HARVARD Kennedy School
BELFER CENTER
for Science and International Affairs

BRIEF
belfercenter.org/project/cyber-project

AP Photo/Ng Han Guan, File

CYBER PROJECT | MARCH 2022

The U.S.-China Tech Rivalry: Don't Decouple – Diversify

Alexa Lee

The U.S. is grappling with increasingly challenging transnational technology, policy, and security issues, which are complicated further by the economic and supply chain relationships with China. As the Biden administration and Congress look at developing policy solutions that will both reduce dependence on China and strengthen the United States' resilience, it is important that these policies form a larger, holistic strategy that articulates the national security narrative clearly.

The Chinese government's unfair international trade practices, malicious cyber activities, and intellectual property theft record are all problematic to U.S. national security, and policymakers have an imperative to address these issues. However, some American policy debates oversimplify these issues with broad policy measures in response to these complex topics—as

technological and economic decoupling with China accelerates. These policies are well-meaning, and while decoupling thus far has been relatively piecemeal, the U.S. should be judicious in its policy actions and consider long-term interests. Moreover, these policies must form a holistic strategy informed by a clear and consistent national security narrative, considerations on foreign availability, and the consequences for shaping global standards.

The economic and supply chain ties with China indeed raise challenging national security questions, but at the same time, the U.S. should not aim for decoupling broadly with China without ensuring its private sector can remain competitive on the global stage. To balance national security and economic interests, the U.S. must use narrow, objective, and consistent national security frameworks that focus on the most critical risks. It is also imperative for the U.S. to focus on strengthening its own technology leadership by investing in critical and emerging technologies, protecting key values and privacy, and collaborating with global partners and allies to advance U.S. competitiveness and national security.

Why Untargeted Technology Decoupling Would Not Work

The U.S.-China technology supply chain has been interconnected for decades, including in the design and manufacturing of hardware, software, and digital services. However, rising geopolitical conflict against the backdrop of competing values systems between the U.S. and China have put Chinese technology under scrutiny because of its use in espionage, theft, surveillance, and export of authoritarian values—which result in unfair economic gains and could culminate in nondemocratic, global tech dominance.[1] While there have been several efforts to unravel U.S.-China technology interdependence,[2] the key turning point was the commercial actions by the U.S. against the Chinese technology giant Huawei in May 2019.[3] The U.S. Commerce Department added Huawei and its 114 overseas affiliates to the Entity List and amended the foreign direct product rule to restrict Huawei's acquisition of semiconductor technology. In doing so, it leveraged export controls linked to U.S.-regulated intellectual property to compel firms to dramatically alter their ties with Huawei—a huge buyer of semiconductors for products ranging from 5G infrastructure to smartphones.

1 National Security Commission on Artificial Intelligence. "Final Report. National Security Commission on AI." National Security Commission on Artificial Intelligence, March 2021.

2 Yan Luo, Samm Sacks, Naomi Wilson, and Abigail Coplin. "Mapping U.S.-China Technology Decoupling." *DigiChina*, 27 August 2020.

3 Bureau of Industry and Security, Commerce. "Addition of Entities to the Entity List." *Federal Register*, 21 May 2019.

In the near-term, the U.S. government's actions against Huawei may have impacted its core mobile phone business abroad.[4] From a strategic perspective, however, continued actions to disentangle the supply chains may lead to bifurcating technology ecosystems for U.S. and China in a way that may not be in the best interests of the U.S. or the world. Ultimately, untargeted decoupling would not be successful in combating China's tech dominance agenda if the U.S. restrains itself from competition, access to critical markets, and development of international standards. Below, I offer three considerations for why broad-brush technology decoupling would not work, including: foreign availability and competition in the private sector, lack of clear and consistent national security narrative, and decreased opportunities for competition and shaping international standards. Later, I provide recommendations for the U.S. policy community to consider in shaping broader policy.

Foreign Availability and Competition in the Private Sector

In an environment in which China is determined to pursue indigenous innovation and self-reliance in technology, it is imperative that the U.S. address China's unfair trade practices to ensure China's innovation mercantilist techniques do not pose a threat to the U.S. economy, particularly advanced industries and the global economic and trade system.[5] However, the strategy and policy tools should ensure that the private sector remains competitive on the global stage. Simply put, we should not allow Chinese companies to export their technologies globally without playing by economic rules, while the U.S. companies walk a tightrope of decreased market share and increased legal and regulatory challenges in doing business around the world. In the U.S.-China decoupling debate, one important issue that the U.S. often overlooks is foreign availability. As the U.S. government considers policy options to combat Chinese aggression, U.S. companies often find themselves hand-cuffed by increased domestic regulatory uncertainties, while Chinese companies are gaining ground in global markets, often through unfair competition practices. Moreover, to do business in China U.S. companies face forced intellectual property and technology transfer and data localization policies that severely hamper the ability to compete without much recourse.

