economy: Trillions Spent on Technological Leadership)." n.d. ИА REGNUM. Accessed December 2, 2021. https://regnum.ru/news/3435695.html.
15 "Russia Lifts Ban on Private Messaging App Telegram." 2020. The Independent. June 18, 2020. https://www.independent.co.uk/news/world/europe/telegram-russia-ban-lift-messaging-app-encryption-download-a9573181.html.
16 "UN GGE and OEWG." 2021. Digital Watch Observatory (blog). 2021. https://dig.watch/processes/un-gge/.
17 Developments in the Field of Information and Telecommunications in the Context of International Security. 2018. https://undocs.org/A/C.1/73/L.27/Rev.1.
18 Markovski, Veni, and Alexey Trepykhalin. 2021. "Russian Federation Internet-Related Laws and United Nations Deliberations." ICANN. https://www.icann.org/en/system/files/files/ge-007-29apr21-en.pdf.

has been steady for many years, as a 2012 resolution proposed by Russia, China, and a coalition of other authoritarian states to affirm UN regulatory control over international technology policy at the World Conference on International Telecommunications shows.[19] While Kremlin goals such as its target of 70% of government technology purchases being based on Russian-made processors by 2023 are ambitious, the Russian tech industry still struggles to achieve the requisite production scales to support such aims.[20] A close partnership has also emerged between the Russian and Chinese tech industries as Russia has become more isolated from the West, which will also complicate Russian efforts to create a wholly independent technology sector.[21]

The Russian technology sector itself benefits from significant support from the Russian state and state-affiliated organizations but has struggled to stand on its own internationally. In particular, the Kremlin has spearheaded the standing up of the "Skolkovo Innovation Center", which is marketed as being a centralized home for a variety of business and consumer technology industries. Although several large national and multinational companies such as Sberbank, Rosatom, Boeing, and Panasonic have signed onto the project near Moscow, it remains dependent on support from the Russian state for continued development and has not filled its intended role as a competitor to the United States' Silicon Valley. After the launch of the project in 2010, the Center is supported by the Skolkovo Foundation, which counts powerful Russian figures such as former President Dmitri Medvedev, First Deputy Prime Minister Andrei Belousov, and Mayor of Moscow Sergei Sobyanin as trustees, a sign of the project's privileged place in Russian policy.[22] Russia is home to several large technology companies such as Yandex and Vkontakte with services akin to Google or Facebook, but these companies have struggled to penetrate markets beyond the former Soviet Union. Others such as cybersecurity company Kaspersky Lab have been ejected from Western countries as government and corporate vendors on concerns that Kaspersky products could be used by Russian government entities for purposes of espionage.[23]

19 Lee, Timothy B. 2012. "Authoritarian Regimes Push for Larger ITU Role in DNS System." Ars Technica. December 8, 2012. https://arstechnica.com/tech-policy/2012/12/authoritarian-regimes-push-for-larger-itu-role-in-dns-system/.

20 Soldatov, Andrei. 2021. "Russia's Drive to Replace Foreign Technology Is Slowly Working." The Moscow Times. August 26, 2021. https://www.themoscowtimes.com/2021/08/26/russias-drive-to-replace-foreign-technology-is-slowly-working-a74908.

21 "The Sinicization of Russia's Cyber Sovereignty Model." n.d. Council on Foreign Relations. Accessed December 2, 2021. https://www.cfr.org/blog/sinicization-russias-cyber-sovereignty-model.

22 "Попечительский Совет [Board of Trustees, Skolkovo Foundation]." n.d. Accessed December 16, 2021. https://sk.ru/fund-skolkovo/team/board-of-trustees/.

23 Solon, Olivia. 2017. "US Government Bans Agencies from Using Kaspersky Software over Spying Fears." The Guardian, September 13, 2017, sec. Technology. https://www.theguardian.com/technology/2017/sep/13/us-government-bans-kaspersky-lab-russian-spying.

A Walled-Off Future?

Development of a domestic technology industry in Russia appears to be oriented towards the goal of serving Russia's pursuit of a sovereign internet segment which can be walled off from the outside world's internet as desired. Beyond basic supply chain considerations which have become much more acute in Russia because of sanctions imposed on Moscow following its 2014 invasion of Ukraine, Roskomnadzor's difficulties in throttling websites such as Twitter in 2021 also highlights the fact that the Kremlin does not currently have the sufficient technological expertise or know-how at its fingertips to accomplish its goal of suppressing uncontrolled flows of information as desired.[24] Russia's drive towards a sovereign internet is primarily driven by domestic considerations by the Kremlin on how it can best maintain a high degree of control over its segment of the wider internet, which will also drive Moscow's support for its domestic technology industry.

24 "Throttling Twitter Traffic in Russia Here's How Moscow's Regulators Are Doing It and Why It's Not Really Working." n.d. Meduza. Accessed December 16, 2021. https://meduza.io/en/cards/throttling-twitter-traffic-in-russia.

Japan: An Ally (Re)Focusing on Geotech

Japanese Prime Minister Fumio Kishida convened his administration's first cabinet meeting on economic security, the Economic Security Promotion Conference, on November 19, 2021.[25] The event essentially marks the official start of Kishida's signature economic security policy which he and his party allies from Japan's ruling Liberal Democratic Party (LDP), including the former LDP Secretary-General Akira Amari, gestated for several years. After Amari's untimely fall from his role as Japan's foremost economic security hand in late October, the conference showcased Kishida's operational team and consolidated the framework for his top priority agenda. It also mandated the Economic Security Minister Takayuki Kobayashi to accelerate the legislative efforts for the proposed Economic Security Promotion Act. While Kishida's economic security agenda is steadily showing tangible progress, it will be important to see how it fits into a comprehensive strategy.

Kishida's first Economic Security Promotion Conference on November 19 was his first public display of leadership on the economic security front since the October 31 general election for the House of Representatives. The general election ended with the surprising defeat of the seasoned lawmaker Amari in a single-seat district, leading to his resignation from his party Secretary-General post as well as his active involvement in Tokyo's economic security discourse. Amari's downfall was significant due to his proactive leadership in charting Japan's nascent policy discourse on economic security toward targeted decoupling from China and a more resilient national economy based on strategic autonomy and strategic indispensability. Despite this setback, Kishida inherited Amari's vision and continued to pursue his economic security policy in earnest, even expanding its scope to include human rights by appointing the former two-time defense minister and Japan's top human rights hand, Representative Gen Nakatani as the prime minister's special adviser on human rights issues. Against this backdrop, the November 19 cabinet meeting involving key ministers reaffirmed Kishida's enduring commitment to economic security and his leadership at the helm of his signature policy even in the absence of his mentor.

