THE EVOLUTION OF U.S. THINKING AND POLICY

In the last few years, the U.S. government has come to see technological interdependence with China as a major threat to American security, prosperity, and values. Washington fears that Beijing can leverage technological linkages to steal secrets, spread disinformation, surveil dissidents, hold U.S. infrastructure hostage, and leap ahead in economic competition, among other threats. As a result, U.S. officials of both parties have sought to substantially—though not completely—reduce the flow of technology products, services, and inputs to and from China. This process is sometimes called "technological decoupling."[3] Decoupling is not just a bilateral phenomenon, nor is it entirely the product of governmental policy. Many public and private sector actors around the world are contributing—in different ways, and with varying motivations and levels of enthusiasm—to the trend.

Although the overall trend toward technological decoupling is clear, its exact course and ultimate extent remain unknown. There are many possibilities. In an extreme scenario, decoupling widens and accelerates until distinct geo-technological spheres emerge—one centered on the United States, one centered on China, and perhaps others. Because technology is so intertwined with all commercial activity, such a technological split would drastically reduce every kind of economic interaction between China and the U.S.-aligned world. In the opposite scenario, U.S.-China technology ties gradually begin to stabilize, finding a new equilibrium that preserves the vast bulk of the global technology supply chain. Various other scenarios lie in between these two poles, and many international actors are vying to shape the future.

The U.S. government has been a principal driver of recent technological decoupling with China and remains uniquely able to adjust this global trend up or down.

The most important decisionmaker, for now, is the U.S. government. Washington has been a principal driver of recent technological decoupling with China and remains uniquely able to adjust this global trend up or down. By comparison, other major actors have been more reactive. While Beijing has long maintained its own limits on American and other foreign technology, it has been more hesitant than Washington to add significant new technology restrictions in recent years. China still appears interested in retaining many of the technological links it has built over decades, at least until it can position itself for greater self-sufficiency. Beijing has therefore responded in a cautious, reciprocal manner to many U.S. tech restrictions (though it is gradually becoming more assertive). Other governments and private sector players have diverse views on technological decoupling, yet very few are as forward-leaning as the U.S. government, and none has pushed the trend as forcefully and effectively.

A NEW CONVENTIONAL WISDOM

Two broad trends have driven the U.S. government's recent interest in technological decoupling. First, beginning in the mid-2010s, U.S. policymakers and political leaders developed much darker views of China. Previously, most in Washington had believed that China's rise was largely compatible with and even beneficial to American interests. Although Beijing's human rights abuses, market distortions, and other behavior were always points of friction, U.S. officials in the 1990s and 2000s thought the best solutions were further integration of China into global institutions and deepening of bilateral political and economic engagement.[4]

This official consensus, never without dissenters, eroded and eventually collapsed during the Obama administration. Major catalysts included China's militarization of disputed islands and broader military buildup; its unrelenting intellectual property theft and exploitation of international trade rules to move up the economic value chain; its deepening authoritarianism and abhorrent repression of Uyghurs and other minority groups; and its bolder encroachments on Hong Kong and Taiwan.[5] Across the board, China seemed increasingly intent on and capable of challenging U.S. interests, values, and visions of global order. These developments caused a sea change in U.S. thinking on China. Within a few short years, cautious optimism or ambivalence turned into distress and fear, and most U.S. policymakers came to identify Beijing as America's primary long-term state threat (see Table 2). As a result, U.S. leaders belatedly started to scrutinize the many ways their country had become dependent on or supportive of China in prior decades—with technology rightly emerging as a central concern.

Table 2: U.S. Rhetoric on China Has Shifted Dramatically Over a Decade

2010 Obama National Security Strategy	**"We will continue to pursue a positive, constructive, and comprehensive relationship with China."**
2015 Obama National Security Strategy	**"The scope of our cooperation with China is unprecedented even as we remain alert."**
2015 Secretary of Defense Ashton Carter, Obama White House	**"A return to great power competition," though "nothing is preordained about this relationship."**
2017 Trump National Security Strategy	**"China . . . want[s] to shape a world antithetical to U.S. values and interests."**
2020 Secretary of State Mike Pompeo	**"The Chinese Communist Party['s] actions are the primary challenge today in the free world."**
2021 Secretary of State Antony Blinken	**"Our relationship with China will be competitive when it should be, collaborative when it can be, and adversarial when it must be."**

Sources: "National Security Strategy," White House, May 2010, https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/national_security_strategy.pdf; White House, "National Security Strategy," February 2015, https://obamawhitehouse.archives.gov/sites/default/files/docs/2015_national_security_strategy_2.pdf; David B. Larter, "White House Tells the Pentagon to Quit Talking About 'Competition' With China," Navy Times, September 26, 2016, https://www.navytimes.com/news/your-navy/2016/09/26/white-house-tells-the-pentagon-to-quit-talking-about-competition-with-china/; Michael R. Pompeo, "Communist China and the Free World's Future," State Department, July 23, 2020, https://2017-2021.state.gov/communist-china-and-the-free-worlds-future-2/index.html; Antony J. Blinken, "A Foreign Policy for the American People," State Department, March 3, 2021, https://www.state.gov/a-foreign-policy-for-the-american-people/.

Second, during roughly the same period, techno-nationalist ideas became ascendant around the world and eventually took hold in the United States. By the 2010s, digital technologies such as online platforms, mobile devices and apps, streaming media, and targeted advertising had matured into powerful new global industries, unsettling previous economic structures. Some tech firms, like social media companies, even subsumed state-like functions—setting terms for public discourse and determining when and how governments could access their own citizens' private information. Digital technologies also came to have great value in espionage and warfare. Because the most globally successful tech companies were American, China and many other countries bristled at the entrenchment and extension of U.S. influence. They sought ways to claw back some measure of digital sovereignty—especially after Edward Snowden's disclosures about U.S. surveillance.

Washington was more sanguine at first. It had long extolled the digital globalization led by U.S.-based multinational tech companies, which enriched Silicon Valley and empowered America on the world stage. But an onslaught of major cyber and influence operations by

foreign actors, including China, gradually convinced U.S. leaders that America's digital openness was also a vulnerability.[6] Meanwhile, there was growing apprehension about the next wave of emerging tech, especially machine learning and 5G. These innovations were said to be even more transformative than previous digital technologies—but this time, China would rival or even surpass Western capabilities, in part due to Beijing's organized exploitation of its technological links with the West. Washington finally realized what other governments already understood: technology had become a key arena of interstate competition that could not simply be left to the marketplace. U.S. technology would need to be better protected from adversaries and more closely aligned with national strategy.

These two trends gave birth to a new American techno-nationalism focused principally on China. The basic ideas began to take shape during former president Barack Obama's second term and drove a few early regulatory actions.[7] The Trump administration then went much further, elevating techno-nationalist thought within U.S. strategy and rhetoric and greatly expanding the number and scope of measures targeting Chinese tech threats. President Joe Biden, while making some tactical adjustments, has largely followed suit so far. There is now bipartisan consensus that the U.S. government must take a lead role in organizing the American technology ecosystem to reduce its interdependence with China.

PAST PRECEDENTS

Today's American techno-nationalism is not wholly unprecedented. In fact, much of the institutional architecture that Washington now uses to nurture and protect U.S. technology strength originated during two prior techno-nationalist periods. Early in the Cold War, U.S. leaders recognized that science and engineering would be key factors in America's military and geopolitical struggle with the Soviet Union. Thus they created the National Science Foundation, spent extraordinary sums on the Space Race, used defense contracts to seed what would become Silicon Valley, expanded the federal role in higher education, and worked with allies to establish the Coordinating Committee for Multilateral Export Controls (COCOM).[8] By the time the Cold War was receding in the late 1980s and early 1990s, Japan had emerged as a fierce economic and technological competitor to the United States. This spurred another wave of U.S. techno-nationalist policies, including the creation of SEMATECH, a public-private partnership with the domestic semiconductor industry, and the Exon-Florio Amendment, which transformed the Committee on Foreign Investment in the United States from a sleepy study group into a powerful regulator of cross-border deals.[9]

These earlier periods of techno-nationalism, which are still being debated, offer many potential lessons for today's U.S. policymakers.[10] Yet historical analogies should be treated with caution, as they fail to capture unique features of the current China challenge. The United States has successfully contested a geopolitical adversary (the Soviet Union) and a

modern technological competitor (Japan), but it must now face a single rival that plays both these roles at once and has more latent capacity than either of its predecessors.

China's economy could become the world's largest in a decade, and it is already about 70 percent as big as America's in nominal terms—roughly equal to Japan's peak proportion (in 1995) and perhaps twice the share (or more) ever achieved by the Soviet Union.[11] China's population is more than four times that of the United States, whereas the Soviet Union was only slightly larger than America, and Japan much smaller.[12] Of course, China lacks the Soviet Union's world-class nuclear arsenal and large network of allies, client states, and ideological bedfellows. And Beijing has fought no proxy wars in recent decades. Yet its deep economic and technological integration with the U.S.-aligned world grants it opportunities that the Kremlin never had, creating novel dilemmas for Washington. And while the Chinese economy faces serious demographic, financial, and political risks in the years to come, Beijing's signature brand of state-guided capitalism appears more dynamic and resilient than the creaky machinery of Soviet central planning.

The United States has successfully contested a geopolitical adversary (the Soviet Union) and a modern technological competitor (Japan). But China now plays both these roles and has more latent capacity than either predecessor.

The technological landscape has also changed a great deal since the mid-to-late twentieth century. Then, the U.S. government was a leading innovator in its own right and "spun off" many breakthroughs to the private sector. Now, private companies develop the most exciting new technologies while the public sector scrambles to understand and absorb them. Then, Washington had relatively cozy relationships with large American companies—as expressed in the famous (though hyperbolic) claim that "what was good for our country was good for General Motors, and vice versa."[13] Today, major U.S.-based tech firms are vast, multinational, digital-physical enterprises with complex loyalties and their own foreign policies.[14]

The American nation has also changed, as has the world and the U.S. role within it. Domestic social cohesion, governance capacity, and political stability have plummeted.[15] U.S. leaders now struggle to do anything big at home, or even to rally the country in the face of foreign threats. Looking outward, Washington confronts a more multipolar system and a somewhat strained set of alliances. America still leads, but with diminished influence, credibility, and prestige. Today's world is also much more interconnected, thanks in large part to decades of U.S.-driven globalization. Collaborative scientific research and international technology supply chains span the globe, creating efficiencies never before possible. But this interconnectedness also comes with looming, systemic risks: global climate change, global financial crises, global pandemics, global supply chain disruptions, and global cyber

Techno-nationalism must be reconsidered for a radically changed world. This means looking with fresh eyes at familiar strategies and policies.

incidents, among others.[16] Global challenges demand global cooperation, yet international institutions have struggled to meet the moment.

In short, U.S. leaders find themselves in uncharted territory. Although America has a rich heritage of techno-nationalist thought and policy to draw upon and learn from, today's circumstances are quite different from those faced by previous generations. Techno-nationalism must be reconsidered for a radically changed world. This means looking with fresh eyes at familiar strategies and policies.

"OFFENSIVE" AND "DEFENSIVE" MEASURES

U.S. techno-nationalist policies are often divided into two groups. "Defensive" measures aim to thwart and contain technology threats from China, while "offensive" measures seek to nurture America's own technological strength. During the Trump era, policymakers in the administration and Congress overwhelmingly focused on defensive measures, such as export controls, investment restrictions, and the denial of visas and regulatory licenses for Chinese workers, students, and businesses. While defensive measures are still being actively developed and deployed, there is now some consensus—among Biden administration officials, members of Congress, and outside policy experts—that offensive measures deserve far more attention. This shift can be seen in bills like the U.S. Innovation and Competition Act and the America COMPETES Act, two mammoth pieces of draft legislation. Although the bills contain multiple defensive measures, they focus primarily on offensive goals like funding and facilitating R&D.

That said, defensive measures continue to raise some of the most acute policy dilemmas. On the one hand, these tools provide uniquely powerful means for Washington to reshape the bilateral technology relationship. Regulations and other coercive federal powers can be used to quickly sever technology links deemed unduly risky. This obviates the need for U.S. leaders to cajole American businesses or universities with patriotic appeals, to place faith in blind market forces that may not align with national policy, or to negotiate directly with the Chinese government or (sometimes) with other governments. Moreover, the executive branch can often impose defensive measures on its own initiative, without the need for new statutes or spending bills from Congress.

However, defensive measures can come with significant costs and risks. They may cut off—perhaps abruptly—key sources of labor, supplies, and funds that U.S. businesses and uni-

versities depend on to develop and deploy important technologies.[17] Defensive actions may provoke China's ire, triggering various forms of retaliation and further damaging a sensitive bilateral relationship. Allies and trading partners may also object to or resist U.S. actions that disrupt global technology supply chains. Moreover, each new defensive measure raises the possibility of still more restrictions in the future, causing outside actors to try to get ahead of U.S. policy and thereby increasing the risk of a decoupling spiral that exceeds U.S. tolerances.

Thus, while U.S. leaders rightly refocus their attention on offensive actions to promote American technological strength from within, they must also make difficult decisions about the role of defensive measures. Washington must find a delicate balance that addresses legitimate concerns about Chinese technology while avoiding overreach and self-sabotage.

There are many kinds of defensive tools, and U.S. policymakers must have a firm grasp of their differences (see Table 3). Defensive tools are often described generically as "sanctions" or "blacklists," but this conflates distinct legal authorities with a range of effects and implementing agencies. For example, SenseTime and Hytera are among the Chinese tech firms most targeted by U.S. controls, yet the restrictions imposed on each company do not overlap at all. Huawei, meanwhile, suffers from nearly all of the controls placed on both SenseTime and Hytera, plus others that are completely unique (see Table 4 at the end of the chapter).