Any unilateral restriction to conduct businesses with Chinese entities without assessing multilateral export controls simply means handing U.S. leadership and market share over to competitors, including to Chinese companies. The Trump administration's plans to discourage other countries from engaging with Chinese technology companies often demonstrated this reality, as restrictions hindered U.S. companies from competing, while European, Asian, and even Chinese companies

4 Gordon Corera. "Huawei's Business Damaged by U.S. Sanctions Despite Success at Home." BBC, 31 March 2021.

5 Robert Atkinson, Nigel Cory, and Stephen Ezell. "Stopping China's Mercantilism: A Doctrine of Constructive, Alliance-Backed Confrontation." Information Technology and Innovation Foundation (ITIF), March 2017.

filled the gap.[6] Furthermore, policies that decrease a company's global sales eliminate a major funding stream for foundational research and development (R&D) that is vital to maintaining leadership in technology segments. For example, the ongoing Section 301 tariffs impose significant economic costs on many ICT products and components, which decreases available R&D funding. The ability for U.S. companies to profit from the global marketplace is also critical to finance investments in emerging technologies, such as AI, 5G, and quantum computing. Preventing sales to any overseas markets without making the national security nexus clear, including China, would undercut U.S. companies' abilities to innovate at a time when the U.S. needs it most.

Decreased Opportunities for Shaping International Technical Standards

The U.S. private sector has long been a leader and major contributor in shaping international standards for ICT technologies. The industry-led model has been a crucial component to innovation in the global digital economy, especially in industry-led international standards development organizations (SDOs), including but not limited to the International Organization for Standardization (ISO), International Electrotechnical Commission (IEC), Internet Engineering Task Force (IETF), Institute of Electrical and Electronics Engineers (IEEE), and the 3rd Generation Partnership Project (3GPP). At the core of the international standards discussion is facilitating interoperability across products and services, lowering barriers to trade, and decreasing costs to companies and consumers. However, with the May 2019 Bureau of Industry and Security (BIS) addition of Huawei to the U.S. Entity List and associated guidance the standards community found itself at the intersection of security concerns and export controls. The published rules and guidance effectively blocked U.S. companies' participation in SDOs where listed entities may be present, leaving Huawei and other Chinese companies free to contribute and shape technology standards. It is clear such restrictions have harmed U.S. standards leadership at a time when the U.S. government claims it wants to encourage greater U.S. participation and influence in international standards development. The U.S. government should therefore take action to exempt standards and specification development and promulgation activities from the scope of Entity List designations and the Export Administration Regulations[7] so the private sector can continue to participate and lead.

In fact, the U.S. should continue to encourage all governments, including China, as has been U.S. policy for decades, to participate in international SDOs to develop standards instead of allowing countries to create country-specific ICT standards that are incompatible with the rest of the world. The key is to ensure that any interested stakeholder can participate in international standards

6 Jeanne Whalen, and Chris Alcantara. "Nine Charts that Show Who's Winning the U.S.-China Tech Race." *The Washington Post*, 21 September 2021.

7 Bureau of Industry and Security, Commerce. "Release of Technology to Certain Entities on the Entity List I the Context of Standards Organizations." *Federal Register*, 18 June 2020.

discussions and allow the rigorous process to prevent undue influence by any actor, regardless of company or nationality. Doing so has deterred some countries from mandating unique standards though domestic regulation.

Lack of Clear and Consistent National Security Narrative

The private sector must be responsible in working with the government to ensure we protect our national security. However, the U.S. should clearly articulate these security concerns based on narrow, objective, and consistent criteria with a holistic view of risks when evaluating commercial transactions with any country, including China. According to the Department of Homeland Security's Cybersecurity & Infrastructure Security Agency (CISA) ICT Supply Chain Risk Management (SCRM) Task Force Threat Scenarios Report,[8] "country of origin" is only one factor that should be considered in assessing the risks related to Information and Communications Technology and Services (ICTS) among a total of 188 supplier-related threats. Therefore, we cannot assume if the U.S. government bans everything from China, the supply chain would be safe and secure. Policy proposals aiming to address only "country of origin" or "China" would not be effective in securing the technology ecosystems. In fact, supply chain security is as much about company practices as it is about assessing threats to U.S. national security. The recent ransomware attack on the Colonial Pipeline on U.S. soil had a profound national security impact as malicious cyber criminals held U.S. critical infrastructure for ransom by stealing a single password.[9] Though China's historically malicious cyber activity presents serious security concerns, it is nevertheless important to holistically assess threats to U.S. national security.

