DigiChina

Stanford | Geopolitics, Technology, and Governance
Cyber Policy Center

NEW AMERICA

Mapping U.S.–China Technology Decoupling

How disparate policies are unraveling a complex ecosystem

By Yan Luo, Samm Sacks, Naomi Wilson, and Abigail Coplin

Over the past two decades, U.S. and Chinese technological trajectories have been closely linked. Internet protocols, hardware design and manufacturing, software development and deployment, and services and standards have to varying degrees been cross-border phenomena, with China and the United States two of the world's most consequential and integrated countries.

The last few years, however, have seen a rise in mutual suspicion and moves—both direct and indirect—to unwind this extraordinary level of technological interdependence. The overall effect is an increasing degree of separation between the two ecosystems, a process widely known as decoupling.

Policy thinkers have fiercely debated the wisdom of disentangling the two countries' high-tech environments, but a wide array of policy actions from both governments already have the effect of increased separation. Many of these actions are undertaken with specific concerns in mind and a degree of decoupling as a side-effect.

Thus far, it has been difficult to understand the degree to which the two countries are already unraveling their technological ties, so we embarked on this effort to map the types of policies and specific moves that in aggregate already amount to a historic shift in the world's technological, scientific, and industrial systems.

The mapping that follows reveals that many of the concerns driving policy change are far from new. Indeed, many of the policy moves now contributing to decoupling build on longstanding patterns. China especially has a history of restricting foreign investment across a wide range of sectors in the name of national security—food security, biological security, information security, etc.—and blocking foreign websites and services to maintain control over information. The Chinese government for decades has been determined to build a more advanced economy and reduce dependency on potentially hostile foreign actors.

Yan Luo *is a Partner in Covington & Burling's Beijing office.* ***Samm Sacks*** *is a Senior Fellow at the Paul Tsai China Center at Yale Law School and a Cybersecurity Policy Fellow with New America.* ***Naomi Wilson*** *is Director of Policy for Asia at the Information Technology Industry Council.* ***Dr. Abigail Coplin*** *is an Assistant Professor of Sociology and Science, Technology and Society at Vassar College.*

In the post-Cold War period, during which digital and internet technologies took flight globally and U.S.–China integration deepened, the U.S. government had a relatively laissez-faire approach, with national security invoked sparingly in regulating high-tech fields. That has changed gradually as a widening circle of policymakers grew concerned about Chinese threats to U.S. security and the Chinese government's efforts to gain advantage or exploit technology against U.S. interests or values.

Despite increasingly open discussion of mutual security concerns, decoupling so far is occurring piecemeal. Our map also highlights the asymmetric nature of actions taken by both governments. Across each category we identify measures coming from Beijing and Washington, and several patterns emerge:

- U.S. actions tend to target China specifically, whereas Chinese policies tend to aim for security against diverse threats or the strength of domestic industries—or at tit-for-tat moves against new U.S. policies.
- The two sides appear to mirror each other in their rising national security scrutiny of data flows, expansion of export controls, and measures to shore up supply chain security for information and communications technology products and services.
- Policies in both countries at times appear questionably suited to achieve their stated goals, while entailing significant collateral effects on research and industry.
- Efforts from both governments suggest a strikingly similar set of concerns around mutual vulnerability lurking in technological systems both societies depend on, and around the overlap between national security and technological advantage.

This mapping is a snapshot at a moment when the U.S.–China technology relationship has witnessed a period of starkly increased conflict. That trajectory is likely to continue, heading into the U.S. election in November, as the Trump administration has continued rolling out policies, initiatives, and sanctions that target China. As developments unfold, our framework aims to provide a basis for tracking and anticipating the mounting impact on the U.S.–China relationship and technology governance. ●

About DigiChina

The DigiChina project, based at Stanford University and in partnership with New America and the Leiden Asia Centre, is a collaborative effort to understand China's digital policy developments through translation, analysis, and contextualization.