What follows is a primer on key U.S. government authorities that have been, or could be, used to curb the flow of technology to and from China. It seeks to outline, in a slightly simplified form, the most important legal authorities. It describes which agencies are involved, what discretion they have, and how the Chinese tech sector has been targeted in recent years.[18]

Table 3: Washington's Large and Growing Tool Kit of Technology Restrictions

	Pre-2017 Authorities	Major China-Related Developments Since 2017
Export Controls	• International Traffic in Arms Regulations (including U.S. Munitions List) • Export Administration Regulations (including Commerce Control List, Entity List, deemed export restrictions, foreign direct product and de minimis rules)	• Export Control Reform Act mandated emerging and foundational technology controls • Military end user (MEU)/end use restrictions tightened and MEU List created • Entity List greatly expanded • Foreign direct product rule tightened for Huawei • Civilian exception rescinded • Hong Kong's preferential treatment ended

	Pre-2017 Authorities	Major China-Related Developments Since 2017
Investment Restrictions	• Committee on Foreign Investment in the United States (CFIUS)	• CFIUS activity increased • Foreign Investment Risk Review Modernization Act passed • Non-SDN Chinese Military-Industrial Complex Companies List created • Holding Foreign Companies Accountable Act passed
Telecoms Licensing and Equipment Authorizations	• Carrier public interest certificate • Submarine cable landing licensing • Radio frequency equipment authorization (technically based)	• Secure and Trusted Communications Networks Act created the FCC's Covered List • Team Telecom formalized • Chinese carrier and cable landing licenses denied or revoked • Secure Equipment Act barred radio frequency equipment on national security grounds
Visa Restrictions	• Section 212(a)(3)(C) of the Immigration and Nationality Act (INA) • Section 212(f) of the INA	• Visa ban instituted for graduate students and researchers tied to military-civil fusion • Certain Huawei employees barred • Chinese Communist Party members restricted
Import Restrictions	• Antidumping duties • Countervailing duties • Section 337 of the Tariff Act of 1930	• Broad-based tariffs imposed under a revived Section 301 of the Trade Act of 1974 • Steel and aluminum tariffs imposed under a revived Section 232(b) of the Trade Expansion Act • DJI drones and Hytera radios excluded (the former later rescinded) • Xinjiang-made goods presumptively banned
Financial Sanctions	• International Emergency Economic Powers Act and National Emergencies Act • Specially Designated Nationals (SDN) List • Global Magnitsky Act	• Chinese actors placed on SDN list for human rights abuses, corruption, and Hong Kong repression • U.S. Innovation and Competition Act passed Senate (would mandate further sanctions on Chinese actors)
Technology Transaction Rules	• International Emergency Economic Powers Act and National Emergencies Act	• "App bans" attempted on TikTok, WeChat, and others (later rescinded) • Bulk power system order instituted (later rescinded) • Information and communications technology or services (ICTS) supply chain security rule enacted
Federal Use and Spending Restrictions	• Various	• Drone use and purchase restricted • Section 889 of the 2019 National Defense Authorization Act restricted government and contractor use of Chinese tech • "Remove and replace" rule enacted
Law Enforcement	• Federal investigation and prosecution	• China Initiative announced (later ended) • Nontraditional collector cases prosecuted

EXPORT CONTROLS

U.S. export controls restrict the transfer of sensitive goods, services, and data to foreign countries. There are multiple, overlaying export control regimes administered by different federal agencies with distinct legal authorities. In general, controls can target the item being exported (as in "list-based" controls), the country an item is being sent to (as in economic embargoes), an item's ultimate recipient (as in end-user or end-use controls), or some combination. Export controls vary in their restrictiveness, from total bans to permissive licensing processes. The government's criteria for granting or denying licenses is a key determinant of an export control's practical impact, though such criteria are often opaque to the public.[19]

U.S. law requires that export controls be justified on national security grounds. However, "national security" might conceivably include an economic component.

U.S. law requires that export controls be justified on national security and foreign policy grounds.[20] Common rationales for export controls include maintenance of U.S. military superiority, nonproliferation of WMDs, and promotion of human rights. However, the concept of "national security" is subject to interpretation and might conceivably include an economic component. For example, the **Export Control Reform Act (ECRA)** of 2018 proclaims that U.S. national security "requires that the United States maintain its leadership in the science, technology, engineering, and manufacturing sectors, including foundational technology that is essential to innovation," and that "such leadership requires that United States persons are competitive in global markets."[21] Congress passed ECRA in large part due to concerns about Chinese technological advancement.[22]

For military items, the primary export control regime is the **International Traffic in Arms Regulations (ITAR)**, administered by the Department of State. ITAR includes a list-based control called the **U.S. Munitions List (USML)**. Despite its name, the USML encompasses a great deal beyond munitions, including military electronics, military cryptographic systems, electronic intelligence systems such as offensive cyber capabilities, and a variety of technical data.[23] The current list reflects a ten-year effort by the State Department to de-list "less sensitive items" and transfer them to more permissive regulatory regimes.[24] The USML is now meant to cover only "those items that provide the United States with a critical military or intelligence advantage or, in the case of weapons, perform an inherently military function."[25] Nothing on the USML may be exported to China.[26] And in 2020, then president Donald Trump ordered that Hong Kong be treated as part of China under U.S. export control (and other) laws—effectively barring the transshipment of USML items through this global trading hub and port city.[27]

Civilian, dual-use, and less sensitive military items are governed by the **Export Administration Regulations (EAR)**, which the Department of Commerce administers.[28]

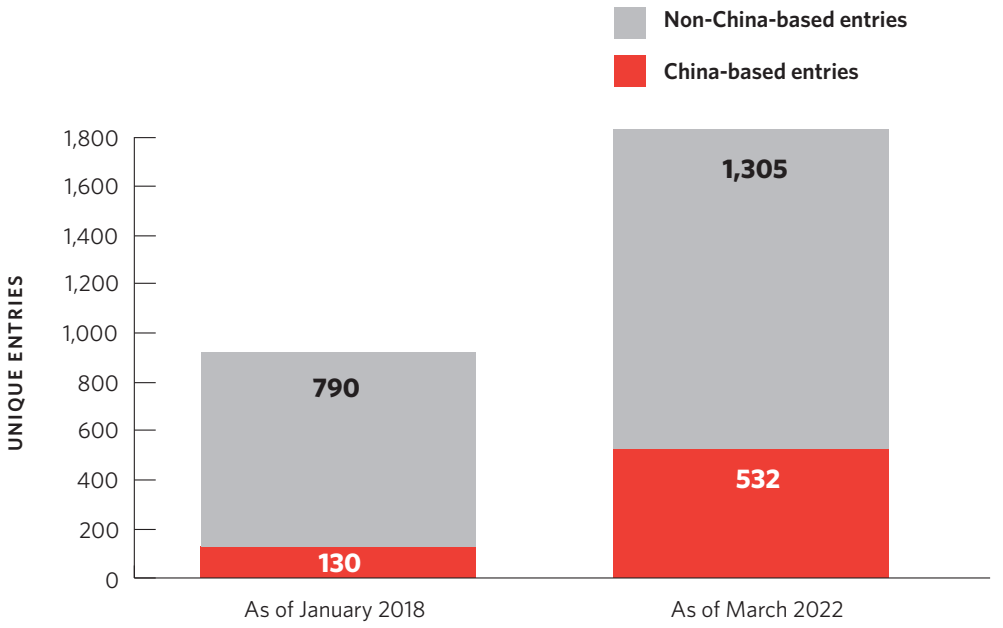
The EAR has multiple components, including a list-based regime called the **Commerce Control List (CCL)**. Each item on the CCL has one or more "reasons for control" that explain the listing's justification and determine which countries it affects. Relatively few reasons for control apply to Canada, for example—only those based on chemical and biological weapons nonproliferation or the Inter-American Firearms Convention. China, by contrast, is subject to a variety of control categories, including those tied to regional stability, missile proliferation, policing abuses, and broad national security concerns.[29] The CCL contains—among many other items—certain software, technology, and manufacturing equipment used to design and produce semiconductors, some of which requires a license to be exported to China.[30]

The Commerce Department says that "generally, the licensing policy for China is to approve items for civil end use to civil end users."[31] However, differentiating civil from military (or dual-use) applications in China is no simple matter. Consider the EAR rule, adopted in 2020, that restricts certain exports—including "low-level electronics" and "mass market encryption hardware and software (such as laptops and smartphones)"—destined for Chinese **"military end uses" and "military end users."**[32] The latter category includes "any person or entity whose actions or functions *are intended to support* 'military end uses.'"[33] The nature and extent of such support, and its relationship to the exported item, are not explicitly defined. Thus, under a strict reading of this language, U.S. companies might need to obtain a license before "supplying non-sensitive, broadly available items to Chinese companies for civilian applications" if those Chinese companies also happen to do business, however little, with the People's Liberation Army (PLA) or its affiliates.[34] The Commerce Department publishes a **Military End User (MEU) List** to aid in due diligence, but it is nonexhaustive, meaning that a recipient's absence from the list provides no guarantee that an export would be legal.[35] As of yet, the MEU List does not include any well-known Chinese commercial technology firms.

The Export Control Reform Act also calls for an effort to identify and control **"emerging and foundational technologies"** that "are essential to the national security of the United States."[36] Congress drafted this provision in large part to prevent China from gaining early access to potentially important U.S. technology. However, the executive branch has struggled to define a set of "emerging and foundational technologies" that warrant export controls yet are not already subject to them. The Trump administration initially considered controls on a wide swath of "emerging" tech areas prioritized by Beijing's Made in China 2025 plan, including genetic engineering, AI, additive manufacturing, robotics, and advanced materials.[37] But U.S. businesses and universities pushed back hard against the notion of controlling such broad and commercially important categories. As a result, the Commerce Department opted to impose only a few narrow controls related to chemical and biological weapons development, high-end semiconductor manufacturing, and advanced digital forensics and lawful intercept.[38]

The Commerce Department also administers the **Entity List**, an end-user-based control that targets foreign companies and other entities involved in "activities contrary to the national security or foreign policy interests of the United States."[39] Designated entities can be barred from importing any items "subject to the EAR" (including almost any U.S.-origin product); the exporter must first obtain a license, which may be subject to presumptive denial.[40] China has been a growing focus of the Entity List (see Figure 1). The number of unique China-based entries has quadrupled since 2018, from 130 to 532.[41] Four years ago, China comprised only 14 percent of the Entity List; today, it accounts for 29 percent. Nearly half of the Entity List's overall growth during that period came from new Chinese entries. The list now includes many of China's leaders in areas such as telecommunications (Huawei), AI (SenseTime, Megvii, iFLYTEK), semiconductors (SMIC, HiSilicon, Phytium), digital cameras (Hikvision, Dahua), drones (DJI), cybersecurity (Qihoo 360), and supercomputers (China's National Supercomputing Centers). These tech leaders were generally cited for supporting China's human rights violations—particularly in Xinjiang—or its military advancement.

Figure 1: The Entity List Is Increasingly Focused on China



Source: Author's analysis of the Commerce Department's Entity List spreadsheet available at https://www.bis.doc.gov/index.php/documents/consolidated-entity-list/1072-el-2.

Note: China figures include Hong Kong. Entries with exact duplicate names were excluded, but entries for close variations of names, aliases, subsidiaries, and affiliates were included. Undated entries were assumed to predate 2018.

The EAR mainly governs U.S.-origin items—whether exported from the United States, re-exported from one foreign country to another, or transferred within a foreign country.[42] But the regulations also cover some foreign-origin goods that have a nexus with controlled U.S. material. Two kinds of foreign products are deemed "subject to the EAR," which means they cannot be re-exported to companies on the Entity List without a license. The first kind is foreign items that incorporate, or are comingled with, a threshold amount of controlled U.S.-origin content.[43] For re-exports to China and most other countries, the usual **"de minimis"** threshold is 25 percent of an item's fair market value. In other words, a Japanese computer costing $1,000 could not be re-exported to SenseTime if it contained more than $250 worth of controlled U.S. components.

The second category is so-called **foreign-produced direct products**—items that may not actually contain any controlled U.S. tech but were nonetheless designed or manufactured with the assistance of such tech.[44] Traditionally, this rule covered only those foreign products deriving from a particular subset of controlled U.S. technologies: those placed on the CCL for "national security" reasons (as opposed to "anti-terrorism," "regional stability," and other rationales).[45] But in 2020, the Trump administration created a harsher version of the rule for select companies on the Entity List—namely, Huawei and more than 150 of its affiliates.[46] These companies, designated with **"footnote 1,"** need permission from the Commerce Department to import foreign semiconductor designs and finished chips (among other items) based partly on U.S. technology.[47] Because the United States "maintains a significant leadership position in [semiconductor design] software and in some segments of semiconductor manufacturing tools," this amounts to a broad-based ban.[48] Licenses are available: the Trump and Biden administrations have both allowed Huawei to continue receiving billions of dollars of less-sensitive U.S.- and foreign-origin semiconductors and other goods.[49] However, any chips destined for use in Huawei's 5G systems are presumptively denied.[50]

The Trump administration created a harsher version of the foreign-produced direct product rule for Huawei and more than 150 of its affiliates.

U.S. controls are not only concerned with exports to foreign countries; they also restrict so-called **deemed exports** to foreign *citizens*, even those lawfully living and working in the United States. This rule means that some U.S. firms—including many in the semiconductor and telecommunications sectors—must apply for a license to employ foreign workers in certain technical roles, depending on their nationality and the controlled technology at issue.[51] Prior to 2020, foreigners without military affiliations were exempt from this requirement; however, the Trump administration eliminated this exemption.[52] China has been by far the biggest supplier of foreign workers subject to deemed export rules: it accounted for 44 percent of approved deemed exports between 2015 and 2019.[53]

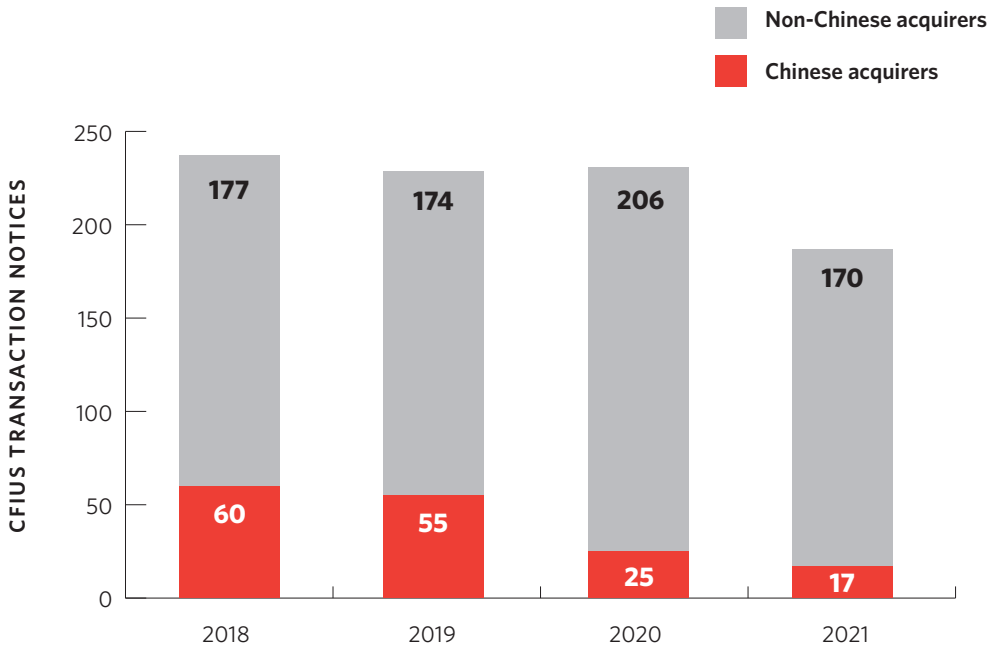
INVESTMENT RESTRICTIONS

U.S. national security agencies can impose restrictions on inbound investments (foreigners investing in U.S. companies) as well as outbound investments (Americans investing in foreign companies).[54] For inbound investments, the primary regulatory mechanism is the **Committee on Foreign Investment in the United States (CFIUS)**, an interagency body chaired by the treasury secretary. CFIUS—or in rare cases, the president—can block transactions that "[threaten] to impair the national security of the United States."[55] In general, CFIUS can review only those transactions where a foreigner would acquire dominant control over a business with U.S. operations. However, the **Foreign Investment Risk Review Modernization Act (FIRRMA)** of 2018 broadened CFIUS's jurisdiction over transactions involving **"critical technology," "critical infrastructure," or "sensitive personal data."**[56] For these, CFIUS can block even noncontrolling stakes that would nevertheless entitle foreign investors to access key information or influence corporate decisionmaking.[57] FIRRMA, like ECRA, was principally intended to limit China's access to U.S. technology.[58]