The event highlighted the revelation of Kishida's goals for Japan's economic security. He unveiled: 1) improving the autonomy of Japan's economic structure, 2) securing competitive advantages of Japanese technologies with an eye toward their indispensability, and 3) maintenance and enhancement of fundamental values and a rules-based international order as the three key objectives for his economic security agenda. While his pronouncements unmistakably reveal Amari's influence, the Japanese prime minister made no references to China or even cooperation with key international allies and partners, such as the US and QUAD countries. His deliberate avoidance of broader geoeconomic competitions suggests a rather narrow framework centered on restructuring Japan's existing industrial bases under the banner of economic security. Indeed, Kishida himself has been promoting "new capitalism" to replace Japan's "neoliberal economy" to fundamentally change the country's existing economic model created on the former prime minister Junichiro Koizumi's watch in the early 2000s. Indeed, the

[25] https://www.kantei.go.jp/jp/101_kishida/actions/202111/19keizaianpo.html

new Japanese prime minister unveiled his plan for a $5 billion economic security fund to support the growth of Japan's emerging technologies, such as artificial intelligence.[26]

Kishida also ordered his economic security minister to expedite the process for the legislation of the Economic Security Promotion Act. Kobayashi immediately set up the Economic Security Legislation Preparation Unit inside the Cabinet Secretariat on the same day to lead the institutional coordination across the government. According to the leaked documents obtained by Yomiuri Shimbun, the proposed legislation is slated to incorporate the following pillars: 1) bolstering supply chain resilience; 2) maintaining the functions of basic infrastructures; 3) classifying select patents; and 4) securing technological bases. While classified patents would significantly bolster Japan's overall information security, the legislation currently under discussion echoes the domestic-oriented framework for economic security unveiled by Kishida at the November 19 cabinet conference.[27]

Needing a Strategic Approach

In today's increasingly hybrid environment, Japan would benefit from working closely with allies and partners to address various economic security challenges to secure a Free and Open Indo-Pacific and beyond. Kishida's economic security strategy will most likely await the official release of an Economic Security Strategy proposed by the LDP in December 2020 and would require in-depth discourse involving both government and non-government inputs for its consolidation.[28] Given this timeline, first reality check of Kishida's economic security agenda will likely occur at the upcoming virtual summit with the US president Joe Biden on January 21, 2022, where the two leaders could further align their respective countries' policies—either bilaterally or through a commitment via the Quad framework.[29]

A Focus on Semiconductors

Japanese prime minister Fumio Kishida unveiled his vision for the future of Japan's semiconductor industry in his video message to the 2021 SEMICON held in Tokyo on December 15. Japan's top advocate for its domestic semiconductor industry, Representative Akira Amari of the ruling Liberal Democratic Party (LDP), also spoke at the event where he echoed Kishida in his support for the industry. The appearance of the two of Japan's leading economic security hands at the semiconductor conference is the culmination of recent developments surrounding the Japanese semiconductor industry and underscores the country's growing focus on its revival as the top priority for the Kishida administration's signature economic security agenda.

[26] https://www.yomiuri.co.jp/economy/20211118-OYT1T50032/
[27] https://www.yomiuri.co.jp/politics/20211113-OYT1T50277/
[28] https://www.jimin.jp/news/policy/201021.html
[29] https://www.csis.org/analysis/economic-security-shared-us-japan-priority

Kishida's recent speech was his declaration of his commitment to the resurrection of the Japanese semiconductor industry. By describing semiconductor as the core technology supporting his vision for a "new capitalism," he emphasized his latest policy initiatives, such as the legislation promoting domestic semiconductor plants for enhanced supply chain resilience and a 1.4 trillion yen (approximately 12 billion USD) investment package for the industry. Amari added by advocating an even larger investment size totaling 10 trillion yen (approximately 88 billion USD) by 2030.

In fact, their appearance is the culmination of emerging political undercurrents promoting the revitalization of the Japanese semiconductor industry. The Japanese semiconductor industry once dominated 51% of the global market in the late 1980s, but it gradually fell, achieving only 6% in 2020. Former U.S. president Donald Trump's trade war with China beginning in 2017 coincided with the Japanese government paying renewed attention to the decaying industry, laying the foundation for Tokyo's current policy focus on reviving Japan's place in the global semiconductor market.

The global coronavirus pandemic beginning in early 2020 created a supply shortage of semiconductors, leading the Japanese government to forge a consensus on the urgent need for revamping the supply chains for the country's semiconductor industry. The semiconductor crisis also coincided with the emerging policy discourse on economic security at the time. These new domestic dynamics led some of Japan's top LDP lawmakers, particularly Amari, to organize high-level political efforts to prop up the country's semiconductor industry. The upshot was the launch of the Semiconductor Caucus led by Amari and other senior lawmakers, including the former prime ministers Taro Aso and Shinzo Abe.

The Ministry of Economy, Trade, and Industry (METI) is the key ministry in charge of implementing the emerging political support for bolstering Japan's semiconductor industry. In June 2021, the Ministry of Economy of Economy, Trade, and Industry unveiled its Semiconductor Strategy consisting of the following: 1) Jointly developing cutting-edge semiconductor manufacturing technology and securing sufficient production capability; 2) Accelerating digital investment and strengthening the design and development of cutting-edge logic semiconductors; 3) Promoting green innovation; 4) Strengthening the portfolio of the domestic semiconductor industry and enhancing its resilience. One of METI's key initiatives is the construction of 3.5 billion USD factory in Kumamoto, Japan, where the Taiwanese chip manufacturer, the Taiwan Semiconductor Manufacturing Company (TSMC), will manufacture 22-28 nanometer semiconductors with additional funding from Tokyo.

Semiconductor is the core component of Kishida's economic security policy. Indeed, the efforts to revitalize the lost industry has been several years in the making. While such initiatives are positive in light of Japan's economic security, how the focus on semiconductors fits into Prime Minister Kishida's signature economic security agenda and larger strategy will be vital components of the Geotechnology competition ahead.