Housed within the Program on Geopolitics, Technology, and Governance, part of the Cyber Policy Center at Stanford's Freeman Spogli Institute for International Studies, the effort is led by Research Scholar and DigiChina Editor in Chief Graham Webster, with a network of contributors spread across dozens of academic, policy research, civil society, and industry institutions.

Export and import controls

Restrictions on cross-border trade in goods often have other primary goals, but their growth unwinds bilateral trade.

Chinese Government Actions	U.S. Government Actions
Export controls	
• An updated **draft Export Control Law** released on June 28 would become China's first national legislation on export controls, but it is unclear how the government might enforce it if enacted. The draft would authorize China to take reciprocal measures against countries that impose "discriminatory export control measures on China," a provision echoed for data regulations in the draft Data Security Law. • The **draft Data Security Law** cites data that is related to China's national security and its performance of international obligations among export-controlled items. • The Ministry of Commerce was **reportedly** considering restricting exports of products made in China by Nokia and Ericsson as retaliation if more European countries ban Huawei from their networks.	• The Commerce Department Bureau of Industry and Security (BIS) **added Huawei and its affiliates to the Entity List** in May 2019, banning U.S. exports to the company without a special license. • In May 2020, BIS followed with an **amendment** to the Foreign-Produced Direct Product Rule (FDPR), requiring licenses for Huawei's suppliers to use U.S. semiconductor manufacturing equipment or software. • The Entity List has also been used to penalize **two sets** of **Chinese companies** "implicated in human rights violations and abuses" against Muslim minority groups in Xinjiang. • BIS published **two** new **rules** and one **proposed rule** to address the risk that U.S. technology exports could contribute to China's "military-civil fusion" efforts. A change to the definition of "Military End Use" and "End user" expanded the number of U.S. products in the semiconductor, aerospace, and other dual-use sectors that will require a license before being exported to China. • The State Department **announced** an end to exports of controlled defense and dual-use technology to Hong Kong in response to new national security legislation imposed by the central government in Beijing. A Commerce Department rule **ended** Hong Kong licensing exceptions for the export of additional technology items under the under the Export Administration Regulations. • The **Uyghur Human Rights Policy Act**, enacted in June, imposes sanctions on individuals and entities identified as responsible for human rights abuses against Uyghurs and others in Xinjiang. It also requires reporting on the Chinese government's acquisition and development of technology to facilitate internment and mass surveillance in Xinjiang.

Chinese Government Actions	U.S. Government Actions
Import controls	
• A government "**unreliable entity list**" of foreign companies targeted for increased scrutiny or penalties has yet to be activated. The list could be used to designate companies for special scrutiny under regulations such as the **Anti-Monopoly Law** and the **Cybersecurity Review Measures**.	• A May 2019 executive order on supply chain security gave the Commerce Department sweeping authority to prohibit purchases deemed a risk to national security and linked to a "foreign adversary"—widely regarded as targeting Chinese suppliers. • The Federal Communications Commission **announced** in June that it would no longer allow U.S. telecommunications providers to use federal money to purchase Huawei or ZTE components.

Data handling and cross-border data flows

Data governance is an emerging regulatory challenge that can affect trade in services and cross-border business.

General or important data	
• A **draft Data Security Law** released in July would establish a national security review system to examine any broadly defined "data activities" that may be deemed to pose risks to national security. The draft law would also authorize retaliatory measures against countries deemed to have adopted "discriminatory prohibitions, limitations," etc., against China in the data sphere. • Under **draft Data Security Management Measures**, network operators must conduct a risk assessment and obtain prior approval(s) from their corresponding industry regulator(s) for cross-border transfers of "important data"—a vaguely defined term encompassing "data that, if divulged, may directly affect national security, economic security, social stability, or public health and safety." A national standard is set to more concretely define the scope. • China's government has long restricted data in certain sectors that it considers "important" to national security. For example, operators of online mapping services are required to place servers storing Chinese geospatial data in China.	• The Department of the Interior **grounded** its drone fleet in January over data security concerns linked to drones made by the Chinese company DJI and other Chinese-made components. • Senators Josh Hawley and Richard Blumenthal in July **called for** a Department of Justice investigation of the U.S. videoconferencing company Zoom's data practices over its links to China.