CFIUS has become more active in recent years as Washington has grown increasingly concerned with the national security risks of foreign investment and Congress has provided the body with new resources and authorities. Since 2017, more companies have had to notify CFIUS of covered transactions and to submit to CFIUS investigations; many have ultimately backed out of business deals amid CFIUS scrutiny.[59] CFIUS has blocked Chinese acquirers from buying several U.S. tech companies, including Grindr (a dating app) and PatientsLikeMe (a healthcare social network) in 2019 and Stayntouch (a hotel management platform) in 2020.[60] A CFIUS investigation also preceded Trump's 2020 executive order requiring ByteDance to sell TikTok.[61] CFIUS also stopped Ant Financial, a fintech affiliate of Alibaba, from buying MoneyGram in 2018.[62] Meanwhile, Chinese investors have become less interested in transactions that involve notifying CFIUS (see Figure 2). They submitted just seventeen notices (9 percent of the global total) in 2020, down from sixty (25 percent) in 2017.[63] Heightened CFIUS scrutiny is probably one of multiple factors at play; Chinese foreign direct investment in the United States fell across the board during this period.[64]

There is no body like CFIUS that systemically reviews Americans' outbound investments for national security risks—though Congress and the Biden administration are actively exploring the idea.[65] For now, outbound investments are subject to a few, narrowly defined restrictions. A 2021 executive order by Biden prohibits Americans from trading securities of any company designated by the Department of the Treasury as operating in "the defense and related materiel sector or the surveillance technology sector of the economy of the PRC [People's Republic of China]."[66] This **Non-SDN Chinese Military-Industrial Complex Companies List**—so named to differentiate it from the Treasury Department's Specially Designated Nationals list, described later—currently cites sixty-eight Chinese companies, including tech firms like Huawei, Hikvision, SenseTime, DJI, Megvii, SMIC,

Figure 2: Chinese Acquirers Are Submitting Fewer CFIUS Notices



Sources: "Annual Report to Congress for CY 2020," CFIUS, July 2021, https://home.treasury.gov/system/files/206/CFIUS-Public-Annual-Report-CY-2020.pdf; and "Annual Report to Congress for CY 2019," CFIUS, July 2020, https://home.treasury.gov/system/files/206/CFIUS-Public-Annual-Report-CY-2019.pdf.

China Telecom, China Unicom, and China Mobile.[67] It replaced a very similar list, created by the Trump administration, that was maintained by the Department of Defense (DOD) and did not cover surveillance technology.[68]

While outbound investment limits are currently narrow, pending regulations of U.S. stock exchanges may further diminish Americans' practical opportunities to invest in Chinese tech firms (and other Chinese companies). The **Holding Foreign Companies Accountable Act**, passed in December 2020, takes aim at publicly traded companies whose financial statements cannot be adequately inspected or investigated by U.S. authorities due to foreign government obstruction.[69] China has long hindered U.S. accounting oversight; in fact, it is the only country currently classified as doing so by the Public Company Accounting Oversight Board, a congressionally chartered nonprofit.[70] The new law essentially gives China three years to come into compliance with U.S. accounting transparency standards. If it fails to do so, the Securities and Exchange Commission (SEC) must order the de-listing of Chinese companies from U.S. stock exchanges and bar other ways of trading their securities, like over-the-counter sales. There are currently about 225 U.S.-listed Chinese companies, including tech giants such as Alibaba, JD.com, Baidu, and Weibo, plus a smaller

number of firms traded over-the-counter, like Tencent and Kingsoft.[71] SEC Chairman Gary Gensler recently warned that "the clock is ticking."[72] In fact, bills to accelerate the delisting timeline by one year have already passed the Senate and been endorsed by House leadership.[73]

TELECOMMUNICATIONS LICENSING AND EQUIPMENT AUTHORIZATIONS

Federal law gives the U.S. government several tools to restrict foreign involvement in domestic telecommunications. Any international carrier wishing to operate in the United States must first receive a **"public interest" certificate** from the Federal Communications Commission (FCC).[74] In weighing the public interest, the FCC considers factors such as "national security, law enforcement, foreign policy, or trade policy concerns related to the applicant's or authorization holder's reportable foreign ownership."[75] Submarine cable landings likewise require an FCC license, which can be denied in order to "promote the security of the United States."[76]

Although the FCC is an independent agency overseen by Congress, it "has sought the expertise of the relevant Executive Branch agencies for over 20 years, and has accorded deference to their expertise when they have identified . . . a concern in a particular application."[77] National security agencies convey their views on FCC licensing decisions through a forum known as **Team Telecom**, now formally called the **Committee for the Assessment of Foreign Participation in the United States Telecommunications Services Sector**, chaired by the attorney general.[78] Team Telecom's roles, responsibilities, and procedures were formalized in 2020, reflecting how national security has become increasingly central to FCC licensing decisions.

Team Telecom's formalization reflects how national security has become increasingly central to FCC licensing decisions, particularly those involving China.

Since 2019, Team Telecom has successfully spurred the FCC to crack down on Chinese entities seen as "vulnerable to exploitation, influence, and control by the Chinese government."[79] The FCC has cited these concerns to deny China Mobile's application for a carrier license and to revoke the licenses of China Telecom, China Unicom, and the Chinese firms Pacific Networks and ComNet.[80] Team Telecom also recommended that the FCC deny permission for Pacific Light Cable Network System, a Chinese company, to lay an undersea cable between Hong Kong and the United States in partnership with Google and Facebook.[81] The application was then withdrawn, as was another application for a U.S.–Hong Kong cable to be built by Facebook, Amazon, and China Mobile.[82]

Beyond telecommunications, the FCC also regulates radio frequency devices—an enormous category that includes "almost all electronic-electrical products" sold to businesses and consumers.[83] Radio frequency devices must receive an **equipment authorization**, or qualify for an exemption, to be imported or marketed in the United States, and such decisions have long been based on technical criteria alone.[84] In June 2021, however, the FCC unanimously voted to invite public comment on a proposal to incorporate national security considerations.[85] It cited statutory and regulatory provisions allowing the commission to consider "the public interest" in making authorization decisions.[86]

Pending national security rules will lead to a virtual U.S. ban on new electronics made by certain companies—almost all Chinese.

The FCC proposed to deny authorizations and exemptions—and potentially revoke existing approvals—for equipment made by companies on its **Covered List**. This list, created by the **Secure and Trusted Communications Networks Act** of 2019, initially contained just five companies (all Chinese): Huawei, ZTE, Hytera, Hikvision, and Dahua.[87] Congress mandated the inclusion of these companies, plus any other entity that the executive branch later determines "poses unacceptable risk to the national security of the United States or the security and safety of United States persons."[88] The FCC's pending equipment authorization rules will lead to a virtual ban on new electronics made by Covered List companies. Although formal rulemaking is still underway, Biden in November signed the **Secure Equipment Act**, which compels the FCC to adopt the core of its proposed rule and thus renders public comments somewhat irrelevant.[89]

In March 2022, the FCC expanded the Covered List beyond the original five companies mandated by Congress. It added China Mobile, China Telecom, and Kaspersky Lab (a Russian cybersecurity firm).[90] Kaspersky, the only non-Chinese company on the list, was most likely targeted due to Russia's invasion of Ukraine. It is also the first software company to be listed, indicating the Covered List has broadened in scope and could come to include Chinese software companies as well. The FCC has promised that it will continue to list more companies as needed. One FCC commissioner has already proposed adding DJI, calling it "Huawei on wings."[91] Such a move could force DJI—by far the dominant drone-seller in the United States and globally—to exit the U.S. market.

VISA RESTRICTIONS

The U.S. government has the discretion to bar noncitizens from entering the country if they are deemed to be national security threats. It can do so for specific individuals or entire classes of people. One mechanism is **Section 212(a)(3)(C)** of the Immigration and Nationality Act (INA), which allows the secretary of state to exclude any noncitizen whose

presence "would have potentially serious adverse foreign policy consequences for the United States."[92] The State Department cited this provision in 2020 to deny entry for "certain employees of Chinese technology companies," including Huawei, "that provide material support to regimes engaging in human rights abuses globally."[93]

Another powerful tool is the INA's **Section 212(f)**, which can be used to ban broad categories of foreigners. It allows presidents to exclude "all aliens or any class of aliens" whose entry "would be detrimental to the interests of the United States."[94] Every president since Ronald Reagan has used this authority at least once; Donald Trump used it particularly often.[95] In May 2020, Trump suspended entry of all foreign graduate students and researchers with past or present ties to "an entity in the PRC that implements or supports the PRC's 'military-civil fusion strategy.'"[96] This policy, which Biden retained, has so far led to the revocation of more than 1,000 visas and the denial of at least 700 to 1,300 visa applications.[97] Georgetown's Center for Security and Emerging Technology estimated that 3,000 to 5,000 Chinese students and researchers in science, technology, engineering, and mathematics (STEM) could be excluded annually.[98]

Other policy tools can be used to limit foreigners' opportunities to visit, study, and work in the United States without banning their entry outright.[99] For example, the Trump administration proposed new regulations to shorten the length of **F-1 (student) visas**[100] and to increase the minimum wages that employers would need to pay **H1-B (specialty occupation) visa** holders.[101] Trump also signed an executive order temporarily suspending issuance of new H1-B visas to applicants outside of the United States during the COVID-19 pandemic.[102] While none of these moves specifically targeted China, Chinese students and workers were among the largest groups affected.[103] (Biden later suspended or rescinded these policies.[104]) Trump also restricted Chinese Communist Party members and their families to single-entry visas valid for one month, whereas other Chinese people can obtain multiple-entry visas lasting up to ten years; Biden has kept this policy.[105]

IMPORT RESTRICTIONS

U.S. domestic law authorizes tariffs, duties, taxes, quotas, exclusions, and other import restrictions under certain circumstances. The lead agency is the Commerce Department, which investigates unfair foreign practices alleged by U.S. industry (or more rarely, launches self-initiated probes) and can impose import restrictions as a remedy.[106] If Commerce finds that imported goods are being sold "at less than [their] fair value," then it can impose **antidumping duties** to negate the predatory price cuts.[107] If the imported goods have been subsidized by a foreign government, then the department can levy **countervailing duties** equal to the value of the subsidies.[108] China has long been a top target of both antidumping and countervailing duties, though typically on raw materials and other commodities (not finished technology products).[109]

Antidumping and countervailing duties require the consent of the U.S. International Trade Commission (USITC)—an independent, nonpartisan, quasi-judicial body.[110] The USITC must find that "an [existing] industry in the United States is materially injured, or is threatened with material injury" by the wrongful dumping or subsidy, or that "the [future] establishment of an industry in the United States is materially retarded."[111] The USITC also has its own separate authority, under **Section 337** of the Tariff Act of 1930, to investigate "unfair methods of competition and unfair acts" by foreign entities.[112] Section 337 investigations tend to focus on intellectual property violations, the main problems singled out in the statutory text. If a foreign product is shown to violate a U.S. patent, copyright, trademark, or other intellectual property protection, then the USITC can ban its importation or sale. Since 2018, the USITC has blocked the importation of some two-way radios made by Hytera because they violated Motorola's patents.[113] Hytera had apparently poached employees from Motorola and directed them to steal large amounts of design data before leaving their former company. (The Justice Department later indicted Hytera for conspiracy to commit trade secret theft.[114]) In 2020, the USITC ordered the exclusion of several popular DJI drone models that it found had infringed a U.S. patent held by Autel Robotics USA, the American subsidiary of a Chinese company.[115] However, the order was paused and eventually rescinded after DJI and Autel reached a settlement in related litigation.[116]

USTR imposed tariffs on most imports from China in response to Beijing's forced tech transfer, discriminatory licensing, strategic foreign investments, and cyber-enabled IP theft.

Antidumping duties and countervailing duties have a long, bipartisan pedigree and are specifically sanctioned by the World Trade Organization (WTO).[117] (Section 337 is less commonly employed and has garnered occasional complaints from U.S. trading partners.[118]) But the Trump administration sought even more powerful trade weapons.[119] It therefore dusted off several controversial statutes that had fallen into disuse during the WTO era.[120] One of these was **Section 301** of the Trade Act of 1974, which enables the U.S. Trade Representative (USTR) to investigate trade agreement violations or any other foreign "act, policy, or practice" that "burdens or restricts United States commerce" and is "unjustifiable," "unreasonable," or "discriminatory."[121] If it finds fault, USTR has broad discretion to institute retaliatory measures against the offending country. These measures—unlike antidumping and countervailing duties or Section 337 exclusions—can target "any goods or economic sector . . . without regard to whether or not [they] were involved in the act, policy, or practice" being investigated.[122]

In 2017, Trump ordered USTR to launch a Section 301 investigation into Chinese practices "that may be harming American intellectual property rights, innovation, or technology development."[123] USTR found China responsible for numerous unfair practices, including forced technology transfer, discriminatory licensing, strategic foreign investments, and

cyber-enabled intellectual property theft.[124] Based on these findings, USTR eventually imposed tariffs of 10 percent to 25 percent on the majority of U.S. imports from China.[125] Affected goods include some finished tech products (such as certain monitors and touch screens, industrial robots, and specialized cameras) and technology components (like integrated circuits, batteries, cooling fans, and disk drives), but not other major categories like cell phones, laptops, or video game consoles.[126] This was only the second time since 2001 that a new Section 301 investigation had led to unilateral U.S. trade restrictions.[127] The tariffs remain largely intact today, though the Biden administration is now considering narrow carve-outs for products only available from China.[128]

Trump also resurrected another moribund authority, **Section 232(b)** of the Trade Expansion Act of 1962, which had not been used since 2001.[129] This provision enables the Commerce Department to investigate whether "an article is being imported into the United States in such quantities or under such circumstances as to threaten to impair the national security."[130] If a national security threat exists, Commerce can remedy the threat by "tak[ing] action to adjust imports." (There need not be any finding of unfair foreign practices.) Notably, the statute "recognize[s] the close relation of the economic welfare of the Nation to our national security," opening the door for economically motivated import restrictions.[131] In 2017, Trump ordered the department to self-initiate Section 232(b) investigations of steel and aluminum.[132] The investigations led to new steel and aluminum tariffs on China and several other countries.[133] So far, Section 232(b) has not been used to target Chinese technology.