Democracies' Cooperation & Global Tech Coalitions

U.S.-EU Trade & Technology Council

The inaugural meeting of the U.S.-EU Trade and Technology Council (TTC) took place in Pittsburgh on September 29, 2021.

Secretary of State Antony Blinken, Secretary of Commerce Gina Raimondo and U.S. Trade Representative Katherine Tai represented the United States, while European Commission Executive Vice Presidents Margrethe Vestager and Valdis Dombrovskis led the EU delegation.

The Council's mandate, established at the June 2021 U.S.-EU Summit in Brussels, addresses some of the most pressing topics facing the digital economy, including semiconductor supply chains, standards governing artificial intelligence technology, climate and environmental initiatives, and cyber security threats. The meeting established working groups tasked with continuing the dialogue until TTC's next meeting scheduled for the spring of 2022.

The meeting in Pittsburgh also served a political purpose: to present a clear message of transatlantic unity in the face of recent challenges to the U.S.-EU relationship. The Trump administration largely shunned constructive dialogue with European partners and abandoned Transatlantic Trade and Investment Partnership negotiations, which had pursued agreement on rules for digital trade. More recently, the AUKUS nuclear submarine deal strained relations with France to the point where French leaders pressured EU officials to withdraw from the TTC. The TTC marks an intention to move past these tensions and step forward into a period of solidarity in the face of common challenges.

Underlying the substance of the Council meetings is the competition against the PRC. PRC companies have captured significant global share of the digital services and hardware market from Western competitors through a Beijing-directed strategy of government subsidies, IP theft, and domestic market trade barriers. Chinese officials have also aggressively pursued leadership of several global standards organizations, including the International Telecommunication Union, a specialized United Nations agency that manages information technologies. This allows the PRC to influence the rules of the road in their favor.

The U.S. and the EU seek to establish trade and technology standards that are rooted in free-market democratic principles they see threatened by authoritarian regimes like the PRC's.

Divergence on Privacy & Competition

The United States and the European Union share the world's largest trade relationship in digital services. And yet the U.S. and EU have been unable to agree on a lasting framework governing the transfer of user data from the EU to the United States. This places a burden on companies

with customers on either side of the Atlantic, impedes the growth of the trade relationship, has implications for the competitiveness of both the United States and Europe.

The EU's Data Protection Regulation (GDPR) imposes strict limitations on the use of EU residents' personal data with steep fines for non-compliance.[30] It also prohibits transfer of EU persons data to another jurisdiction unless the receiving country's data protection framework is deemed "adequate" by the European Commission. In 2016, U.S. and EU completed negotiation on the Privacy Shield Framework. This allowed companies that pledged to follow a set of rules for data protection to transfer EU customer data to the United States. In 2020, however, the EU Court of Justice invalidated the agreement down based on a finding that rules for U.S. government access to data for national security purposes did not adequately protect EU citizen's fundamental rights to privacy. Since then, companies have relied on cumbersome standard contractual clauses for data transfers, but even these are under scrutiny by European courts. CSPC has hosted discussions on the importance of securing a new a lasting framework for Transatlantic data transfers. The Biden Administration says that negotiations with the EU are underway on a replacement for the Privacy Shield. Success on this front will be a challenge so long as European courts continue to hold the United States to a higher standard than European governments when it comes to rules on government access to data for national security purposes. Toward this end, the adoption U.S. national data privacy legislation can replace what is currently a disjointed patchwork of state and federal laws, paired with a creative solution to circumvent EU court objections on national security access to data.

An additional point of contention between the United States and the European Union is their approach to antitrust concerns.

The European Union, has led the charge in antitrust lawsuits against major U.S. tech companies. Google, Facebook, Apple and Microsoft have collectively been fined billions of dollars.

Additionally, the European Commission has proposed the Digital Services Act and the Digital Markets Act, which will set even tougher standards for tech companies doing business in EU countries when passed.[31] The bills are designed to simultaneously expand and protect the rights of consumers while curbing the anticompetitive practices undertaken by many tech companies. The EU has largely not welcomed private sector input in these legislative initiatives. The Office of the U.S. Trade Representative and the U.S. Department of Commerce have expressed U.S. concerns about the process and potential impact of these measures. Further coordination between the U.S. Federal Trade Commission, which is responsible for anti-trust enforcement, and the European Commissioner for Competition can ensure a joint approach to modernizing regulations for digital platforms in a way that benefits citizens and the digital market on both sides of the Atlantic.

[30] http://trade.gov/european-union-data-privacy-and-protection
[31] https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package

Solving U.S. and EU differences on data privacy and digital competition could pave the way for a Transatlantic digital trade zone that would strengthen the economic competitiveness of both the U.S. and the EU, and would help the U.S. and EU pose a united front against the digital authoritarianism that China seeks to export.

A Growing Emphasis on the Quad

The Quadrilateral Security Dialogue, Quad for short, is a group of four nations: the United States, Japan, Australia and India. While the partnership does not constitute an official alliance, recent emphasis on its existence has signaled cooperation in the face of growing Chinese influence in the Indo-Pacific region.

The group was initially proposed by Japanese Prime Minister Shinzo Abe in 2007 in an effort to develop an "Asian Arc of Democracy" for countries in Central and Southeast Asia. The move was met with stark opposition on behalf of the Chinese establishment, and Australian Prime Minister Kevin Rudd pulled out of the group in 2008.

After a lengthy hiatus, President Biden hosted the leaders of the Quad in their first ever in-person meeting on September 24, 2021. The group released a joint statement that addressed a range of topics, including COVID-19, infrastructure, climate, education, cybersecurity and space.[32]

The broad scope of subjects addressed in the latest Quad meeting indicates an interest in tightening their relationship to a level never before seen. The group is not technically an alliance, and its messages are not necessarily binding, but the released statement suggests a desire to collaborate in areas that affect geopolitical positioning in the Indo-Pacific.

While the Quad never explicitly addresses China in its statements or press releases, it remains clear that countering Chinese influence in the Indo-Pacific remains a priority.

Technological Aspects of the AUKUS Deal

AUKUS is a security arrangement between Australia, the United Kingdom and the United States. The three nations agreed to a number of strategic initiatives including the manufacture of nuclear-powered submarines for the Australian Royal Navy. This will make Australia the seventh country to obtain nuclear-powered submarine capabilities.