One example of broad policy is Executive Order (EO) 13873, Securing the Information and Communications Technology and Services Supply Chain. The EO, which the Biden administration has chosen to continue to implement, is broad and effectively targets any ICTS transaction between a U.S. company and a foreign business partner, such as routine business transactions or Chinese civilians. In addition to reviewing ICTS transactions, it specifically grants the Secretary of Commerce the authority to block or unwind transactions deemed to be of unacceptable risk. Without clarification on how the authority may be triggered, it increases uncertainty for the industry as it could create unpredictable business interruptions. Further, although the government has defined China as a "foreign adversary" in the course of developing the interim final rule (IFR), the current definition of the term is unclear, and could include any individual employee of a U.S. company who is a citizen of China (including visa holders and green card employees in the United States). The U.S. government should clarify how industry should interpret and comply with the EO;

8 Cybersecurity and Infrastructure Security Agency Information and Communications Technology Supply Chain Risk Management Task Force. "Threat Evaluation Working Group: Supplier, Products, and Services Threat Evaluation." July 2021.

9 Stephanie Kelly, and Jessica Resnick-Ault. "One Password Allowed Hackers to Disrupt Colonial Pipeline." Reuters, 9 June 2021.

as it stands currently, it could broadly capture all types of ICT transactions with China. The U.S. government could provide an objective, narrowly scoped matrix or threshold for assessing risks to make their decisions more transparent to protect security and economic interest.

Over the last several years, the U.S. government has not communicated a cohesive and clear national security narrative and assessment criteria to the business community when it comes to the risks of doing business with China. Over the years, there have been different policy measures actively aimed at addressing the China threat, especially in the ICT sector. Though these tools are all well-intended for national security purposes, including the EO mentioned above, lack a comprehensive strategy to assess the threat, explain the problem, and communicate to the industry and other stakeholders. Even though sometimes with public consultations, these policy tools often identify the China factor then move quickly to implementation. However, without walking through threat assessment, explaining the risk, and communicate clearly to all stakeholders the national security risk, it could negatively impact U.S.-China economic relationship that has been serving as a cornerstone amid a deepening U.S.-China divide. The private sector and U.S. government have a real opportunity to develop a risk-based, evidence-driven, and holistic view to facilitate policy discussions on this issue that can enhance transparency and predictability for private companies to the greatest extent possible while ensuring national security concerns are addressed, which I offer more suggestions in the next section.[10] Otherwise, the U.S. risks confusing beneficial business activity for threats or misidentifying true vulnerabilities. Ultimately, U.S. policy cannot eliminate all threats, which is why risk mitigation is important and the U.S. needs to identify high-consequence threats that have a high likelihood of occurring, and not get distracted by the broad "what if" scenarios.

Policy Recommendations

Develop Narrow and Objective National Security Criteria

To diversify its supply chains and ties with China, the U.S. needs to develop a set of targeted national security criteria first that are consistent across all policies by leveraging resources already available, such as the SCRM Task Force recommendations, Committee on Foreign Investment in the United States (CFIUS), and BIS's ongoing review of foundational and emerging technology. The U.S. has attempted to develop some evaluation criteria around national security for transactions with foreign adversaries, even though the criteria is still too broad, it at least provides a general direction and opportunity to narrow it down further. For example, the Interim Final Rule on Securing the Information and Communications Technology and Services Supply

10 Information Technology Industry Council. "Supply Chain Security Policy Principles." June 2021.

Chain (Supply Chain Rule),[11] published on January 19, 2021, included 10 criteria as evaluation criteria for ICTS transactions in Section 7.103. Overall, most of the descriptive criteria are too broad, including the nature of the ICTS transaction, jurisdiction by the foreign adversary, statement and actions of the persons involved and the parties, etc., which could capture a lot of transactions, but sub-bullet 9 proposes considering the severity of the harm posed by the ICTS Transaction on factors, such as health, which demonstrates why the U.S. needs to diversify supply chains to ensure sufficient supplies of personal protective equipment (PPE) during the global pandemic. Additionally, this criterion also underscores the need for greater diversity of suppliers—whether it is for health or natural disaster—companies and governments need to prepare for disruptions in the supply chain and make sure they have access to necessary resources. Though there are other factors listed that potentially connect more closely with technology, such as critical infrastructure and sensitive data, it demonstrates the need for additional clarity and guidance around ICT supply chain and tech issues.