In addition to these economic- and national security–oriented statutes, U.S. law has long prohibited the import of goods made with forced labor.[134] Since 2018, Customs and Border Protection (CBP) has steadily ramped up enforcement against Chinese-origin items made by Uyghur detainees.[135] CBP has issued several **Withhold Release Orders** to ban computer parts, silica-based products used in solar panels and electronics, and various non-tech goods from specified companies operating in Xinjiang.[136] Dissatisfied with this piecemeal approach, Congress passed the **Uyghur Forced Labor Prevention Act**, which Biden signed in December 2021. It creates a rebuttable presumption that all Xinjiang-made goods are products of forced labor and therefore cannot be imported.[137]

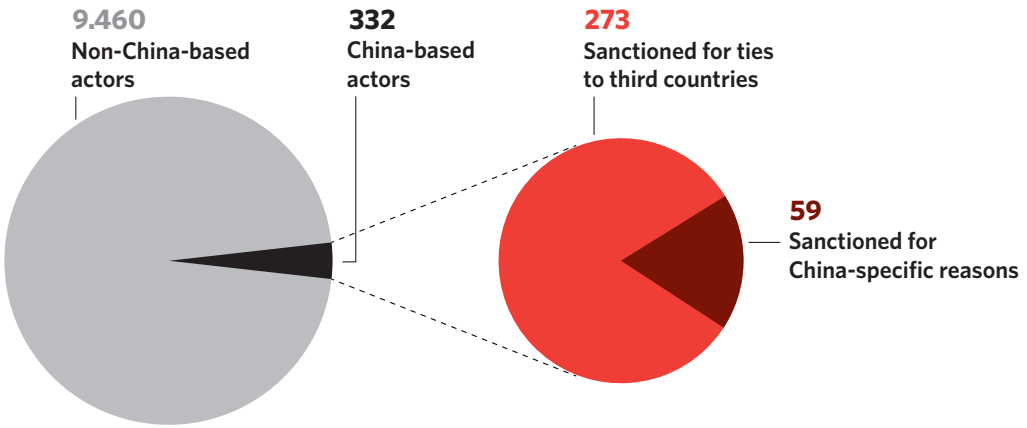
FINANCIAL SANCTIONS

Dozens of U.S. government programs authorize financial sanctions on foreign individuals and entities.[138] Congress created some of these programs, but most were fashioned by presidents using the **International Emergency Economic Powers Act (IEEPA)**.[139] IEEPA allows the president to declare a "national emergency" regarding "any unusual and extraordinary [foreign] threat . . . to the national security, foreign policy, or economy of the United States."[140] The president may then "deal with" the threat by blocking some or all financial activities of designated actors—for example, freezing their assets and barring them from

receiving any money or property.[141] Presidents have declared seventy-four national emergencies since 1979, with forty still in effect.[142] (Emergencies must be renewed annually and comply with other procedural requirements in the **National Emergencies Act**.[143])

After a sanctions program has been established, the power to designate specific actors is typically delegated to the Treasury Department. Those subject to the harshest sanctions are placed on Treasury's **Specially Designated Nationals (SDN) List**.[144] A review of this list shows that China has been sparingly targeted by U.S. financial sanctions to date (see Figure 3). The SDN List includes 332 China-based actors, about 3 percent of the global total (9,792).[145] Moreover, these China-based actors were generally not sanctioned for China-specific reasons, such as involvement with Beijing's domestic human rights abuses.[146] Rather, most were punished for their dealings with North Korea, Iran, and other sanctioned nations. For example, the Chinese state-owned enterprise CEIEC (China National Electronics Import & Export Corporation) was designated in 2020 for helping undermine democracy in Venezuela by "supporting the Maduro regime's malicious cyber efforts" and providing "a commercialized version of China's 'Great Firewall.'"[147]

Figure 3: The SDN List Rarely Targets China or Cites China-Specific Rationales



Source: Author's analysis of the Treasury Department's Sanctions List Search and SDN spreadsheet, available at https://sanctionssearch.ofac.treas.gov/ and https://home.treasury.gov/policy-issues/financial-sanctions/specially-designated-nationals-list-data-formats-data-schemas (primary names), as of March 27, 2022.

Note: Entries with exact duplicate names were excluded, but entries with close variations of names, aliases, subsidiaries, and affiliates were included. "China" here refers to mainland China, Hong Kong, and Macau. China-based actors include some third-country entities that maintain a presence in China. China-specific reasons mean human rights abuses and corruption (Executive Order 13818) and Hong Kong repression (Executive Order 13936).

Two relatively new sanctions programs have been used to target Chinese government officials and entities for their domestic abuses, suggesting that China could become a more explicit focus of U.S. financial sanctions over time. In 2017, Trump declared that "serious human rights abuse and corruption around the world" constituted a national emergency, invoking IEEPA and the **Global Magnitsky Act**.[148] Seventeen Chinese individuals and organizations have been designated under this authority (mostly for activities in Xinjiang), and many more could be targeted in the future—including people or companies that provide "technological support" to Chinese human rights abuses.[149] (The **Uyghur Human Rights Policy Act** of 2020 and the **Uyghur Forced Labor Prevention Act** of 2021 call for additional Xinjiang-related sanctions to be imposed.[150]) Trump created another new authority in 2020 to punish the suppression of Hong Kong's autonomy, democracy, and human rights, including online censorship; forty-two local and national Chinese officials have since been designated on that basis.[151]

The draft **U.S. Innovation and Competition Act**, recently passed by the Senate, further suggests the likelihood of additional financial sanctions targeting China and its technology ecosystem. Identifying "sanctions and other restrictions" as "[central] to strategic competition with China," the bill criticizes the executive branch for not sufficiently utilizing the "broad range of tough authorities" provided by Congress.[152] It demands SDN List designation and/or other harsh sanctions for foreign actors found to be supporting trade secret theft or Chinese government efforts to "undermin[e] cybersecurity."[153] The equivalent House bill, the **America COMPETES Act**, contains no similar provisions.[154]

TECHNOLOGY TRANSACTION RULES

The breadth and flexibility of executive powers can permit U.S. administrations to apply existing authorities in novel ways, sometimes spinning up whole new regulatory regimes without the need for further legislation. The Trump administration did this on several occasions. Leveraging IEEPA's power to restrict "transactions," Trump debuted new kinds of restrictions that operated differently from the SDN List—including what is now called the Non-SDN Chinese Military-Industrial Complex Companies List. This tool, described earlier, allows the U.S. government to ban outbound investments in certain Chinese firms while stopping short of a full asset freeze.

One of Trump's most high-profile innovations was his attempted **"app bans"** of TikTok and WeChat.[155] To impose these bans, Trump declared that "the unrestricted acquisition or use in the United States of information and communications technology or services" (ICTS) associated with

The breadth and flexibility of executive powers can permit U.S. administrations to spin up whole new regulatory regimes without the need for further legislation.

The ICTS supply chain security rule establishes a CFIUS-like mechanism for federal government review of almost any large-scale use of Chinese ICTS in the United States.

"foreign adversaries" constituted a national emergency.[156] His Commerce Department then issued rules to block app stores, hosting services, content delivery networks, and peering services from supporting these two apps—effectively banning them in the United States.[157] Trump later sought to ban AliPay, Tencent QQ, and six other Chinese apps as well.[158] But no app ban was ever enforced. Federal courts enjoined the TikTok and WeChat bans; Trump left office before detailed rules on the others could be published; and Biden wiped the slate clean.[159]

Mobile apps were not the only targets of Trump's novel technology restrictions. Relying on the same ICTS national emergency, he ordered U.S. **bulk power systems**, which are key elements of the electrical grid, to curb the use of equipment sourced from "foreign adversary" countries such as China.[160] Specifically, the Department of Energy barred Chinese equipment from being used in bulk power systems that serve military facilities "critical to the defense of the United States."[161] Biden paused implementation of this rule pending a review.[162]

More recently, the U.S. government has sought to replace such ad hoc restrictions with formalized regulatory structures. In March 2021, Biden allowed a major new regulation developed by the Trump administration to come into force. The **ICTS supply chain security rule** cites, once again, the national emergency regarding foreign adversary ICTS.[163] It establishes a CFIUS-like mechanism for federal government review of almost any large-scale use of Chinese ICTS in the United States. The Department of Commerce can block such transactions if they pose "undue or unacceptable risks."

Biden later issued an executive order outlining "a criteria-based decision framework and rigorous, evidence-based analysis" to help guide the rule's application to internet-connected software.[164] He told the Commerce Department to examine any links to adversarial military, intelligence, proliferation, or cyber activities, and to consider the quality of third-party auditing, the scope and sensitivity of data collected, the number and sensitivity of users, and any verifiable risk remediation measures, among other factors. The department has not yet taken any public enforcement action under the new authority, but multiple investigations are apparently under way. Commerce has issued subpoenas to unnamed Chinese companies, is reportedly investigating Alibaba's cloud business and DiDi, and is probably also reviewing at least some of the mobile apps that Trump sought to ban by executive order.[165]

FEDERAL USE AND SPENDING RESTRICTIONS

The federal government has increasingly acted to limit its own use of and financial support for certain Chinese technologies, although these actions are not a primary focus of this report. These efforts can have wider impacts due to the U.S. government's large purchasing power. **Drones**, for example, have been the target of several recent federal restrictions. The Defense Department suspended its purchase of all commercial drones in 2018 due to concerns about the security of Chinese products, and the next year, Congress permanently barred DOD from using any drones with Chinese components.[166] After the Department of the Interior grounded its entire drone fleet for similar reasons, Trump sought to institute government-wide restrictions on foreign drones.[167] Days before leaving office, he signed an executive order telling agencies not to buy drones whose key hardware, software, or data services come from "adversary countries" like China.[168]

Telecommunications and video surveillance equipment have also been subjects of recent China-related procurement restrictions. The National Defense Authorization Act for Fiscal Year 2019 included a provision—**Section 889**—prohibiting agencies from spending any federal funds on such equipment made by Huawei, ZTE, Hytera, Hikvision, and Dahua.[169] This government-wide blacklist may expand in the future; the law allows DOD to add other firms "connected to" the Chinese government. (Any additions would automatically be placed on the FCC's Covered List as well.[170])

As the U.S. government curbs its own direct purchase or use of Chinese technology, it has also imposed parallel restrictions on federal contractors and grantees, a much bigger universe. Section 889, which blacklists certain Chinese equipment within the federal government, separately bars agencies from *contracting with* entities that "use" such equipment—even if their "use" has no connection to the federal contract and involves an unrelated unit of the contractor's business.[171] More than 16,000 companies had federal prime contracts as of 2018, suggesting the wide reach of Section 889.[172] Similarly, the FCC has leveraged federal subsidies to discourage the private use of Chinese telecommunications equipment. It will subsidize carriers' efforts to **"remove and replace"** Huawei and ZTE equipment, while denying future subsidies for carriers who retain such equipment.[173] Although technically voluntary, this program operates as a de facto ban on Huawei and ZTE usage in the telecoms sector. Small and rural carriers cannot afford to lose federal funds, while large carriers already generally avoid Huawei and ZTE.[174]

LAW ENFORCEMENT

Outside the regulatory domain, federal law enforcement activities can also have the effect of restricting China's illicit (and licit) access to U.S. technology. From November 2018 to February 2022, the **China Initiative** was the Department of Justice's strategic campaign

to investigate and prosecute theft of trade secrets, espionage, foreign influence activities, supply chain subversion, and other threats from China. The Justice Department publicly categorized at least seventy-seven criminal cases against more than 150 defendants as part of the China Initiative, according to a database compiled by the *MIT Technology Review*.[175] However, the Justice Department had no official definition of a China Initiative case, and many of these cases would presumably still have been filed even without such an initiative. The most high-profile indictments charged Huawei and its chief financial officer, Meng Wanzhou, with theft of trade secrets and fraud.[176] Cases against other Chinese, American, and third-country nationals and companies alleged export control violations, hacking, economic and national security espionage, and failure to register as a foreign agent.[177] Many cases did not have an explicit connection to the Chinese government.[178]

The most controversial and arguably significant element of the China Initiative was the Justice Department's crackdown on what it called **"nontraditional collectors"** at U.S. universities. Fearing illicit transfer of technology and intellectual property, federal prosecutors charged about twenty U.S.-based Chinese and American researchers with hiding their ties to the Chinese government.[179] For example, multiple cases alleged that researchers applied for federal grants without disclosing their participation in Beijing's Thousand Talents Plan.

The crackdown led many Chinese researchers to leave the United States and made American academics more reluctant to collaborate with Chinese counterparts.[180] Critics called this a harmful chilling effect, but Justice Department officials (even well into the Biden administration) characterized it as successful deterrence.[181] Over time, some of the cases proved weak. Since 2021, the department has dropped charges against five Chinese researchers, dismissed its case against a China-born American academic, and failed to convict a Chinese Canadian professor.[182] It also secured some victories, such as the conviction of a high-profile American chemistry professor for hiding his ties to China.[183]

After a monthslong review, the Biden administration announced an end to the China Initiative in February 2022.[184] The change was partly cosmetic: the Justice Department's China-related work largely continues under different branding. Matt Olsen, assistant attorney general for national security, explained that the China Initiative label "helped give rise to a harmful perception that the department applies a lower standard to investigate and prosecute criminal conduct related to that country or that we in some way view people with racial, ethnic or familial ties to China differently." Although Olsen disputed this perception, he nevertheless announced one key policy change. "Cases involving academic integrity and research security" (formerly described by the more charged term "nontraditional collection") are now mainly handled as administrative matters by the federal agencies that fund research. Prosecutions of such cases will be rarer and require closer scrutiny from senior department officials.[185]

Table 4: Select Chinese Tech Companies Subject to Multiple U.S. Restrictions

	Huawei	ZTE	Hikvision	Hytera	Alibaba	Tencent	Dahua	China Telecom	China Mobile	DJI	ByteDance	Kingsoft	SenseTime	Megvii	SMIC	China Unicom	Fujian Jinhua
Non-SDN CMIC List	X		X					X	X	X			X	X	X	X	
Entity List	X	✶	X				X			X			X	X	X		X
Covered List	X	X	X	X			X	X	X								
Section 889 blacklist	X	X	X	X			X										
Federal indictment	X	X		X													X
App ban						✶					✶	✶					
ICTS supply chain security review					X	?					?	?					
FCC license denial/ revocation								X	X							X	
CFIUS action					X	†					X						
Stock exchange de-listing/over-the-counter ban					†	†						†					
Remove and replace rule	X	X															
Section 337				X						✶							
Foreign-produced direct product footnote 1	X																
Employee visa ban	X																

LEGEND

X = active **? = probable** **† = pending** **✶ = rescinded** Sources: U.S. government documents and press reports cited throughout this chapter.