While the submarine aspect of the deal has received the most press coverage, AUKUS aligns Australia, the United Kingdom and the United States on a variety of technological objectives. The agreement designates long-range missiles, artificial intelligence, quantum computing and cyber technology as priorities for the three nations.[33]

[32] https://www.whitehouse.gov/briefing-room/statements-releases/2021/09/24/fact-sheet-quad-leaders-summit/
[33] https://www.eastasiaforum.org/2021/09/29/aukus-is-deeper-than-just-submarines/

AUKUS represents a clear response to the growing influence and power of China, since the pact specifically addresses areas in which the United States is lagging behind. Artificial intelligence is an area the United States must develop, as evidenced by the Pentagon's chief software officer's recent resignation along with the following statement: "We have no competing chance against China in 15 to 20 years."[34]

International press coverage of the AUKUS deal focused largely on France's reaction, because Australia had previously committed to a $66 billion contract for diesel-electric submarines from a French defense contractor before entering the AUKUS agreement.

In terms of military capabilities, the French deal was inferior. The technology Australia would acquire is outdated compared to the nuclear-powered submarines the country stands to obtain under the new AUKUS deal. Whether or not the agreement was handled correctly in a foreign relations sense is another question.

The trilateral collaboration of the military industrial complexes of these countries signals a repositioning in the Indo-Pacific. As competition moves to the region, the United States is working with historical allies to make a concerted effort to meet Chinese influence head on.

Framing Geotech Efforts for the Summit for Democracy

In December 2021, the Biden administration convened a virtual Summit for Democracy. The goal of the event was to "galvanize commitments and initiatives across three principal themes: defending against authoritarianism, fighting corruption, and promoting respect for human rights."[35]

The meeting sought to synthesize a coordinated response on behalf of the democratic countries invited. Ideally, from two-day summit future dialogues will materialize into concrete initiatives. The invitation list included democratic and semi-democratic countries that span the entirety of the globe. Many of these nations are geographically situated in key strategic locations for U.S. geotechnological objectives, including the Indo-Pacific region.

In alignment with campaign promises, the Biden administration seeks to broaden its international ties by opening channels of communication and setting baseline democratic ideals to be adhered to by invited nations. The meeting is one component of a larger effort to counter growing Chinese power on the global stage.

[34] https://www.ft.com/content/f939db9a-40af-4bd1-b67d-10492535f8e0

[35] https://www.whitehouse.gov/briefing-room/statements-releases/2021/08/11/president-biden-to-convene-leaders-summit-for-democracy/

Southeast Asia has become a pressure point for the struggle between U.S. and Chinese influence. China has surpassed the United States in nations like Malaysia and Indonesia, and it stands to sway the entire region if the United States fails to rise to the challenge.

The Summit for Democracies is an opportunity for the United States to assert itself in the Indo-Pacific with countries that are swaying towards China. Beyond this meeting, the United States must leverage its alliances across the globe in order to consolidate its influence in the region. Vietnam, for example, is closely tied to South Korea, a reliable U.S. ally. Relationships like this can be leveraged to develop stronger ties in Southeast Asia.

Indo-Pacific Economic Framework

During the virtual East Asia Summit in October 2021, President Biden announced that the United States would aim to develop "an Indo-Pacific economic framework."[36] In meetings in the region in November, Secretary of Commerce Gina Raimondo indicated that the United States would seek to develop such a framework in 2022, and reiterated that the United States would not be joining the Comprehensive and Progressive Agreement for Transpacific Partnership (CPTPP)[37]—the follow on to the Transpacific Partnership (TPP) from which the Trump administration withdrew.

Moving towards such a framework recognizes the absence of a comprehensive U.S. economic approach to the transpacific region following the withdrawal from the TPP. While the Quad and the AUKUS arrangements skew towards more traditional defense and national security arrangements—albeit with significant Geotech implications—a strategic approach to trade and commerce is needed to compete with China.

While past and current political dynamics that prevent any kind of rehashing of TPP or entering CPTPP, how the administration approaches the Indo-Pacific Economic Framework will require a careful balancing of emphasizing the importance of competition with China and engagement with partners alongside the thorny issues of trade in U.S. domestic politics. Initial efforts in such an Indo-Pacific Economic Framework could focus on specific verticals or Geotech arenas, to make the framework more flexible, as Secretary Raimondo describes.[38] Such flexibility, or varying levels of participation, could make an agreement more politically viable.

[36] https://www.whitehouse.gov/briefing-room/statements-releases/2021/10/27/readout-of-president-bidens-participation-in-the-east-asia-summit/
[37] https://www.bloomberg.com/news/articles/2021-11-17/u-s-likely-to-launch-new-asia-framework-in-2022-raimondo-says?sref=iNToYtBt
[38] https://www.bloomberg.com/news/articles/2021-12-09/u-s-eyes-powerful-asia-economic-deal-in-2022-raimondo-says?sref=iNToYtBt

U.S. Efforts

The Biden Administration Supply Chain Efforts

Throughout the Covid-19 Pandemic, supply chain issues have been brought to the forefront of challenges facing the public and particular Geotech concerns. In June of 2021, following Executive Order 14017, the Biden Administration released a report on "Building Resilient Supply Chains, Revitalizing American Manufacturing, and Fostering Broad-Based Growth." The report includes analysis from the Departments of Commerce, Energy, Defense, and Health and Human Services. Along with the executive order that established this report, it also created the Supply Chain Disruptions Task Force, which works in conjunction with the Covid Relief Task Force and industry leaders to help secure the supply chain issues that arose over the past 18 months.

The supply chain review from the Department of Commerce focused on reviewing "Semiconductor Manufacturing and Advanced Packaging." In this review, the Department of Commerce examined the semiconductor supply chain from design, fabrication, assembly, etc. After examining these elements, the Department of Commerce found that the supply chain was in a fragile and precarious state that left the US open vulnerable to disruptions and obsolescence.

In addition to the comprehensive review of the state of the US and international supply chain, the Biden Administration on October 31 announced new domestic steps to address the supply chain issues exacerbated by the Covid-19 pandemic.[39] One of these responses was increasing the operating hours of the Los Angeles and Long Beach ports starting in early October.[40] Alongside this effort, the Biden administration also announced an executive order to use the National Defense Stockpile to fill in the gaps created by the reduced efficiency of the supply chain.[41] The executive order stated that "by strengthening the National Defense Stockpile, the Federal Government will both ensure that it is keeping adequate quantities of goods on hand and provide a model for the private sector, while recognizing that private sector stockpiles and reserves can differ from government ones." The Biden administration also looked internationally for its relief efforts to the issues with the supply chain, to ensure that our neighbors and allies will be able to provide mutual support. This is done through an allotment of State Department funds to other North American countries, and funding for US-ASEAN (Association of Southeast Asian Nations) trade procedures to increase efficiency and build more reliable supply connections.