Data handling and cross-border data flows (continued)

Chinese Government Actions	U.S. Government Actions
Personal data	
• Under China's **Cybersecurity Law** and various implementing regulations, upcoming regulatory requirements could impose restrictions on the cross-border flow of personal data. • The draft **Personal Information Outbound Transfer Security Assessment Measures**, released in 2019 and pending finalization would require: network operators to undergo a security assessment process before transferring abroad personal data collected in China; and network operators and overseas recipients to enter into contracts with specific provisions, among other requirements. Broad restrictions raise the potential for targeted enforcement or delay of data transfers, and contract requirements could lead to extraterritorial implications.	The United States has not historically restricted the transfer of personal data to other jurisdictions, but several actions mark a shift: • CFIUS reviews of transactions involving sensitive personal information, with divestment required for Chinese companies (e.g. Grindr and TikTok); • The **National Security & Personal Data Protection Act** (sponsored by Senator Josh Hawley) would restrict companies from "countries of concern" including China and Russia from transferring user data to such countries; • Federal Trade Commissioner Rohit Chopra **stated** that "Surveillance and data collection on American children raise concerns that go beyond privacy. According to a **State Department official**, there are critical national security issues with respect to technology companies affiliated with the Chinese government, such as Huawei, ZTE, Alibaba, Baidu, and Tencent"; • The State Department Clean Network initative, which seeks separation from Chinese technology providers, **includes** a planned "Clean Cloud" component, highlighting Alibaba, Baidu, and Tencent as threat to personal and business data; • Executive orders on the Chinese-owned apps TikTok and WeChat, discussed under "App and website bans" below, cite risks to personal information among their concerns.

Data handling and cross-border data flows (continued)

Chinese Government Actions	U.S. Government Actions
Biological and genetic data	
• The 2019 **Regulation on the Management of Human Genetic Resources** bars foreigners from collecting human genetic resources or exporting them from China outside the context of a government-approved collaboration. In those collaborations, the Chinese partners must be guaranteed access to all records and data and provided with a backup copy, and they must jointly hold any patent rights. "Genetic resources" here includes both physical samples and data or information produced from such samples. These requirements come with increased penalties versus prior interim regulations, and enforcement appears on the rise. • A 2020 second draft of the **Biosecurity Law** states that the Chinese state shall implement a uniform system for publishing biosecurity information, including information on biosecurity incidents and their investigation/handling. No unit or individual may publish this information without authorization. There is some debate regarding whether this provision extends to scientific research, including the publication of viral genomes, etc. • The draft law would require government permission for foreign entities to collect or transfer abroad any species unique to China or specimens that could be used to reproduce them. • The draft law would require the government to classify biotechnology research by risk level, and only Chinese entities could conduct high- or medium-risk research within China.	*U.S. regulations on biological and genetic data generally focus on privacy protection and de-identification, but do not specifically address cross-border transfers.*

Supply chain security reviews

Supply chain security is a rising priority in both countries, and both consider risks associated with the other's government.

Chinese Government Actions

Network products and services

- China's **Cybersecurity Law** requires "critical information infrastructure" (CII) operators to undergo a security review if the procurement of "network products and services" implicates China's national security.
- The recently finalized **Cybersecurity Review Measures** lay out a system of reviews for security and supply chain reliability for products and services procured by CII operators—a broad category including "sectors and areas including telecommunications, radio and television, energy, finance, road and water transport, railroads, civil aviation, post, water management, emergency management, hygiene and healthcare, social security, national defense science, technology and industry, etc."
- The Cybersecurity Review process includes a self-assessment of risks to China's national security and, if the self-assessment flags specific risks, a mandatory review led by the Cyberspace Administration of China (with participation from other agencies).
- Among the supply chain risks considered is "the risk of supply disruptions due to political, diplomatic, and trade factors."