Note: This table covers actions taken between January 1, 2017, and March 27, 2022. Alibaba here includes Ant Group, a closely related company.

IMPLICATIONS FOR U.S. STRATEGY

This overview of U.S. policy tools holds at least two important lessons for American strategists weighing the larger issues at stake in technological decoupling. First, Washington's restrictive powers are dizzyingly complex to administer, with authority fragmented across multiple agencies, statutes, and policy areas. It is therefore essential to articulate a government-wide strategy that can align these disparate elements into a coherent whole. Without such a strategy, different policy levers may operate out of sync, or even work at cross-purposes, based on agencies' divergent views of key goals and trade-offs.

Second, U.S. law gives the executive branch vast discretion to pursue a technological decoupling of its choosing. By interpreting pliable concepts like "national security" or "the public interest," U.S. officials can unlock an extraordinary range of powers to restrict the technology products, services, and inputs flowing between America and China. Most of these powers have only been used to a tiny fraction of their full potential. And Congress has been an eager partner—providing several new authorities and prodding administrations to act. Legally speaking, U.S. officials have a blank canvas on which to paint new restrictive measures and effect technological decoupling.[186] This is both an opportunity and a danger, as overreach becomes more likely in such circumstances.

All of the policy tools defined and explained above will be collectively referred to as "technology restrictions," "technology controls," or "defensive measures." The remainder of this report explores *which technologies* Washington should target with this general tool kit to reduce U.S.-China technological interdependence. Identifying the best tool or tools to use with each technology area is a topic for another paper.

3 See endnote 2 for a discussion of this term and how it relates to this report's scope.

4 A 2005 speech by then deputy secretary of state Robert Zoellick crystallized this viewpoint, which was already widely held and would continue to hold sway into the Obama administration. Robert B. Zoellick, "Whither China: From Membership to Responsibility?," State Department, September 21, 2005, https://2001-2009.state.gov/s/d/former/zoellick/rem/53682.htm.

5 Zoellick himself recognized these concerns in a 2019 speech, though he opposed the "logic of constant confrontation" that had come to characterize Washington's China policy. Robert B. Zoellick, "Can America and China Be Stakeholders?," Carnegie Endowment for International Peace, December 4, 2019, https://carnegieendowment.org/2019/12/04/can-america-and-china-be-stakeholders-pub-80510.

6 Jack Goldsmith and Stuart Russell, "Strengths Become Vulnerabilities: How a Digital World Disadvantages the United States in Its International Relations," June 5, 2018, Hoover Institution, Aegis Series Paper no. 1806, June 5, 2018, https://www.hoover.org/sites/default/files/research/docs/381100534-strengths-become-vulnerabilities.pdf.

7 For a notable executive branch action, see "President Obama Blocks Chinese Acquisition of Aixtron SE," Covington & Burling, December 5, 2016, https://www.cov.com/-/media/files/corporate/publications/2016/12/president_obama_blocks_chinese_acquisition_of_aixtron_se.pdf. In Congress, a 2012 committee report on Huawei and ZTE became a touchstone for future scrutiny of these companies and Chinese technology more generally. House Permanent Select Committee on Intelligence, *Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE*, October 8, 2021, https://republicans-intelligence.house.gov/sites/intelligence.house.gov/files/documents/huawei-zte%20investigative%20report%20(final).pdf.

8 Seth Center and Emma Bates, "Tech-Politik: Historical Perspectives on Innovation, Technology, and Strategic Competition," CSIS, December 19, 2019, https://www.csis.org/analysis/tech-politik-historical-perspectives-innovation-technology-and-strategic-competition.

9 James L. Schoff, "U.S.-Japan Technology Policy Coordination: Balancing Technonationalism With a Globalized World," Carnegie Endowment for International Peace, June 29, 2020, https://carnegieendowment.org/2020/06/29/u.s.-japan-technology-policy-coordination-balancing-technonationalism-with-globalized-world-pub-82176.

10 Adam Kline and Tim Hwang, "From Cold War Sanctions to Weaponized Interdependence: An Annotated Bibliography on Competition and Control Over Emerging Technologies," Center for Security and Emerging Technology, September 2021, https://cset.georgetown.edu/publication/from-cold-war-sanctions-to-weaponized-interdependence/.

11 Eric Zhu and Tom Orlik, "When Will China Rule the World? Maybe Never," *Bloomberg*, July 5, 2021, https://www.bloomberg.com/news/features/2021-07-05/when-will-china-s-economy-beat-the-u-s-to-become-no-1-why-it-may-never-happen; World Bank, "GDP (Current US$) - United States, China, Japan," https://data.worldbank.org/indicator/NY.GDP.MKTP.CD?locations=US-CN-JP; and Marc Trachtenberg, "Assessing Soviet Economic Performance During the Cold War: A Failure of Intelligence?," *Texas National Security Review* 1, no. 2 (2018), https://tnsr.org/2018/02/assessing-soviet-economic-performance-cold-war/.

12 "Population Total - China, Japan, United States," World Bank, https://data.worldbank.org/indicator/SP.POP.TOTL?locations=CN-JP-US; and Murray Feshbach, "The Soviet Union: Population Trends and Dilemmas," *Population Bulletin* 37, no. 3 (1982), https://pubmed.ncbi.nlm.nih.gov/12264357/.

13 Ellen Terrell, "When a Quote Is Not (Exactly) a Quote: General Motors," *Inside Adams* (blog), Library of Congress, April 22, 2016, https://blogs.loc.gov/inside_adams/2016/04/when-a-quote-is-not-exactly-a-quote-general-motors/.

14 John Chipman, "Why Your Company Needs a Foreign Policy," *Harvard Business Review*, September 2016, https://hbr.org/2016/09/why-your-company-needs-a-foreign-policy.

15 Jon Bateman, "National Security in an Age of Insurrection," Carnegie Endowment for International Peace, January 14, 2021, https://carnegieendowment.org/2021/01/14/national-security-in-age-of-insurrection-pub-83635.

16 David Forscey, Jon Bateman, Nick Beecroft, and Beau Woods, "Systemic Cyber Risk: A Primer," Carnegie Endowment for International Peace and Aspen Institute, March 7, 2022, https://carnegieendowment.org/2022/03/07/systemic-cyber-risk-primer-pub-86531.

17 Raj Varadarajan et al., "What's at Stake If the US and China Really Decouple," Boston Consulting Group, October 20, 2020, https://www.bcg.com/fr-ca/publications/2020/high-stakes-of-decoupling-us-and-china.

18 This primer is necessarily a snapshot in time, accurate as of March 27, 2022, unless stated otherwise. The U.S. government debuts new policy actions targeting Chinese technology on an almost weekly basis.

19 Federal regulations reveal some basic outlines of licensing policy, such as 15 C.F.R. § 742 for the CCL. However, they leave substantial room for interpretation.

20 50 U.S.C. § 4811.

21 50 U.S.C. § 4811(3).

22 Ian F. Fergusson and Karen M. Sutter, "U.S. Export Control Reforms and China: Issues for Congress," Congressional Research Service, January 15, 2021, https://sgp.fas.org/crs/natsec/IF11627.pdf.

23 22 C.F.R. § 121.1.

24 "International Traffic in Arms Regulations: U.S. Munitions List Categories I, II, and III," State Department, 85 Fed. Reg. 3819, (March 9, 2020), https://www.federalregister.gov/documents/2020/01/23/2020-00574/international-traffic-in-arms-regulations-us-munitions-list-categories-i-ii-and-iii.

25 "International Traffic in Arms Regulations: U.S. Munitions List Categories I, II, and III," State Department, 85 Fed. Reg. 3819, (March 9, 2020), https://www.federalregister.gov/documents/2020/01/23/2020-00574/international-traffic-in-arms-regulations-us-munitions-list-categories-i-ii-and-iii.

26 22 C.F.R. § 126.1(d)(1).

27 "2021 Hong Kong Policy Act Report," State Department, March 31, 2021, https://www.state.gov/2021-hong-kong-policy-act-report/.

28 15 C.F.R. § 730.3.

29 15 C.F.R. Supplement No. 1 to Part 738.

30 "Export Administration Regulations: Amendments to General Prohibition Three (Foreign-Produced Direct Product Rule) and the Entity List," Commerce Department, 85 Fed. Reg. 29,849 (March 19, 2020), https://www.federalregister.gov/documents/2020/05/19/2020-10856/export-administration-regulations-amendments-to-general-prohibition-three-foreign-produced-direct.

31 "China - Country Commercial Guide - U.S. Export Controls," U.S. International Trade Commission (USITC), September 14, 2021, https://www.trade.gov/knowledge-product/china-us-export-controls.

32 15 C.F.R. § 744.21; and John R. Shane and Lori E. Scheetz, "Commerce Department Further Restricts U.S. Exports to China, Russia, and Venezuela; Aims to Combat China's Military-Civil Fusion Strategy," Wiley, April 28, 2020, https://www.wiley.law/alert-Commerce-Department-Further-Restricts-U-S-Exports-to-China-Russia-and-Venezuela-Aims-to-Combat-China-s-Military-Civil-Fusion-Strategy.

33 Emphasis added. 15 C.F.R. § 744.21(g).

34 Sylwia A. Lis, Lise S. Test, and Maria Sergeyeva, "Commerce Tightens Restrictions on Technology Exports to Countries of Concern, in Particular China, Russia, and Venezuela," *Sanctions & Export Controls Update* (blog), Baker McKenzie, April 30, 2020, https://sanctionsnews.bakermckenzie.com/commerce-tightens-restrictions-on-technology-exports-to-countries-of-concern-in-particular-china-russia-and-venezuela/.

35 "Military End User (MEU) List," Commerce Department, https://www.bis.doc.gov/index.php/policy-guidance/lists-of-parties-of-concern/1770.

36 50 U.S.C. § 4817.

37 "Review of Controls for Certain Emerging Technologies," Commerce Department, 83 Fed. Reg. 58,201 (November 19, 2018), https://www.federalregister.gov/documents/2018/11/19/2018-25221/review-of-controls-for-certain-emerging-technologies; and Emma Rafaelof, "Unfinished Business: Export Control and Foreign Investment Reforms," U.S.-China Economic and Security Review Commission, June 1,

2021, https://www.uscc.gov/sites/default/files/2021-06/Unfinished_Business-Export_Control_and_Foreign_Investment_Reforms.pdf.

38 "New Controls on Emerging Technologies Released, While U.S. Commerce Department Comes Under Fire for Delay," Gibson Dunn, October 27, 2020, https://www.gibsondunn.com/new-controls-on-emerging-technologies-released-while-us-commerce-department-comes-under-fire-for-delay/.

39 15 C.F.R. § 744.16.

40 15 C.F.R. § 734.3.

41 As of March 27, 2022, based on author's analysis of the Commerce Department's Entity List spreadsheet available at https://www.bis.doc.gov/index.php/documents/consolidated-entity-list/1072-el-2. These figures include both China and Hong Kong. They exclude all entries with exact duplicate names; however, they include entries for close variations of names, aliases, subsidiaries, and affiliates. Undated entries were assumed to predate 2018.

42 15 C.F.R. § 734.3(a).

43 15 C.F.R. § 734.4.

44 15 C.F.R. § 736.2(b)(3).

45 Charles L. Capito, Panagiotis C. Bayz, and Joseph A. Benkert, "The Commerce Department Modifies 'Direct Product Rule' to Restrict Transfers of More Foreign-Made Items to Huawei," Morrison Foerster, May 28, 2020, https://www.mofo.com/resources/insights/200529-commerce-department-modifies.html.

46 "Addition of Huawei Non-U.S. Affiliates to the Entity List, the Removal of Temporary General License, and Amendments to General Prohibition Three (Foreign-Produced Direct Product Rule)," Commerce Department, 85 Fed. Reg. 51,596 (August 20, 2020), https://www.federalregister.gov/documents/2020/08/20/2020-18213/addition-of-huawei-non-us-affiliates-to-the-entity-list-the-removal-of-temporary-general-license-and; and "Export Administration Regulations: Amendments to General Prohibition Three (Foreign-Produced Direct Product Rule) and the Entity List," Commerce Department, 85 Fed. Reg. 29,849 (May 15, 2020), https://www.federalregister.gov/documents/2020/05/19/2020-10856/export-administration-regulations-amendments-to-general-prohibition-three-foreign-produced-direct.

47 15 C.F.R. § 736.2(e); 15 C.F.R. Supplement No. 4 to Part 744, footnote 1; and "Commerce Addresses Huawei's Efforts to Undermine Entity List, Restricts Products Designed and Produced With U.S. Technologies," press release, Commerce Department, May 15, 2020, https://2017-2021.commerce.gov/news/press-releases/2020/05/commerce-addresses-huaweis-efforts-undermine-entity-list-restricts.html; Kay C. Georgi, Marwa M. Hassoun, Sylvia G. Costelloe, and Aman Kakar, "BIS Expands the Huawei Foreign Direct Product Rule to Capture a Wide Swath of COTS Products," Arent Fox, August 19, 2020, https://www.arentfox.com/perspectives/alerts/bis-expands-the-huawei-foreign-direct-product-rule-capture-wide-swath-cots.

48 "Comments of the Semiconductor Industry Association (SIA) on Amendments to General Prohibition Three (Foreign-Produced Direct Product Rule) and the Entity List," Semiconductor Industry Association, July 14, 2020, https://www.semiconductors.org/wp-content/uploads/2020/07/SIA-Comments-on-Foreign-Direct-Product-July-14-2020.pdf.

49 "Export Control Licensing Decisions for Huawei (November 9, 2020-April 20, 2021)," Commerce Department, https://gop-foreignaffairs.house.gov/wp-content/uploads/2021/10/Huawei-Licensing-Information.pdf.

50 "Addition of Huawei Non-U.S. Affiliates to the Entity List, the Removal of Temporary General License, and Amendments to General Prohibition Three (Foreign-Produced Direct Product Rule)," Commerce Department, 85 Fed. Reg. 51,596 (August 20, 2020), https://www.federalregister.gov/documents/2020/08/20/2020-18213/addition-of-huawei-non-us-affiliates-to-the-entity-list-the-removal-of-temporary-general-license-and.

51 Evan Burke, "Trump-Era Policies Toward Chinese STEM Talent: A Need for Better Balance," Carnegie Endowment for International Peace, March 25, 2021, https://carnegieendowment.org/2021/03/25/trump-era-policies-toward-chinese-stem-talent-need-for-better-balance-pub-84137.

52 Evan Burke, "Trump-Era Policies Toward Chinese STEM Talent: A Need for Better Balance," Carnegie Endowment for International Peace, March 25, 2021, https://carnegieendowment.org/2021/03/25/trump-era-policies-toward-chinese-stem-talent-need-for-better-balance-pub-84137.

53 "2019 Statistical Analysis of BIS Licensing Deemed Export 2015-2019," Commerce Department, April 25, 2020, https://www.bis.doc.gov/index.php/country-papers/2648-2019-statistical-aalysis-of-bis-licensing-deemed-export-2015-2019/file.