[39] https://www.whitehouse.gov/briefing-room/statements-releases/2021/10/31/fact-sheet-summit-on-global-supply-chain-resilience-to-address-near-term-bottlenecks-and-tackle-long-term-challenges/
[40] https://www.whitehouse.gov/briefing-room/statements-releases/2021/10/13/fact-sheet-biden-administration-efforts-to-address-bottlenecks-at-ports-of-los-angeles-and-long-beach-moving-goods-from-ship-to-shelf/
[41] https://www.whitehouse.gov/briefing-room/presidential-actions/2021/10/31/executive-order-on-the-designation-to-exercise-authority-over-the-national-defense-stockpile/

Legislation for Geotech Competition

The passage of the FY21 NDAA retains Senate provisions to authorize, but not fund, $52 billion for U.S. semiconductor manufacturing. Of additional note in the bill's language, is a provision to strengthen the U.S. semiconductor supply chain by "requiring the DoD to establish a national network for microelectronics research and development, further requiring the defense department to brief congress at interval on the establishment of such a safeguard". Further, a panoply of cyber initiatives are expanded, including removal of duplicative IT contracts, implementing a full-sweep zero trust strategy for defense information networks, streamlining congressional reporting by the Pentagon's principal cyber advisor, and a DoD mandate to assess the impact of the Cybersecurity Maturity Model Certification (CMMC) program for small businesses, improving the cybersecurity of the defense industrial base.

In June of 2021, the Senate passed the United States Innovation and Competition Act (USICA), which "establishes a Directorate for Technology and Innovation in the National Science Foundation (NSF) and establishes various programs and activities."[42] This would involve investing in research into artificial intelligence, computing, manufacturing, and the commercialization of tech. The Office of Science and Technology Policy will also be required to write an annual strategy investigating weakness and recommending improvements for the federal government to support competition in science and national security strategy. Lastly, the bill places the Department of Commerce in charge of creating programs that would center around securing supply chain gaps.

Until recently, following the Senate passage, the U.S. Innovation and Competition Act was stalled in the House of Representatives and there was little traction in the House to get it to the floor for a vote. On November 10, 2021, nine governors called for the passage of the U.S. Innovation and Competition Act. The letter was co-signed by governors representing the states of Alabama, California, Illinois, Kansas, Kentucky, Michigan, North Carolina, Pennsylvania, and Wisconsin.[43]

In response to the lack of action by the House of Representatives, Senator Chuck Schumer attempted to push the bill through as part of the National Defense Authorization Act.[44] This proved to be an unsuccessful strategy, and the bill was blocked by Republicans who sought to pass the NDAA without USICA included.

However, the move by Schumer did lead to a discussion with House Speaker Nancy Pelosi on the passage of USICA. On November 17, in a press release, Speaker Pelosi said that "there are still a number of important unresolved issues. After Senate Republicans made it clear they would block the inclusion of USICA on the NDAA, we have decided that the best way to get an

[42] https://www.govtrack.us/congress/bills/117/s1260
[43] https://www.reuters.com/world/us/nine-governors-press-us-lawmakers-pass-semiconductor-funding-bill-2021-11-10/
[44] https://www.reuters.com/world/us/schumer-push-add-china-tech-bill-us-defense-bill-faces-hurdles-2021-11-16/

agreement will be through the conference process. Therefore, the House and Senate will immediately begin a bipartisan process of reconciling the two chambers' legislative proposals so that we can deliver a final piece of legislation to the President's desk as soon as possible."[45] It was reported on January 21, 2022, that Speaker Pelosi's "dear colleague" included details on competitiveness legislation to be shepherded by the House Science, Space, and Technology Committee.[46]

The EAGLE Act, introduced by Chairman Gregory Meeks (D-NY) of the House Foreign Affairs Committee, provided frameworks for investments in U.S. competition with China, a focus on diplomatic efforts to counter Chinese influence in regions around the world, and further measures to counter China's Belt and Road Initiative with particular focus on green technologies.

Similar legislation introduced in the House includes H.R.2225, the National Science Foundation for the Future Act, which would focus on increasing investments into STEM research and education.[47] If signed into law, the bill would also fund research grants and create a Research Security and Policy office to coordinate initiatives across the NSF.

As of this report's writing, we await details on the nature of the conference between the House and Senate on this legislation and the status of specific policy proposals and funding authorizations proposed by lawmakers.

[45] https://www.speaker.gov/newsroom/111721-1
[46] https://twitter.com/jakesherman/status/1484521104173637637?s=21
[47] https://www.congress.gov/bill/117th-congress/house-bill/2225

5G Deployment & the Road to 6G

While a range of technologies are important parts of the Geotech portfolio, 5G technologies—and the future beyond to 6G technologies—are of particular interest due to its vital importance for future connectivity. The July 2021 CSPC report "5G and beyond to 6G: Opportunities for the Biden Administration & 117th Congress" looked at current Geotech proposals with a particular focus on 5G and its future beyond to 6G.[48]

5G is a field where this challenge was recognized in the early stages of Geotech competition, yet one where important decisions still remain for the future of 5G and the path towards leadership in 6G technologies. 5G technology provides higher speed connections with lower latency and energy use. Beyond providing faster connections for smartphones, 5G has the potential to reshape entire industries and fuel economic prosperity and job growth. Even as 5G's roll out is underway—and should not be considered "finished" in any way—many are turning attention to 6G leadership, from allies in Europe and Japan to competitors in China. Fortunately, many of the actions that we can take for 5G success serve to put us on the path to 6G leadership, while many of the lessons from the 5G race can serve as guideposts for 6G policy making. What policymakers must do is work quickly, and in partnership with the private sector, to position the United States, in concert with allies, for 6G leadership.

Secure 5G Implementation Plan

In March 2020, Congress passed and President Trump signed into law, the Secure 5G and Beyond Act, which required the President to work with federal agencies to create a strategy to build lasting infrastructure for 5G and future wireless communications systems.[49] As a result of this act, the National Telecommunications and Information Administration's (NTIA) National Strategy to Secure 5G Implementation Plan was developed and released on January 6, 2021.[50] The strategy outlines four efforts central to developing 5G infrastructure.