U.S. Government Actions

- The **Secure 5G and Beyond Act of 2020**, enacted in March, requires a strategy involving strategic allies and partner countries to secure wireless communication infrastructure and services, ensure competitiveness of U.S. companies, and protect consumer privacy and the intergrity of standards-setting bodies.
- **National Defense Authorization Act of 2019** Section 889 restricts government procurement from companies with supply chains with any nexus to Huawei or ZTE.
- The State Department **Clean Network** initiative expands upon "trusted vendor" discussions among the United States, Australia, the United Kingdom, and others, pushing toward effectively banning Huawei from 5G networks, while also calling for "trusted digital standards" across app stores, apps, cloud services, and infrastructure cables.
- The **Secure & Trusted Communications Networks Act**, enacted in March, prohibits the use of federal funds for equipment or services from a company deemed to pose a national security risk to U.S. communications networks.
- The **Executive Order on Securing the Information and Communications Technology and Services Supply Chain** gives the Commerce Department broad authority to ban U.S. tech purchases deemed a national security threat.
- Under the **Executive Order on Securing the United States Bulk-Power System**, certain transactions involving bulk-power system electric equipment designed, developed, manufactured or supplied by a "foreign adversary" may be blocked.
- In January, Senator Tom Cotton **introduced** a bill that would "prohibit the sharing of United States intelligence with countries that permit the operation of Huawei fifth generation telecommunications technology within their borders."

Financial untangling

Mutual investment had grown in recent years, but several moves add uncertainty or risk to U.S.–China investment flows.

Chinese Government Actions	U.S. Government Actions
Delisting companies or forcing divestment	
	• The **Holding Foreign Companies Accountable Act (HFCAA),** under consideration in the Senate, would require companies listed on U.S. stock exchanges to certify they are not under the control of a foreign government and undergo three consecutive years of audits by the Public Company Accounting Oversight Board (PCAOB), requirements that many U.S.-listed Chinese companies might find difficult to meet. The Trump administration may take executive action without HFCAA to increase pressure on Chinese companies to delist. • The State Department has **warned universities** to divest of Chinese stock holdings, because "enhanced listing standards [could likely] lead to a wholesale de-listing of PRC firms from U.S. exchanges" by the end of 2021.
Foreign acquisitions or investment	
• China imposes restrictions on foreign investment in industries that are included on the "Negative List." For example, foreign investors are not allowed to hold more than 50% equity interest in companies providing value-added telecom services (including cloud-related services) in China. Some sectors addressed by the **negative list**, updated in 2020, are totally off-limits to foreign investment.	• The interagency Committee on Foreign Investment in the United States (CFIUS) **ordered** the Chinese firm ByteDance to divest from social media subsidiary TikTok's U.S. operations after examining its earlier acquisition of the U.S. firm Musical.ly. A 90-day clock, with a possible 30-day extension, began on August 14.

Limits on travel, visa issuance, and work or study authorization

Policies that effectively decrease people-to-people ties are amplified by pandemic-based restrictions.

Chinese Government Actions

- In a tit-for-tat dynamic with U.S. government restrictions, the Chinese government expelled U.S. journalists working for *The New York Times*, the *Wall Street Journal*, and the *Washington Post*, forcing China-related coverage in the papers to be produced from abroad.

U.S. Government Actions

- A series of executive orders have **blocked** entry to Chinese students linked with universities or other groups involved in China's "military-civil fusion strategy," which is defined here in terms of "acquir[ing] or divert[ing] foreign technologies" for Chinese military purposes.
- The Trump administration announced and then rescinded an **order** that would have expelled foreign students whose schools planned to meet only online due to the pandemic. This and **other limits** on visas would affect students from all countries, though Chinese students and scholars are particularly numerous.
- Some scientific research in a **range of fields** requires a "deemed export" license in order for foreign nationals to participate.