54 What counts as an "American" or "foreign" investor or business is a complicated and increasingly contested legal question. For example, see Brandon L. Van Grack and James Brower, "CFIUS's Expanding Jurisdiction in the Magnachip Acquisition," Lawfare, October 11, 2021, https://www.lawfareblog.com/cfiuss-expanding-jurisdiction-magnachip-acquisition.

55 31 C.F.R. § 800.101, 800.601.

56 Farhad Jalinous, Karalyn Mildorf, Keith Schomig, and Ata Akiner, "CFIUS Finalizes New FIRRMA Regulations," White & Case, https://www.whitecase.com/publications/alert/cfius-finalizes-new-firrma-regulations.

57 David Mortlock, Noman Goheer, and Ahmad El-Gamal, "Expanded CFIUS Jurisdiction Under FIRRMA Regulations: An Overview," Wilkie Farr & Gallagher, May 19, 2020, https://www.willkie.com/-/media/files/publications/2020/05/expandedcfiusjurisdictionunderfirrmaregulations.pdf.

58 James K. Jackson and Cathleen D. Cimino-Isaacs, "CFIUS Reform Under FIRRMA," Congressional Research Service, February 21, 2020, https://sgp.fas.org/crs/natsec/IF10952.pdf.

59 "Annual Report to Congress for CY 2020," Committee on Foreign Investment in the United States (CFIUS), July 2021, https://home.treasury.gov/system/files/206/CFIUS-Public-Annual-Report-CY-2020.pdf.

60 Harry Clark, Gregory Hume, and Jeanine McGuinness, "President Trump Orders Divestment of U.S. Company; CFIUS Clears Semiconductor Transaction," JD Supra, March 16, 2020, https://www.jdsupra.com/legalnews/president-trump-orders-divestment-of-u-12562/.

61 "Statement by Secretary Steven T. Mnuchin on the President's Decision Regarding the Acquisition by ByteDance Ltd. of the U.S. Business of musical.ly," Treasury Department, August 14, 2020, https://home.treasury.gov/news/press-releases/sm1094.

62 Greg Roumeliotis, "U.S. Blocks MoneyGram Sale to China's Ant Financial on National Security Concerns, Reuters, January 2, 2018, https://www.reuters.com/article/us-moneygram-intl-m-a-ant-financial/u-s-blocks-moneygram-sale-to-chinas-ant-financial-on-national-security-concerns-idUSKBN1ER1R7.

63 "Annual Report to Congress for CY 2020," CFIUS, July 2021, https://home.treasury.gov/system/files/206/CFIUS-Public-Annual-Report-CY-2020.pdf; and "Annual Report to Congress for CY 2019," CFIUS, July 2020, https://home.treasury.gov/system/files/206/CFIUS-Public-Annual-Report-CY-2019.pdf.

64 Thilo Hanemann, Daniel H. Rosen, Mark Witzke, Steve Bennion, and Emma Smith, "Two-Way Street: 2021 Update US-China Investment Trends," Rhodium Group, May 2021, https://rhg.com/wp-content/uploads/2021/05/RHG_TWS-2021_Full-Report_Final.pdf; and Andres B. Schwarzenberg and Karen M. Sutter, "U.S.-China Investment Ties: Overview," Congressional Research Service, January 15, 2021, https://sgp.fas.org/crs/row/IF11283.pdf.

65 Jake Sullivan, "Remarks by National Security Advisor Jake Sullivan at the National Security Commission on Artificial Intelligence Global Emerging Technology Summit," White House, July 13, 2021, https://www.whitehouse.gov/nsc/briefing-room/2021/07/13/remarks-by-national-security-advisor-jake-sullivan-at-the-national-security-commission-on-artificial-intelligence-global-emerging-technology-summit/; Thilo Hanemann et al., "An Outbound Investment Screening Regime for the United States?," Rhodium Group, January 2022, https://rhg.com/wp-content/uploads/2022/01/RHG_TWS_2022_US-Outbound-Investment.pdf; and Sarah Bauerle-Danzman, "Is the US Going to Screen Outbound Investment?," Atlantic Council, January 10, 2022, https://www.atlanticcouncil.org/blogs/econographics/is-the-us-going-to-screen-outbound-investment/.

66 Executive Order 14032, "Addressing the Threat From Securities Investments That Finance Certain Companies of the People's Republic of China," June 3, 2021, https://www.federalregister.gov/documents/2021/06/07/2021-12019/addressing-the-threat-from-securities-investments-that-finance-certain-companies-of-the-peoples.

67 As of March 27, 2022, based on author's analysis of the Treasury Department's Sanctions List Search and Consolidated Sanctions List (Non-SDN Lists) spreadsheet (primary names) available at https://

sanctionssearch.ofac.treas.gov/ and https://home.treasury.gov/policy-issues/financial-sanctions/consolidated-sanctions-list-non-sdn-lists. This figure includes some duplication for companies listed two or more times under aliases or closely related entities.

68 "President Biden Revamps Communist Chinese Military Companies (CCMC) Sanctions Program," Paul, Weiss, June 7, 2021, https://www.paulweiss.com/practices/litigation/economic-sanctions-aml/publications/president-biden-revamps-communist-chinese-military-companies-ccmc-sanctions-program?id=40293.

69 Holding Foreign Companies Accountable Act, Public Law No. 116-222 (2020), https://www.govinfo.gov/content/pkg/PLAW-116publ222/pdf/PLAW-116publ222.pdf.

70 "Rule Governing Board Determinations Under the Holding Foreign Companies Accountable Act," Public Company Accounting Oversight Board (PCAOB), September 22, 2021, https://pcaob-assets.azureedge.net/pcaob-dev/docs/default-source/rulemaking/docket048/2021-004-hfcaa-adopting-release.pdf?sfvrsn=f6dfb7f8_4.

71 As of March 27, 2022, 225 China- and Hong Kong-based companies had filed audit reports in the last year, according to PCAOB: "Audit Reports Issued by PCAOB-Registered Firms Located Where Authorities Deny Access to Conduct Inspections," PCAOB, https://pcaobus.org/oversight/international/denied-access-to-inspections. See also "Chinese Companies Listed on Major U.S. Stock Exchanges," U.S.-China Economic and Security Review Commission, May 5, 2021, https://www.uscc.gov/sites/default/files/2021-05/Chinese_Companies_on_US_Stock_Exchanges_5-2021.pdf. The SEC estimated that about 10 percent of companies affected by the new law would have over-the-counter or unlisted securities. "Holding Foreign Companies Accountable Act Disclosure," SEC, 86 Fed. Reg. 70,027 (December 9, 2021), https://www.federalregister.gov/documents/2021/12/09/2021-26528/holding-foreign-companies-accountable-act-disclosure.

72 Robert Schmidt and Benjamin Bain, "SEC Chief Warns 'Clock Is Ticking' on Delisting Chinese Stocks," *Bloomberg*, August 25, 2021, https://www.bloomberg.com/news/articles/2021-08-25/sec-chief-warns-clock-is-ticking-on-delisting-chinese-stocks?sref=QmOxnLFz.

73 Senator John Kennedy, "Senate Passes Kennedy Bill to Strengthen America's Protection Against Fraudulent Foreign Companies," press release, June 22, 2021, https://www.kennedy.senate.gov/public/2021/6/senate-passes-kennedy-bill-to-strengthen-america-s-protection-against-fraudulent-foreign-companies; and H.R. 4521, The America COMPETES Act of 2022, § 60301, https://rules.house.gov/sites/democrats.rules.house.gov/files/BILLS-117HR4521RH-RCP117-31.pdf.

74 47 U.S.C. § 214; and 47 C.F.R. § 63.18.

75 "Order on Revocation of China Unicom Americas' Sec. 214 Authority," Federal Communications Commission (FCC), March 17, 2021, https://www.fcc.gov/document/order-revocation-china-unicom-americas-sec-214-authority.

76 47 U.S.C. §§ 34-35; and Executive Order 10530, "Providing for the Performance of Certain Functions Vested in or Subject to the Approval of the President," 19 Fed. Reg. 2,709 (May 10, 1954), https://www.archives.gov/federal-register/codification/executive-order/10530.html.

77 "Order on Revocation of China Unicom Americas' Sec. 214 Authority," FCC, March 17, 2021, https://www.fcc.gov/document/order-revocation-china-unicom-americas-sec-214-authority; and "Order on Revocation/Termination: Pacific Networks/ComNet 214 Authority," FCC, March 17, 2021, https://docs.fcc.gov/public/attachments/FCC-21-38A1.pdf.

78 Executive Order 13913, "Establishing the Committee for the Assessment of Foreign Participation in the United States Telecommunications Services Sector," April 4, 2020, https://www.federalregister.gov/documents/2020/04/08/2020-07530/establishing-the-committee-for-the-assessment-of-foreign-participation-in-the-united-states; and "The Committee for the Assessment of Foreign Participation in the United States Telecommunications Services Sector – Frequently Asked Questions," Justice Department, December 7, 2021, https://www.justice.gov/nsd/committee-assessment-foreign-participation-united-states-telecommunications-services-sector.

79 "FCC Denies China Mobile Telecom Services Application," FCC, May 9, 2019, https://www.fcc.gov/document/fcc-denies-china-mobile-telecom-services-application-0. For an overview, see Adam Chan, "CFIUS, Team Telecom and China," Lawfare, September 28, 2021, https://www.lawfareblog.com/cfius-team-telecom-and-china.

80 "FCC Denies China Mobile Telecom Services Application," FCC, May 9, 2019, https://www.fcc.gov/document/fcc-denies-china-mobile-telecom-services-application-0; "China Telecom Americas Order on Revocation and Termination," FCC, October 26, 2021, https://www.fcc.gov/document/china-telecom-americas-order-revocation-and-termination; "FCC Revokes China Unicom Americas' Telecom Services Authority," press release, FCC, January 27, 2022, https://www.fcc.gov/document/fcc-revokes-china-unicom-americas-telecom-services-authority; and "FCC Revokes Pacific Networks' & ComNet's Telecom Service Authority," press release, FCC, March 16, 2022, https://www.fcc.gov/document/fcc-revokes-pacific-networks-comnets-telecom-service-authority.

81 "Team Telecom Recommends That the FCC Deny Pacific Light Cable Network System's Hong Kong Undersea Cable Connection to the United States," press release, Justice Department, June 17, 2020, https://www.justice.gov/opa/pr/team-telecom-recommends-fcc-deny-pacific-light-cable-network-system-s-hong-kong-undersea.

82 Daphne Leprince-Ringuet, "Facebook and Google Drop Plans for Underwater Cable to Hong Kong After Security Warnings," ZDNet, September 1, 2020, https://www.zdnet.com/article/facebook-and-google-drop-plans-for-underwater-cable-to-hong-kong-after-security-warnings/; and Adam Chan, "CFIUS, Team Telecom and China," Lawfare, September 28, 2021, https://www.lawfareblog.com/cfius-team-telecom-and-china.

83 "Equipment Authorization – RF Device," FCC, https://www.fcc.gov/oet/ea/rfdevice.

84 Joel Griffin, "FCC Moves One Step Closer to Banning Hikvision, Dahua Products," SecurityInfoWatch.com, June 17, 2021, https://www.securityinfowatch.com/video-surveillance/article/21227289/fcc-moves-one-step-closer-to-banning-hikvision-dahua-products.

85 Joel Griffin, "FCC Moves One Step Closer to Banning Hikvision, Dahua Products," SecurityInfoWatch.com, June 17, 2021, https://www.securityinfowatch.com/video-surveillance/article/21227289/fcc-moves-one-step-closer-to-banning-hikvision-dahua-products; and "Notice of Proposed Rulemaking and Notice of Inquiry, Protecting Against National Security Threats to the Communications Supply Chain Through the Equipment Authorization Program; Protecting Against National Security Threats to the Communications Supply Chain through the Competitive Bidding Program," FCC, ET Docket Nos. 21-232 and 21-233, https://docs.fcc.gov/public/attachments/DOC-372818A1.pdf.

86 47 U.S.C. § 302a; and 47 C.F.R. § 2.915.

87 "List of Equipment and Services Covered By Section 2 of The Secure Networks Act," FCC, https://www.fcc.gov/supplychain/coveredlist.

88 47 U.S.C. § 1601(c); and John S. McCain National Defense Authorization Act for Fiscal Year 2019, Public Law No. 115-232, § 889(f)(3)(A-B).

89 Secure Equipment Act of 2021, Public Law No. 117-55.

90 "List of Equipment and Services Covered By Section 2 of The Secure Networks Act," FCC, https://www.fcc.gov/supplychain/coveredlist.

91 "Citing National Security Risks, Carr Calls for Starting Process of Adding DJI—a Chinese Drone Company—to FCC's Covered List," press release, FCC Commissioner Brendan Carr, October 19, 2021, https://www.fcc.gov/document/carr-calls-review-dji-citing-national-security-risks.

92 8 U.S.C. § 1182(a)(3)(C).

93 "U.S. Imposes Visa Restrictions on Certain Employees of Chinese Technology Companies That Abuse Human Rights," State Department, July 15, 2020, https://2017-2021.state.gov/u-s-imposes-visa-restrictions-on-certain-employees-of-chinese-technology-companies-that-abuse-human-rights/index.html.

94 8 U.S.C. § 1182(f).

95 Ben Harrington and Theresa A. Reiss, "Presidential Actions to Exclude Aliens Under INA § 212(f)," Congressional Research Service, May 4, 2020, https://crsreports.congress.gov/product/pdf/LSB/LSB10458.

96 Proclamation 10043, "Suspension of Entry as Nonimmigrants of Certain Students and Researchers From the People's Republic of China," May 29, 2020, https://www.federalregister.gov/documents/2020/06/04/2020-12217/suspension-of-entry-as-nonimmigrants-of-certain-students-and-researchers-from-the-peoples-republic.

97 Humeyra Pamuk, "U.S. Revokes More Than 1,000 Visas of Chinese Nationals, Citing Military Links," Reuters, September 9, 2020, https://www.reuters.com/article/us-usa-china-visas-students/u-s-revokes-more-than-1000-visas-of-chinese-nationals-citing-military-links-idUSKBN26039D; and Stuart Anderson, "Biden Keeps Costly Trump Visa Policy Denying Chinese Grad Students," *Forbes*, August 10, 2021, https://www.forbes.com/sites/stuartanderson/2021/08/10/biden-keeps-costly-trump-visa-policy-denying-chinese-grad-students/.

98 Remco Zwetsloot, Emily Weinstein, and Ryan Fedasiuk, "Assessing the Scope of U.S. Visa Restrictions on Chinese Students," Center for Security and Emerging Technology, February 2021, https://cset.georgetown.edu/publication/assessing-the-scope-of-u-s-visa-restrictions-on-chinese-students/.