"Line of Effort One: Facilitate Domestic 5G Rollout" describes the preemptive measures needed before implementation of the 5G infrastructure plan. This includes developing research, development, and training programs to ensure that we are prepared to meet the challenges of 5G and that future generations are equipped with the knowledge and skills to face the ever-changing telecommunications landscape. This section of the implementation plan is also designated for investigating incentives for "trusted international and domestic partner suppliers," which will promote public-private relationships across industries and secure the US's continued position as a global leader in the future of telecommunications.

[48] https://www.thepresidency.org/geotechnology-competition
[49] https://www.congress.gov/bill/116th-congress/senate-bill/893
[50] https://www.ntia.gov/5g-implementation-plan

"Line of Effort Two: Assess Risks to Identify Core Security Principles of 5G Infrastructure" outlines ways to approach the critically important security of our 5G infrastructure. The first step in the process outlined, is an evaluation of risks both domestic and abroad. Followed by identifying possible vulnerabilities to 5G infrastructure.

"Line of Effort Three: Address Risks to United States Economic and National Security during Development and Deployment of 5G Infrastructure Worldwide," will involve investigating and investing in ways to address the risks discovered in "Line of Effort Two." This will involve working with the private sector closely and build upon work already done by the Committee on Foreign Investment in the United States (CFIUS), the Federal Acquisition Security Council (FASC), and the Federal Communications Commission (FCC).

"Line of Effort Four: Promote Responsible Global Development and Deployment of 5G" will ensure that trusted allies part of mutual defense treaties also have the same high standard of communications systems and infrastructure to reduce the number of untrusted vendors entering the network. Ultimately, this will lead to secure and reliable global connectivity and support our allies in becoming leaders in 5G and future generations of wireless communications.

Securing Existing Networks

On November 11, 2021, President Biden signed the bipartisan Secure Equipment Act, which bans the Federal Communications Commission (FCC) from considering products from companies that are considered national security threats.[51] Companies such as Huawei and ZTE would both fall into this category, after they were flagged as a security threat and therefore US telecommunications companies would not be able to purchase any products from these companies using federal funds.

Another piece of proposed legislation to note is the "Understanding Cybersecurity of Mobile Networks Act" sponsored by Reps. Anna Eshoo (D-CA), Jerry McInerny (D-CA), Darren Soto (D-FL), and Adam Kinzinger (R-IL).

2021 Prague 5G Security Conference

Following up on the proposals and activities of the 2019 and 2020 conferences, the 2021 Prague 5G Security Conference continued discussions amongst government officials, private sector leaders, and academic experts to discuss the security of critical 5G infrastructure and its relationship to other strategically critical technologies. The conference introduced both the "Prague Proposals on Cyber Security of Emerging and Disruptive Technologies (EDT)" which:

[51] https://thehill.com/policy/cybersecurity/581184-biden-signs-into-law-bill-to-secure-telecommunications-systems-against?rl=1

> Draw attention to the risk profiles and threat landscape of EDTs and provide guidance which governments should consider when developing, building, deploying, managing, governing, or acquiring current and future EDTs to safeguard their citizens' data, rights, freedom and security.[52]

And the "Prague Proposals on Telecommunications Supplier Diversity":

> Which are intended to guide efforts to advance and promote supplier diversity and open and interoperable networks. Open and interoperable telecoms networks support supplier diversity, contributing to supply chain resilience and more secure, transparent, and reliable infrastructure.[53]

The continue efforts of the Prague 5G Security Conferences are a welcome forum for the discussion of 5G and other strategically critical technologies' security. National Security Council spokeswoman Emily Horne welcomed the conference in a statement:

> These Proposals highlight the vital role of governments in fostering trustworthy, secure and resilient telecommunications, that are foundational to our privacy and security online. The United States supports these Proposals, which build upon prior efforts with the G7 and the Quad and we intend to promote them in our global engagements on 5G, which is the future of internet connectivity.[54]

Moving Ahead for Open RAN & 6G Leadership

As stated by the Open RAN Policy Coalition, "The key concept of Open RAN is 'opening' the protocols and interfaces between the various subcomponents (radios, hardware and software) in the [Radio Access Network (RAN)]." Thus, moving towards Open RAN for 5G can break the stranglehold that some wireless equipment vendors have on the traditional single-vendor network architectures.

To better understand this, it is important to understand the key players: network equipment vendors—e.g. Huawei, Ericsson, Samsung—and the network operators—e.g. Verizon, AT&T, and T-Mobile (in the United States).

By allowing for a diversity of network equipment vendors for various components and software, 5G and future 6G network operators could enjoy the same diversity of vendors that is seen in in other IT fields. This represents an initial opportunity to potentially disrupt the

[52] https://www.prague5gsecurityconference.com
[53] Ibid.
[54] https://www.whitehouse.gov/briefing-room/statements-releases/2021/12/02/statement-by-nsc-spokesperson-emily-horne-on-u-s-support-for-the-third-annual-prague-5g-security-conference/

business model used by Huawei, but other U.S. and allied firms will also have to adapt to this Open RAN model as well. At the same time, open architectures provide an avenue for new market entrants and innovators to enter the 5G and 6G marketplace.

While policymakers have continued to support the development and deployment of Open RAN, now is the time to accelerate efforts to test integrated Open RAN systems—where the equipment and software of different vendors can be tested in the same environment. This will further efforts to promote interoperability and vendor diversification. Vendor diversification empowers the network operators, where the leaders are in the United States, Europe, South Korea, and Japan.

Similarly, as next steps in 5G help to lay the road to 6G, it is important for U.S. policymakers to begin public-private efforts to foster and sustain U.S. 6G leadership. These efforts can also be coordinated with allies, as demonstrated by the April 2021 announcement of joint $4.5 billion investment in 6G and 5G Open RAN research, development, and testing by President Biden and former Japanese Prime Minister Suga.[55]

One piece of legislation to note is the FUTURE Act, sponsored by Reps. Mike Doyle (D-PA), Bill Johnson (R-OH) and Lucy McBath (D-GA), instructing the FCC to establish a "6G task force."[56] At the same time, as policymakers could soon be standing up proposed National Science Foundation Technology Directorate as outlined in the US Innovation and Competitiveness Act—passed by the Senate and as of this report's writing in conference with the House—this could serve as an opportune center of gravity for public-private 6G partnerships and coordination with entities managing similar efforts in allies and partners.