Take a Risk-Based Approach

The U.S. could also leverage CISA's criticality assessment to the Executive Order 13873 entitled, Assessing the Most Critical Information and Communications Technologies and Services in the Information Technology and Communications Sectors in order to develop the national security criteria and assess the most critical risks.[12] As a prime example of private-public partnerships, the National Risk Management Center (NRMC) worked with the industry to identify 10 critical information and communication technology (ICT) elements, which identified home subscriber servers (HSS), mobile switching centers (MSC), and many satellite-related elements as the most critical in the entire ICT ecosystem.[13] The U.S. should leverage this criticality assessment and prioritize these ICT elements that are labeled as "the most critical with high risks" and develop a diversification strategy, instead of trying to capture every technology that might potentially pose manageable or little risks. After all, ICT risk management is about directing precious resources to mitigate the most critical risk areas; if everything is critical, then nothing is critical.

11 Commerce Department. "Securing the Information and Communications Technology and Services Supply Chain." *Federal Register*, 19 January 2020.

12 Cybersecurity and Infrastructure Security Agency. "EO 13873 Response: Methodology for Assessing the Most Critical ICT and Services." April 2020.

13 Ibid.

Diversification Takes Time and Strategic Thinking

In general, diverse production and supply chains are often a source of resilience in an unpredictable environment. Companies with diversified supply chains are better able to adjust to external supply chain shocks to keep production and shipments online. However, it is also important to recognize that diversification requires patience and strategy, including assessing cost, availability, and stability. Companies often spend months if not years negotiating contracts with suppliers, analyzing their components and deciding how to assemble and test products in the most cost-effective ways, customized for specific regions of the world. For example, the recent semiconductor supply chain challenge demonstrates the issue has no quick fix, and that global supply chains are complex and require both long-term planning and active management of supplier relationships with hundreds of vendors around the world. Simply put, the process is a constant assessment of resource allocation to meet supply and demand, and identifying opportunities where diversification can bring sustainable long-term gains.

The Path Forward: Investments, Values, and Partnerships

Even though China is becoming a global leader in technology, the U.S. should not develop policy by responding to China's technology agenda; instead, the U.S. should maintain technology leadership by focusing on investing in critical and emerging technologies, protecting democratic values and privacy, and cooperating with global partners and allies.

Investment in Critical and Emerging Technologies

The Biden administration's ongoing efforts pursuant to the Executive 14017 on America's Supply Chains provides an opportunity to strengthen ICT supply chains and critical technologies, including semiconductors. Given that semiconductors enable a range of emerging technologies including AI, quantum computing, and 5G, investing in semiconductor ecosystem in the United States has the potential to drive innovation across many different sectors for decades to come. As demand for electronics and connectivity continues to grow, the U.S. should move quickly to provide necessary funding and incentives to build new capacity to meet these demands. To that end, funding the bipartisan CHIPS for America Act, passing legislation with a strong investment tax credit, and making sure these programs can come to fruition quickly should be a policy priority for the Biden administration.

Additionally, 5G, AI, and IoT are all critical national security technologies, and while China has developed various national plans to direct investments into these strategic areas, the U.S.' efforts are more scattered. Given that these technologies are still in early stages of development, ensuring the U.S. has a fuller picture of the technology ecosystems to enable more use cases is essential. To harness this growth and direct resources to the right space, public private partnerships are key to capturing opportunities for the rapid development and adoption of these technologies. More specifically on AI, the U.S. government should invest further in R&D that supports the responsible use of AI, including areas that improve accountability, fairness, and privacy of the AI systems that are critical in protecting human values.