Encryption

Which types of encryption are permitted affects how products might be localized, or prohibited, in the other market.

- China's **Encrytion Law** establishes an import and export licensing framework for commercial encryption products and sets out separate mandatory and voluntary testing and certifit-aion requirements for commercial encryption products. Import and export of the commercial encryption products that "may impact national security or the public interest" are to be subject to licensing requirements.
- The government has released the **Commercial Encryption Product Certification Catalogue** (First Batch) and the **Commercial Encryption Product Certification Measures** to implement the volutary certification scheme established under the Encryption Law. The certifications obtained by product manufacturers under this voluntary scheme serve as assurance to customers that the commercial encryption products conform with Chinese encryption standards.
- The Encryption Law imposes specific obligations on "critical information infrastructure" operators, including a required security assessment if they use commercial encryption. If the procurement and use of commercial encryption products and services may impact national security, they must undergo a government-run security review.

Website and app bans

Chinese censorship has long resulted in barriers for users and companies, and the U.S. government has recently threatened its own bans.

Chinese Government Actions

- Websites hosted outside of China may be blocked at will.
- The Chinese government has put in place measures to ensure that Chinese users only use VPN services that are provided by licensed Chinese VPN services providers.
- The Chinese government has long blocked access to U.S. online products ranging from Facebook, YouTube, Twitter, and other social platforms to Google products and a wide array of media outlets.
- China's **Administrative Measures on Information Services Provided by Mobile Internet Applications** specifically prohibits app operators from conducting any activity that may jeopardize national security, disrupt social order, or infringe upon others' legitimate rights and interests, and from producing, duplicating, publishing or disseminating information that is otherwise prohibited.

U.S. Government Actions

- Trump Executive Orders (EOs) targeting TikTok and WeChat rely on authorities granted under the International Emergency Economic Powers Act to address the "national emergency" posed by these apps.
- The **TikTok EO** cites concerns with the app's capture of "vast swaths of information" from users including network activity and browsing histories, saying this capability "threatens to allow the Chinese Communist Party access to Americans' personal and proprietary information."
- The proposed **No TikTok on Federal Devices Act** would ban federal employees from using TikTok on government devices.

Efforts to reduce dependence on the other country

Some policies are aimed directly at reducing mutual dependency, counteracting the interwoven status quo or doubling down on longstanding self-reliance goals.

Government funding and policy support for advanced technology industries

- A $1.4 trillion **"New Infrastructure" initiative** aims to build up domestic capability in 5G, industrial Internet of Things, high-speed rail, data centers, artificial intelligence, ultra-high-voltage transmission grids, and electric vehicle charging stations. Foreign chipmakers could still have a role to play, given a lack of domestic substitutes.
- The State Council's new Integrated Circuit (IC) Development Policy creates financial and investment support to boost local industry. It is the latest in a series of central and local government IC plans over the years.
- Following the U.S. Commerce Department's May amendment to the Foreign-Produced Direct Product Rule, the Chinese government **injected $2 billion** into China's leading semiconductor foundry to build up new chip capacity.
- The proposed **Creating Helpful Incentives to Produce Semiconductors (CHIPS) for America Act** (House) and **American Foundries Act** (Senate) call for federal investment to bring chip manufacturing back to the United States and increase R&D spending.
- In May, the Department of Health and Human Services **launched** the "Pharmaceutical Manufacturing in America" effort to increase domestic production of active pharmaceutical ingredients and ancillary supplies such as vials and syringes, working with **industry partners**.

Scientific and research collaboration

- China's **Scientific Data Management Measures** define "scientific data" broadly to include outcomes of scientific or engineering efforts and their derivatives and regulate its collection, production, and sharing when supported by government funds.
- The Department of Justice's **China Initiative** places strategic priority on prosecution of Chinese state-backed efforts related to trade secret theft, hacking, and economic espionage. Investigations of researchers connected with China have sharply increased.