Competition in the Developing World

While U.S.-China economic interdependence will remain for the foreseeable future, competition in the developing world is already underway. Many indicators suggest that China is in the lead, with an Atlantic Council Study finding that 50 percent of Africa's 3G and 70 percent of its 4G networks are built by Huawei.[57] This report noted the continued infrastructure dependence of African countries on Chinese providers and the abundance of Chinese state aid in facilitating network build outs. CSPC's assessment concurs with this report, as well, in noting that the advantages already enjoyed by Huawei require a "leapfrogging" approach focused on future technologies including satellite-based options, Open RAN 5G where possible, 6G deployment, and long-distance/undersea cable connections and nodes.

[55] https://asia.nikkei.com/Business/Telecommunication/US-and-Japan-to-invest-4.5bn-in-next-gen-6G-race-with-China
[56] https://www.congress.gov/bill/117th-congress/house-bill/4045?r=37&s=1
[57] https://www.atlanticcouncil.org/blogs/africasource/the-digital-infrastructure-imperative-in-african-markets/

China is applying the same playbook that it used to success in Africa in Latin America. In some instances, China has linked vaccine diplomacy with Huawei access—notably in Brazil.[58] Brazil is a key future marketplace for 5G and its standard influences others in Latin America. Huawei has already established itself throughout Latin America, and U.S. diplomats' efforts at vendor bans have been met with a cold shoulder. The challenge is to again lead in the next generation of technologies to leapfrog the current advantage of Chinese firms.

Geotech diplomacy and Geotech development assistance efforts are in their nascent stages, and will require greater engagement, resourcing, and leveraging of public-private partnerships. Multilateral efforts working with allies and partners can also provide opportunities for greater resource and burden-sharing, as well as avoiding perceptions of American domineering in regions with sensitive historical memories. A model from Oceana is the recently announced partnership with Australia and Japan to provide improved undersea network cable connections to a range of Pacific Island partners. This follows similar efforts by Australia to remove Huawei from planned connections to the Solomon Islands and avoid the connection of Chinese-built and operated infrastructure to Australia's core communications networks.[59]

[58] https://www.mcclatchydc.com/news/nation-world/national/national-security/article249986534.html
[59] https://www.abc.net.au/news/2021-12-12/new-undersea-cable-internet-pacific-australia-us-japan/100694212

Innovation Leadership & Strengthening the Value of U.S. Intellectual Property

In terms of the relationship between innovation leadership, economic prosperity, and national security, intellectual property protections and policies play a key role in incentivizing the next generation of strategically critical technologies by rewarding the innovators who make breakthrough advancements. As part of the Geotech competition, it is important to understand the nexus of intellectual property, innovation leadership, and national security.

The relationship between intellectual property and national security is as old as the Republic itself, as the Founding Fathers saw fit to enumerate both clear responsibilities for the nation's defense and the establishment of patents and the basis of intellectual property protections. As we find ourselves in a heated Geotech competition, IP policies underpin our innovation ecosystem and the R&D of market-based innovation leaders—many of which are U.S.-based—via the revenues derived from their IP and its licensing. Given that revenue from intellectual property feeds R&D—and since R&D decisions are made by corporate leaders years, if not a decade, in advance—strategic, long-term, and consistent approaches to IP policy are needed.

In discussions with current and former policymakers and private sector innovation leaders, CSPC Geotech research has identified areas where U.S. IP policy suffers from what former USPTO Director David Kappos describes as "cognitive dissonance", where U.S. innovation leadership in global standards is discouraged; U.S. IP is devalued; and a negative example is set for global partners and competitors.[60] Addressing these issues, incorporating national security stakeholders in IP policy decision-making, and addressing shortcomings in the patent system related to strategic critical technologies will ensure that our IP system helps to protect our national security and economic prosperity.

Standards-Essential Patents

As previous reports from the CSPC Geotech project have noted, leadership in international standards forums is vital to U.S. innovation leadership, and, resultantly, U.S. national security. This is particularly the case in standards related to telecom and wireless technologies, where the intellectual property of American innovation leaders is licensed to manufacturers and other equipment integrators via standards-essential patents (SEPs). This licensing revenue funds that R&D—notably the talent: engineers, researchers, and scientists—and as innovators seek to make long-term plans, policies that devalue SEPs devalue a critical area of American intellectual property.

Furthermore, on one hand, the Biden administration and other policymakers acknowledge the importance of participation and leadership in international standards bodies. On the other

[60] https://www.youtube.com/watch?v=BT22qJCh5yA

hand, measures and policies that devalue or lessen the standard to which SEPs are held discourage American innovators from participating in those very bodies in which they are encouraged to participate. While some may focus on these patents through the focus of antitrust concerns, a holistic approach to IP policymaking—especially in strategically critical technologies—requires input from stakeholders focused on innovation leadership and national security.

Finally, weakening standards to which U.S. patents are held, including SEPs, encourages other countries to weaken their IP enforcement and their respect for U.S. patentholders' rights. This message contradicts other efforts to promote IP enforcement and protection standards, as well as the efforts to stop, prosecute, and penalize IP pirates and industrial espionage.

Incorporating National Security in IP Policymaking

Technologies like 5G and 6G, artificial intelligence, quantum computing and other strategically critical technologies are vital to national security—policymakers and private sector leaders have recognized this over the past several years, and an increasing number of stakeholders are involved in the relationship of technology, innovation, and national security. Throughout the CSPC Geotech project and its research, recommendations have repeatedly highlighted the need for coordination of various stakeholders in government with perspectives on national security, foreign policy, regulatory matters, and innovation leadership.

IP policymaking is one such area that requires the inputs of various stakeholders, especially in areas closely related to these strategically critical technologies and international leadership in those fields, including SEPs. Those with perspectives related to the application of critical technologies to national security, including those in the Defense Department and Intelligence Community should be considered when considering changes in IP policy and the creation, ideally, of long-term, consistent IP policy.