99 For an overview, see Evan Burke, "Trump-Era Policies Toward Chinese STEM Talent: A Need for Better Balance," Carnegie Endowment for International Peace, March 25, 2021, https://carnegieendowment.org/2021/03/25/trump-era-policies-toward-chinese-stem-talent-need-for-better-balance-pub-84137; and Evan Burke, "The Right Way to Bring Chinese STEM Talent Back to the U.S.," ChinaFile, April 27, 2021, https://www.chinafile.com/reporting-opinion/viewpoint/right-way-bring-chinese-stem-talent-back-us.

100 "Establishing a Fixed Time Period of Admission and an Extension of Stay Procedure for Nonimmigrant Academic Students, Exchange Visitors, and Representatives of Foreign Information Media," Department of Homeland Security, 85 Fed. Reg. 60,526 (September 25, 2020), https://www.federalregister.gov/documents/2020/09/25/2020-20845/establishing-a-fixed-time-period-of-admission-and-an-extension-of-stay-procedure-for-nonimmigrant.

101 "Strengthening Wage Protections for the Temporary and Permanent Employment of Certain Aliens in the United States," Department of Labor, 86 Fed. Reg. 3,608 (January 14, 2021), https://www.federalregister.gov/documents/2021/01/14/2021-00218/strengthening-wage-protections-for-the-temporary-and-permanent-employment-of-certain-aliens-in-the.

102 Proclamation 10052, "Suspension of Entry of Immigrants and Nonimmigrants Who Present a Risk to the United States Labor Market During the Economic Recovery Following the 2019 Novel Coronavirus Outbreak," 85 Fed. Reg. 38,263 (June 22, 2020), https://www.federalregister.gov/documents/2020/06/25/2020-13888/suspension-of-entry-of-immigrants-and-nonimmigrants-who-present-a-risk-to-the-united-states-labor.

103 Evan Burke, "Trump-Era Policies Toward Chinese STEM Talent: A Need for Better Balance," Carnegie Endowment for International Peace, March 25, 2021, https://carnegieendowment.org/2021/03/25/trump-era-policies-toward-chinese-stem-talent-need-for-better-balance-pub-84137.

104 "Establishing a Fixed Time Period of Admission and an Extension of Stay Procedure for Nonimmigrant Academic Students, Exchange Visitors, and Representatives of Foreign Information Media," Department of Homeland Security, 86 Fed. Reg. 35,410 (July 6, 2021), https://www.federalregister.gov/documents/2021/07/06/2021-13929/establishing-a-fixed-time-period-of-admission-and-an-extension-of-stay-procedure-for-nonimmigrant; "Biden Admin Proposes 18-Month Delay in Calculating Prevailing Wages of H-1B, Other Visas," *Economic Times*, March 24, 2021, https://economictimes.indiatimes.com/nri/work/biden-admin-proposes-18-month-delay-in-calculating-prevailing-wages-of-h-1b-and-other-visas/articleshow/81646252.cms; and "Biden Lets Trump Era H-1B Visa Bans Expire; Indian IT Professionals to Benefit," *Economic Times*, April 1, 2021, https://economictimes.indiatimes.com/nri/work/biden-lets-trump-era-h-1b-visa-bans-expire-indian-it-professionals-to-benefit/articleshow/81813752.cms.

105 Abby Lemert and Eleanor Runde, "New U.S. Visa Rules Prompt Scrutiny of CCP Members," Lawfare, December 11, 2020, https://www.lawfareblog.com/new-us-visa-rules-prompt-scrutiny-ccp-members.

106 Chad P. Bown and Cathleen Cimino-Isaacs, "Will Trump Invoke National Security to Start a Trade War?," Peterson Institute for International Economics (PIIE), July 5, 2017, https://www.piie.com/blogs/trade-investment-policy-watch/will-trump-invoke-national-security-start-trade-war.

107 19 U.S.C. § 1673.

108 19 U.S.C. § 1671.

109 Chad P. Bown, "Steel, Aluminum, Lumber, Solar: Trump's Stealth Trade Protection," PIIE, June 2017, https://www.piie.com/system/files/documents/pb17-21.pdf.

110 "Understanding Antidumping & Countervailing Duty Investigations," USITC, https://www.usitc.gov/press_room/usad.htm.

111 19 U.S.C. §§ 1671, 1673.

112 19 U.S.C. § 1337. For a discussion of how Section 337 relates to China, see Yiqing Yin, "Section 337 of the Tariff Act of 1930 and Its Impacts on China," *Catholic University Journal of Law and Technology* 25, no. 2 (2017), https://scholarship.law.edu/cgi/viewcontent.cgi?article=1038&context=jlt.

113 "Certain Two-Way Radio Equipment and Systems, Related Software and Components Thereof; Commission Decision to Affirm-in-Part, Modify-in-Part, Reverse-in-Part, and Strike Certain Portions of a Final Initial Determination Finding a Violation of Section 337; Issuance of Limited Exclusion Order and Cease and Desist Orders; and Termination of the Investigation," USITC, 83 Fed. Reg. 59,415 (November 23, 2018), https://www.federalregister.gov/documents/2018/11/23/2018-25463/certain-two-way-radio-equipment-and-systems-related-software-and-components-thereof-commission.

114 "Federal Indictment Charges PRC-Based Telecommunications Company With Conspiring With Former Motorola Solutions Employees to Steal Technology," press release, Justice Department, February 7, 2022, https://www.justice.gov/opa/pr/federal-indictment-charges-prc-based-telecommunications-company-conspiring-former-motorola.

115 "Certain Unmanned Aerial Vehicles and Components Thereof; Final Determination Finding a Violation of Section 337 and Issuance of Remedial Orders; Suspension of Enforcement of the Remedial Orders Pending Final Resolution of a Final Written Decision by the Patent Trial and Appeal Board; and Termination of the Investigation," USITC, 85 Fed. Reg. 52,640 (August 26, 2020), https://www.federalregister.gov/documents/2020/08/26/2020-18695/certain-unmanned-aerial-vehicles-and-components-thereof-final-determination-finding-a-violation-of.

116 Qingyu Yin et al., "Latest Development in the DJI-Autel Disputes," Finnegan, August 24, 2020, https://www.finnegan.com/en/insights/ip-updates/latest-development-in-the-dji-autel-disputes.html; "Certain Unmanned Aerial Vehicles and Components Thereof; Commission Determination to Institute a Rescission Proceeding and Rescind Permanently a Limited Exclusion Order and Cease and Desist Orders; Termination of Rescission Proceeding," USITC, 86 Fed. Reg. 51,676 (August 16, 2021), https://www.federalregister.gov/documents/2021/09/16/2021-19977/certain-unmanned-aerial-vehicles-and-components-thereof-commission-determination-to-institute-a; and Ishveena Singh, "DJI, Autel Settle Years-Long Patent Dispute Days Before Jury Trial," DroneDJ, August 19, 2021, https://dronedj.com/2021/08/19/dji-autel-settle-years-long-patent-dispute-days-before-jury-trial/.

117 "Anti-dumping, Subsidies, Safeguards: Contingencies, Etc.," World Trade Organization (WTO), https://www.wto.org/english/thewto_e/whatis_e/tif_e/agrm8_e.htm; and Chad P. Bown, "Steel, Aluminum, Lumber, Solar: Trump's Stealth Trade Protection," PIIE, June 2017, https://www.piie.com/system/files/documents/pb17-21.pdf.

118 "DS186: United States — Section 337 of the Tariff Act of 1930 and Amendments Thereto," WTO, https://www.wto.org/english/tratop_e/dispu_e/cases_e/ds186_e.htm; and Joel W. Rogers and Joseph P. Whitlock, "Is Section 337 Consistent With the GATT and the TRIPs Agreement?," *American University International Law Review* 17, no. 3 (2002), https://digitalcommons.wcl.american.edu/cgi/viewcontent.cgi?article=1220&context=auilr.

119 For a general overview, see Brock R. Williams et al., "Trump Administration Tariff Actions: Frequently Asked Questions," Congressional Research Service, December 15, 2020, https://crsreports.congress.gov/product/pdf/R/R45529; and Chad P. Bown and Melina Kolb, "Trump's Trade War Timeline: An Up-to-Date Guide," PIIE, October 31, 2021, https://www.piie.com/sites/default/files/documents/trump-trade-war-timeline.pdf.

120 Another example is Section 201 of the Trade Act of 1974, which authorizes the ITC to investigate surges of foreign imports in "such increased quantities" that are or threaten to become "a substantial cause of serious injury" to U.S. industry. (The import surge need not be unfair in any way.) A USITC finding then allows the President to impose temporary "global safeguards," such as tariffs or other import restrictions, on the imported item from all countries. Trump instituted safeguards for solar panels and washing machines, following the first new investigations under this authority since 2001. 19 U.S.C. § 2251; "Understanding Safeguard Investigations," USITC, https://www.usitc.gov/press_room/us_safeguard.htm; "President Trump Approves Relief for U.S. Washing Machine and Solar Cell Manufacturers," press release, U.S. Trade Representative (USTR), January 22, 2018, https://ustr.gov/about-us/policy-offices/press-office/press-releases/2018/january/president-trump-approves-relief-us; and Chad P. Bown and Junie Joseph, "Solar and Washing Machine Safeguards in Context: The History of US Section 201 Use," PIIE,

October 31, 2017, https://www.piie.com/blogs/trade-and-investment-policy-watch/solar-and-washing-machine-safeguards-context-history-us.

121 19 U.S.C. § 2411.

122 19 U.S.C. § 2411(c)(3)(B).

123 "Addressing China's Laws, Policies, Practices, and Actions Related to Intellectual Property, Innovation, and Technology," Presidential Memorandum for the USTR, 82 Fed. Reg. 39,007 (August 14, 2017), https://trumpwhitehouse.archives.gov/presidential-actions/presidential-memorandum-united-states-trade-representative/.

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

125 Chad P. Bown and Melina Kolb, "Trump's Trade War Timeline: An Up-to-Date Guide," PIIE, October 31, 2021, https://www.piie.com/sites/default/files/documents/trump-trade-war-timeline.pdf; Chad P. Bown, "US-China Trade War Tariffs: An Up-to-Date Chart," PIIE, March 16, 2021, https://www.piie.com/research/piie-charts/us-china-trade-war-tariffs-date-chart; and Andres B. Schwarzenberg, "Section 301 of the Trade Act of 1974: Origin, Evolution, and Use," Congressional Research Service, December 14, 2020, https://sgp.fas.org/crs/misc/R46604.pdf.

126 "USTR Issues Tariffs on Chinese Products in Response to Unfair Trade Practices," press release, USTR, June 15, 2018, https://ustr.gov/about-us/policy-offices/press-office/press-releases/2018/june/ustr-issues-tariffs-chinese-products; USTR, "USTR Finalizes Tariffs on $200 Billion of Chinese Imports in Response to China's Unfair Trade Practices," September 18, 2018, https://ustr.gov/about-us/policy-offices/press-office/press-releases/2018/september/ustr-finalizes-tariffs-200; and Brock R. Williams et al., "Trump Administration Tariff Actions: Frequently Asked Questions," Congressional Research Service, December 15, 2020, https://crsreports.congress.gov/product/pdf/R/R45529.

127 Andres B. Schwarzenberg, "Section 301 of the Trade Act of 1974: Origin, Evolution, and Use," Congressional Research Service, December 14, 2020, https://sgp.fas.org/crs/misc/R46604.pdf; and Brock R. Williams et al., "Trump Administration Tariff Actions: Frequently Asked Questions," Congressional Research Service, December 15, 2020, https://crsreports.congress.gov/product/pdf/R/R45529.

128 Joseph L. Barloon et al., "USTR Relaunches Exclusion Process for China Section 301 Tariffs," Skadden, Arps, Slate, Meagher & Flom, October 12, 2021 https://www.skadden.com/insights/publications/2021/10/ustr-relaunches-exclusion-process.

129 Chad P. Bown and Cathleen Cimino-Isaacs, "Will Trump Invoke National Security to Start a Trade War?," PIIE, July 5, 2017, https://www.piie.com/blogs/trade-investment-policy-watch/will-trump-invoke-national-security-start-trade-war.

130 19 U.S.C. § 1862.

131 19 U.S.C. § 1862(d).

132 Chad P. Bown and Melina Kolb, "Trump's Trade War Timeline: An Up-to-Date Guide," PIIE, October 31, 2021, https://www.piie.com/sites/default/files/documents/trump-trade-war-timeline.pdf.

133 Chad P. Bown, "Trump's Long-awaited Steel and Aluminum Tariffs Are Just the Beginning," PIIE, March 26, 2018, https://www.piie.com/blogs/trade-and-investment-policy-watch/trumps-long-awaited-steel-and-aluminum-tariffs-are-just; and Chad P. Bown and Melina Kolb, "Trump's Trade War Timeline: An Up-to-Date Guide," PIIE, October 31, 2021, https://www.piie.com/sites/default/files/documents/trump-trade-war-timeline.pdf.

134 19 U.S.C. § 1307.

135 "Withhold Release Orders and Findings List," Customs and Border Protection (CBP), https://www.cbp.gov/trade/forced-labor/withhold-release-orders-and-findings.

136 "DHS Cracks Down on Goods Produced by China's State-Sponsored Forced Labor," press release, CBP, September 14, 2020, https://www.cbp.gov/newsroom/national-media-release/dhs-cracks-down-goods-produced-china-s-state-sponsored-forced-labor; and "The Department of Homeland Security Issues Withhold Release Order on Silica-Based Products Made by Forced Labor in Xinjiang," press release, CBP, June 24, 2021, https://www.cbp.gov/newsroom/national-media-release/department-homeland-security-issues-withhold-release-order-silica.

137 Uyghur Forced Labor Prevention Act of 2021, Public Law No. 117-78, § 3, https://www.govinfo.gov/content/pkg/PLAW-117publ78/pdf/PLAW-117publ78.pdf.

138 "Sanctions Programs and Country Information," Treasury Department, https://home.treasury.gov/policy-issues/financial-sanctions/sanctions-programs-and-country-information.

139 "Reference Sheet on Economic Sanctions," Brookings Institution, December 2020, https://www.brookings.edu/wp-content/uploads/2020/12/ReferenceSheet_EconomicSanctions.pdf.

140 50 U.S.C. § 1701.

141 50 U.S.C. § 1701, 1702.

142 As of March 11, 2022. "Declared National Emergencies Under the National Emergencies Act," Brennan Center, December 15, 2021, https://www.brennancenter.org/our-work/research-reports/declared-national-emergencies-under-national-emergencies-act.

143 50 U.S.C. §§ 1601-1651.

144 "Reference Sheet on Economic Sanctions," Brookings Institution, December 2020, https://www.brookings.edu/wp-content/uploads/2020/12/ReferenceSheet_EconomicSanctions.pdf.