Protection of Democratic Values and Privacy

In the digital era, data protection is essential to protect individuals not only from companies' misuse of personal data, but also from government surveillance. As Chinese companies have become successful globally, many recent U.S. actions toward China are driven by data security concerns, and a major concern is whether Chinese companies can be compelled to turn over user data to the Chinese government.[14] Indeed, the U.S. and like-minded partners should protect democratic values, including ensuring individual privacy is protected from government collection of data. Even though Chinese government and companies have recognized this issue as a challenge, so far, they have not done well in clarifying surveillance practices. Inspired by EU's General Data Protection Regulation (GDPR), China passed its comprehensive privacy law—the Personal Information Protection Law (PIPL)—in August 2021. Even though PIPL has strong provisions that are similar to the GDPR to safeguard individual privacy, it is unclear how the law would meaningfully protect Chinese citizens from the government's broad use of surveillance. For example, a new report from the European Data Protection Board (EDPB) report on Government Access to Data in Third Countries states that substantial protection of personal data against government access does not exist in the PRC.[15] With the recent Schrems II judgment calling for greater privacy protections in government access to data, it is unclear how the Chinese government could engage with these pressing questions globally without significant reforms and transparency regarding its own surveillance practices.[16]

To uphold privacy and democratic values, the U.S. and like-minded countries should continue to develop consensus on this matter. The Organisation for Economic Cooperation and Development's (OECD) work on Government Access to Private Sector Data gathers countries around the world to identify privacy best practices in government surveillance to address these pressing issues on

14 Eva Dou. "Documents Link to Huawei to China's Surveillance Programs." *The Washington Post*, 14 December 2021.

15 European Data Protection Board (EDPB). "Government Access to Data in Third Countries." November 2021.

16 Alexa Lee. "Personal Data, Global Effects: China Draft Privacy Law in the International Context." *DigiChina*, 4 January 2021.

transparency, redress, proportionality, and more. Even though China has a different political system, highlighting the importance of privacy in the government access to data context should be a priority to ensure individuals are sufficiently protected no matter where the data is collected, processed, and transferred. Additionally, the U.S. needs to pass comprehensive federal privacy legislation immediately to ensure U.S. citizens data is protected from any governments or companies from abusing it, including China. Failure to offer a compelling vision for U.S. data governance will make the U.S. less secure and more vulnerable to China's global data governance agenda.[17]

Cooperation with Global Partners and Allies

As geographic diversification has become critical in the U.S.-China technology competition, the U.S. should work with partners and allies such as the EU, Japan, South Korea, Taiwan, and others in the Asia Pacific and Latin America to minimize damaging interruptions and ensure stability of the global supply chains. Diversification with global partners and allies includes many dimensions, including lowering costs, promoting efficiency and productivity, enabling access to global talent and growing customer bases, and mitigating supply chain risks. Given the immense opportunities for cooperation in these areas, the U.S. should work with allies and partners to drive alignment on strategic objectives and convene technology and supply chain cooperation. For example, the U.S.-EU Trade and Technology Council provides opportunity to seek alignment on many technology topics, including semiconductors, AI, cybersecurity, and others, serving as a platform for consistent exchange on the most critical issues across the Atlantic. The recent developments of the U.S.-Mexico High-Level Economic Dialogue, U.S.-South Korea Semiconductor Supply Chain Forum, and the new U.S.-Taiwan Trade and Technology Framework are all encouraging examples.

Moreover, given the fact that several Asian economies are essential in evolving global ICT supply chains, their roles as growing hubs for trusted supply chain partners continue to be crucial, and the concept of "trusted supplier" should be further discussed. The recent U.S.-China trade tensions and pandemic have also accelerated diversification of supply chains in the Asia Pacific region as companies have sought to move supply chains to ensure that they are not overly reliant on any one supplier or geography. To ensure that the U.S. can capitalize on these opportunities and enhance its competitive advantage with respect to China, increasing bilateral, regional, and multilateral engagements on digital trade priorities could unleash more technology cooperation, including organizing tech-sector specific dialogues and forming digital trade partnerships.

17 Samm Sacks. "Testimony of Hearing on Promoting Competition, Growth, and Privacy Protection in the Technology Sector: Senate Finance Committee." Senate Finance Subcommittee on Fiscal Responsibility and Economic Growth, 7 December 2021.

Conclusion

The U.S. and China have had profound economic and technology ties for decades. A successful U.S. response to China's technological challenge will depend upon improvements at home as well as external actions[18]—namely, to diversify and lead. An untargeted U.S-China decoupling would not benefit either side, but instead, diversifying supply chains with a clear, narrowed, and objective national security framework can mitigate risks to balance national security interest and economic opportunities. Further, it is also imperative for the U.S. to focus on strengthening its own technology leadership by investing in critical and emerging technologies, protecting key values and privacy, and collaborating with global partners and allies.

18 Joseph S. Nye. "What Really Matters in the Sino-American Competition." Project Syndicate, 6 December 2021.

CYBER PROJECT
Belfer Center for Science and International Affairs
Harvard Kennedy School
79 JFK Street
Cambridge, MA 02138

belfercenter.org/project/cyber-project