Furthermore, the U.S. patent system needs reforms to encourage innovation and patent making in strategically critical technologies. As stated by the 2021 final report of the National Security Commission on Artificial Intelligence:

> The United States must recognize IP policy as a national security priority critical for preserving America's leadership in AI and emerging technologies. This is especially important in light of China's efforts to leverage and exploit IP policies. The United States lacks the comprehensive IP policies it needs for the AI era and is hindered by legal uncertainties in current U.S. patent eligibility and patentability doctrine. The U.S. government needs a plan to reform IP policies and regimes in ways that are designed to further national security priorities.[61]

[61] https://www.nscai.gov/wp-content/uploads/2021/03/Full-Report-Digital-1.pdf

The Commission's report notes that as China has consolidated and modified its patent policies, a resultant void in U.S. patent policymaking has allowed China to move ahead in incentives for innovation and the pool of patents for strategically critical technologies. The absence of coordination or a strategic policymaking approach for these technologies and their intellectual property allows China to set standards and establish leadership on the Geotech stage.

Conclusion & Recommendations

There are opportunities to be seized as policymakers and private sector leaders increasingly focus on Geotech competition and its impact on our economic prosperity and national security. Recognizing the importance of strategically critical technologies is the first step, but then it must be accompanied by actions designed to foster innovation leadership, value our intellectual property, and build global coalitions to set tech standards.

Working with allies, we must be clear-eyed about how the broader "China, Inc." model is applied to technologies important to national security, as well as other fields where leadership is seen as critical to China's strategic interests. This approach must also acknowledge deep interdependence between China and the global economy, as well as the trends pushing decoupling—both wholesale and in specific fields.

The bipartisan consensus surrounding Geotech is also an opportunity to make significant investments in public-private partnerships and set markers for leadership in technology standards that reflects our values and those of our allies and partners. Given how our Geotech adversaries seek to exploit and deepen political divides within our countries—as well as the incentives within our politics themselves—we cannot take for granted the political consensus surrounding Geotech policymaking.

These recommendations reflect the need to move ahead with strategy-making and investments in strategically critical technologies and to do so with speed and purpose reflecting the gravity of this competition.

- **Continue to Protect U.S. Innovation & Technology with Targeted Export Controls:** Cutting-edge U.S. technology should not be in the hands of the Chinese government and government-affiliated entities. That said, the continued interdependence of many supply chains at lower levels of technological sophistication requires careful application of export controls and investment restrictions.

- **Set U.S. Standards for Key Geotech Policies & Data Cooperation with Allies & Partners:** U.S. Geotech interests and national security benefit when the United States can set the standards for international Geotech policy and strategically critical technologies, but such efforts are hampered by a lack of policy or policies that disincentivize international digital commerce or standards-setting. Toward this end, 1) the adoption U.S. national data privacy legislation can replace what is currently a disjointed patchwork of state and federal laws and be paired with a creative solution to circumvent EU court objections on national security access to data; 2) policymakers should avoid any interpretations of export controls that would lead U.S. companies to believe that they cannot participate in widely-attended, transparent international forums that also include companies on the U.S. government entity list or other restrictions.

- **Better Coordinate Cooperation with Europe:** Further coordination between the U.S. Federal Trade Commission, which is responsible for anti-trust enforcement, and the European Commissioner for Competition can ensure a joint approach to modernizing regulations for digital platforms in a way that benefits citizens and the digital market on both sides of the Atlantic.

- **Build on Cooperative Agreements with Geotech Allies with Active Cooperation & Real-World Testing:** As agreements are made with partners regarding Geotech standards, investments, and broader joint approaches to Geotech competition, policymakers should support efforts to stand up real-world opportunities for cooperative technology testing and deployment. The AUKUS deal is an example of this, where immediate successes can deepen long-term defense and technology cooperation.

- **Embrace Opportunities when Allies & Partners Adjust Geotech Policies:** The examples of Australia and Japan show how allies and partners can align themselves closer to the United States when faced with China's aggressive behavior. As Japan re-emphasizes Geotech concerns under the framework of overall economic security, this is an opportunity for the United States to engage with a key ally and deepen Geotech cooperation.

- **Craft Policies Focused on Geotech Competition in the Developing World:** As China continues to build out Geotech infrastructure and ties in the developing world, it is important for the United States and allies to provide near-term and long-term alternatives that include financing and development assistance in this area. Given the advantages already enjoyed by Chinese providers, an emphasis on leapfrogging existing Chinese tech infrastructure is necessary.

- **Accelerate efforts to promote and support interoperability testing of Open RAN technologies:** To speed the deployment of Open RAN 5G systems, interoperability testing can ensure that the software and hardware of diversified vendors work together to provide 5G network service. Where possible, policymakers should support these interoperability test beds and foster opportunities to test interoperability with allied and partner countries' companies.

- **Develop Strategies for Next Generation Technologies Such as 6G:** As both partner countries and competitors push ahead with 6G strategies and efforts to coordinate 6G research and development, the United States should develop its own similar strategies focused on 6G, as the race for leadership in that technology is already underway. These strategies can benefit from coordination with allied and partner governments and innovation leaders.

- **Apply Next Generation Technology Strategies towards Competition in Developing Countries:** Approaches focused on security and espionage concerns cannot compete with the bottom-line value of Chinese telecom build outs in the developing world. The race to provide the next generation of technologies will determine the leader in connecting the developing world and bringing even more of humanity into the digital world.

- **Avoid Weakening Standards-Essential Patents (SEPs):** Any measures that weaken the standard to which SEPs are held devalue U.S. intellectual property and discourage American innovation leaders from establishing leadership in international standards-setting bodies. Such measures disrupt the R&D ecosystem that underpins U.S. innovation leadership, while ceding leadership in international standards to competitors—harming economic and national security interests.

- **Include National Security Stakeholders in IP Policymaking:** Given that leadership in strategically critical technologies is a matter of national security, national security stakeholders from the Department of Defense, Intelligence Community, and other related entities should be included in policymaking regarding IP policy. Congressional bodies responsible for oversight of national security matters and their counterparts overseeing intellectual property laws should also consider opportunities for joint hearings or action.

- **Reform IP Policies for Leadership in Strategically Critical Technologies:** As China has moved ahead to strengthen its patent system and align it with national goals related to strategically critical technologies, U.S. IP policy has failed to keep up with this challenge. Following the recommendation of entities including the National Security Commission on Artificial Intelligence, IP reforms should aim to encourage U.S. innovation leadership in fields such as artificial intelligence, 5G and 6G networks, and quantum computing.