145 As of March 27, 2022, based on author's analysis of the Treasury Department's Sanctions List Search and SDN spreadsheet, available at https://sanctionssearch.ofac.treas.gov/ and https://home.treasury.gov/policy-issues/financial-sanctions/specially-designated-nationals-list-data-formats-data-schemas (primary names). Figures exclude all entries with exact duplicate names; however, they may include entries for close variations of names, aliases, subsidiaries, and affiliates. "China" here refers to mainland China plus Hong Kong and Macau. China-based actors include some third-country entities that maintain a presence in China.

146 For the purpose of these figures, China-specific reasons refer to human rights abuses and corruption (Executive Order 13818) and Hong Kong repression (Executive Order 13936).

147 "Treasury Sanctions CEIEC for Supporting the Illegitimate Maduro Regime's Efforts to Undermine Venezuelan Democracy," Treasury Department, November 30, 2020, https://home.treasury.gov/news/press-releases/sm1194.

148 Executive Order 13818, "Blocking the Property of Persons Involved in Serious Human Rights Abuse or Corruption," 82 Fed. Reg. 60,839 (December 20, 2017), https://www.federalregister.gov/documents/2017/12/26/2017-27925/blocking-the-property-of-persons-involved-in-serious-human-rights-abuse-or-corruption.

149 As of March 27, 2022, based on author's analysis of the Treasury Department's Sanctions List Search, available at https://sanctionssearch.ofac.treas.gov/. Figures include China, Hong Kong, and Macau-based actors, excluding duplicate entries associated with more than one of these jurisdictions. Rob Berschinski, "Trump Administration Notches a Serious Human Rights Win. No, really." Just Security, January 10, 2018, https://www.justsecurity.org/50846/trump-administration-notches-human-rights-win-no-really/.

150 Uyghur Human Rights Policy Act of 2020, Public Law No. 116-145, § 6, https://www.govinfo.gov/content/pkg/PLAW-116publ145/pdf/PLAW-116publ145.pdf; and Uyghur Forced Labor Prevention Act of 2021, Public Law No. 117-78, § 5, https://www.govinfo.gov/content/pkg/PLAW-117publ78/pdf/PLAW-117publ78.pdf.

151 As of March 27, 2022, based on author's analysis of the Treasury Department's Sanctions List Search, available at https://sanctionssearch.ofac.treas.gov/. Executive Order 13936, "The President's Executive Order on Hong Kong Normalization," 85 Fed. Reg. 43,413 (July 14, 2020), https://www.federalregister.gov/documents/2020/07/17/2020-15646/the-presidents-executive-order-on-hong-kong-normalization.

152 S.1260, "United States Innovation and Competition Act of 2021," §§ 3211, 5202, https://www.congress.gov/bill/117th-congress/senate-bill/1260/text.

153 S.1260, "United States Innovation and Competition Act of 2021," §§ 5203-5204, https://www.congress.gov/bill/117th-congress/senate-bill/1260/text.

154 H.R. 4521, The America COMPETES Act of 2022, https://rules.house.gov/sites/democrats.rules.house.gov/files/BILLS-117HR4521RH-RCP117-31.pdf.

155 Executive Order 13942, "Addressing the Threat Posed by TikTok, and Taking Additional Steps to Address the National Emergency With Respect to the Information and Communications Technology

and Services Supply Chain," 85 Fed. Reg. 48,637 (August 6, 2020), https://www.federalregister.gov/documents/2020/08/11/2020-17699/addressing-the-threat-posed-by-tiktok-and-taking-additional-steps-to-address-the-national-emergency; and Executive Order 13943, "Addressing the Threat Posed by WeChat, and Taking Additional Steps to Address the National Emergency With Respect to the Information and Communications Technology and Services Supply Chain," 85 Fed. Reg. 48,641 (August 6, 2020), https://www.federalregister.gov/documents/2020/08/11/2020-17700/addressing-the-threat-posed-by-wechat-and-taking-additional-steps-to-address-the-national-emergency.

156 Executive Order 13873, "Securing the Information and Communications Technology and Services Supply Chain," 84 Fed. Reg. 22689 (May 15, 2019) https://www.federalregister.gov/documents/2019/05/17/2019-10538/securing-the-information-and-communications-technology-and-services-supply-chain.

157 "Identification of Prohibited Transactions to Implement Executive Order 13942 and Address the Threat Posed by TikTok and the National Emergency With Respect to the Information and Communications Technology and Services Supply Chain," Commerce Department, 85 Fed. Reg. 60,061 (September 24, 2020), https://www.federalregister.gov/documents/2020/09/24/2020-21193/identification-of-prohibited-transactions-to-implement-executive-order-13942-and-address-the-threat.

158 Executive Order 13971, "Addressing the Threat Posed by Applications and Other Software Developed or Controlled by Chinese Companies," 86 Fed. Reg. 1249 (January 5, 2021), https://www.federalregister.gov/documents/2021/01/08/2021-00305/addressing-the-threat-posed-by-applications-and-other-software-developed-or-controlled-by-chinese.

159 Robert Chesney, "TikTok, WeChat, and Biden's New Executive Order: What You Need to Know," Lawfare, June 9, 2021, https://www.lawfareblog.com/tiktok-wechat-and-bidens-new-executive-order-what-you-need-know.

160 Executive Order 13920, "Securing the United States Bulk-Power System," 85 Fed. Reg. 26595 (May 1, 2020), https://www.federalregister.gov/documents/2020/05/04/2020-09695/securing-the-united-states-bulk-power-system.

161 Department of Energy, "Prohibition Order Securing Critical Defense Facilities," 86 Fed. Reg. 533 (January 6, 2021), https://www.federalregister.gov/documents/2021/01/06/2020-28773/prohibition-order-securing-critical-defense-facilities.

162 "Notice of Request for Information (RFI) on Ensuring the Continued Security of the United States Critical Electric Infrastructure," Department of Energy, 86 Fed. Reg. 21,309 (April 22, 2021), https://www.federalregister.gov/documents/2021/04/22/2021-08482/notice-of-request-for-information-rfi-on-ensuring-the-continued-security-of-the-united-states.

163 "Securing the Information and Communications Technology and Services Supply Chain," Commerce Department, 86 Fed. Reg. 4909 (January 19, 2021), https://www.federalregister.gov/documents/2021/01/19/2021-01234/securing-the-information-and-communications-technology-and-services-supply-chain.

164 "Fact Sheet: Executive Order Protecting Americans' Sensitive Data From Foreign Adversaries," press release, White House, June 9, 2021, https://www.whitehouse.gov/briefing-room/statements-releases/2021/06/09/fact-sheet-executive-order-protecting-americans-sensitive-data-from-foreign-adversaries/; and Executive Order 14034, "Protecting Americans' Sensitive Data From Foreign Adversaries," 86 Fed. Reg. 31,423 (June 9, 2021), https://www.federalregister.gov/documents/2021/06/11/2021-12506/protecting-americans-sensitive-data-from-foreign-adversaries.

165 "U.S. Secretary of Commerce Gina Raimondo Statement on Actions Taken Under ICTS Supply Chain Executive Order," press release, Commerce Department, March 17, 2021, https://www.commerce.gov/news/press-releases/2021/03/us-secretary-commerce-gina-raimondo-statement-actions-taken-under-icts; Alexandra Alper, "Exclusive: U.S. Examining Alibaba's Cloud Unit for National Security Risks – Sources," Reuters, January 19, 2022, https://www.reuters.com/technology/exclusive-us-examining-alibabas-cloud-unit-national-security-risks-sources-2022-01-18/; and Ben Brody, "A Secretive US Security Program Has Its Sights on DiDi," Protocol, March 23, 2022, https://www.protocol.com/policy/didi-commerce-icts.

166 Haye Kesteloo, "Department of Defense Bans the Purchase of Commercial-Over-the-Shelf UAS, Including DJI Drones Effective Immediately," DroneDJ, June 7, 2018, https://dronedj.com/2018/06/07/department-of-defense-bans-the-purchase-of-commercial-over-the-shelf-uas-including-dji-drones/; and

National Defense Authorization Act for Fiscal Year 2020, Public Law No. 116-92, § 848, https://www.govinfo.gov/content/pkg/PLAW-116publ92/pdf/PLAW-116publ92.pdf.

167 "Secretary Bernhardt Signs Order Grounding Interior's Drone Fleet for Non-Emergency Operations," press release, Department of Interior, January 29, 2020, https://www.doi.gov/pressreleases/secretary-bernhardt-signs-order-grounding-interiors-drone-fleet-non-emergency.

168 Executive Order 13981, "Protecting the United States From Certain Unmanned Aircraft Systems," 86 Fed. Reg. 6,821 (January 18, 2021), https://www.federalregister.gov/documents/2021/01/22/2021-01646/protecting-the-united-states-from-certain-unmanned-aircraft-systems.

169 John S. McCain National Defense Authorization Act for Fiscal Year 2019, Public Law No. 115-232, § 889(f)(3)(A-B).

170 John S. McCain National Defense Authorization Act for Fiscal Year 2019, Public Law No. 115-232, § 889(f)(3)(D).

171 Angela B. Styles, Scott M. Heimberg, Robert K. Huffman, and Chris Chamberlain, "Section 889(a)(1)(B): Five Things to Know About the Interim Rule and a Roadmap for Compliance," Akin Gump, August 5, 2020, https://www.akingump.com/en/news-insights/section-889a1b-five-things-to-know-about-the-interim-rule-and-a-roadmap-for-compliance.html.

172 Author's analysis of the Treasury Department's Federal Contract Explorer spreadsheet, available at https://datalab.usaspending.gov/unstructured-data/contract-explorer/awards_contracts_FY18_v2.csv. This figure excludes all entries with exact duplicate names; however, they include entries for close variations of names, aliases, subsidiaries, and affiliates.

173 47 C.F.R. §§ 54.9–54.11; and "Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs," FCC, 86 Fed. Reg. 46,995 (August 23, 2021), https://www.federalregister.gov/documents/2021/08/23/2021-17279/protecting-against-national-security-threats-to-the-communications-supply-chain-through-fcc-programs.

174 Matt Kapko, "Rural US Carriers Secure $1.9B to Rip Out Chinese Equipment," SDxCentral, December 23, 2020, https://www.sdxcentral.com/articles/news/rural-us-carriers-secure-1-9b-to-rip-out-chinese-equipment/2020/12/; and Mike Dano, "Verizon, CenturyLink, Windstream Still Using Huawei, ZTE Equipment," September 4, 2020, https://www.lightreading.com/security/verizon-centurylink-windstream-still-using-huawei-zte-equipment/d/d-id/763705.

175 As of December 1, 2021. Eileen Guo, Jess Aloe, and Karen Hao, "We Built a Database to Understand the China Initiative. Then the Government Changed Its Records." MIT Technology Review, December 2, 2021, https://www.technologyreview.com/2021/12/02/1039397/china-initiative-database-doj/.

176 "Chinese Telecommunications Conglomerate Huawei and Subsidiaries Charged in Racketeering Conspiracy and Conspiracy to Steal Trade Secrets," press release, Justice Department, February 13, 2020, https://www.justice.gov/opa/pr/chinese-telecommunications-conglomerate-huawei-and-subsidiaries-charged-racketeering.

177 "Information About the Department of Justice's China Initiative and a Compilation of China-Related Prosecutions Since 2018," Justice Department, November 19, 2021, https://www.justice.gov/nsd/information-about-department-justice-s-china-initiative-and-compilation-china-related.

178 "Chinese Telecommunications Conglomerate Huawei and Subsidiaries Charged in Racketeering Conspiracy and Conspiracy to Steal Trade Secrets," press release, Justice Department, February 13, 2020, https://www.justice.gov/opa/pr/chinese-telecommunications-conglomerate-huawei-and-subsidiaries-charged-racketeering.

179 As of September 15, 2021. Ellen Nakashima and David Nakamura, "China Initiative Aims to Stop Economic Espionage. Is Targeting Academics Over Grant Fraud 'Overkill'?," *Washington Post*, September 15, 2021, https://www.washingtonpost.com/national-security/china-initiative-questions-dismissals/2021/09/15/530ef936-f482-11eb-9738-8395ec2a44e7_story.html.

180 Ellen Nakashima and David Nakamura, "U.S. Drops Cases Against Five Researchers Accused of Hiding Ties to Chinese Military," *Washington Post*, July 23, 2021, https://www.washingtonpost.com/national-security/us-drops-cases-against-five-researchers-accused-of-hiding-ties-to-chinese-military/2021/07/23/54a8b268-ec04-11eb-8950-d73b3e93ff7f_story.html; and Elizabeth Redden, "A Retreat From China Collaborations in the Face of U.S. Scrutiny," *Inside Higher Ed*, October 29, 2021, https://www.insidehighered.com/news/2021/10/29/survey-finds-chilling-effect-china-initiative.

181 George P. Varghese, Benjamin Conery, Hyun-Soo Lim, and Christina Luo, "DOJ's 'China Initiative' Falters," Wilmer Hale, August 5, 2021, https://www.wilmerhale.com/en/insights/client-alerts/20210805-dojs-china-initiative-falters.

182 Ellen Nakashima and David Nakamura, "U.S. Drops Cases Against Five Researchers Accused of Hiding Ties to Chinese Military," *Washington Post*, July 23, 2021, https://www.washingtonpost.com/national-security/us-drops-cases-against-five-researchers-accused-of-hiding-ties-to-chinese-military/2021/07/23/54a8b268-ec04-11eb-8950-d73b3e93ff7f_story.html; Associated Press, "Tennessee Professor With Ties to China Acquitted by District Judge," *Washington Post*, September 10, 2021, https://www.washingtonpost.com/national/tennessee-professor-with-ties-to-china-acquitted-by-district-judge/2021/09/10/30d32e74-0c64-11ec-aea1-42a8138f132a_story.html; and Ellen Barry and Katie Benner, "U.S. Drops Its Case Against M.I.T. Scientist Accused of Hiding China Links," *New York Times*, January 20, 2022, https://www.nytimes.com/2022/01/20/science/gang-chen-mit-china-initiative.html.

183 "Harvard University Professor Convicted of Making False Statements and Tax Offenses," press release, Justice Department, December 21, 2021, https://www.justice.gov/usao-ma/pr/harvard-university-professor-convicted-making-false-statements-and-tax-offenses.

184 Matthew Olsen, "Assistant Attorney General Matthew Olsen Delivers Remarks on Countering Nation-State Threats," Justice Department, February 23, 2022, https://www.justice.gov/opa/speech/assistant-attorney-general-matthew-olsen-delivers-remarks-countering-nation-state-threats.

185 Matthew Olsen, "Assistant Attorney General Matthew Olsen Delivers Remarks on Countering Nation-State Threats," Justice Department, February 23, 2022, https://www.justice.gov/opa/speech/assistant-attorney-general-matthew-olsen-delivers-remarks-countering-nation-state-threats.

186 The canvas is not entirely blank, as Congress has made it difficult for the executive branch to rescind certain China-tech restrictions. In this way, Congress is contributing to the risk (discussed later) of feedback loops that entrench and accelerate technological decoupling.