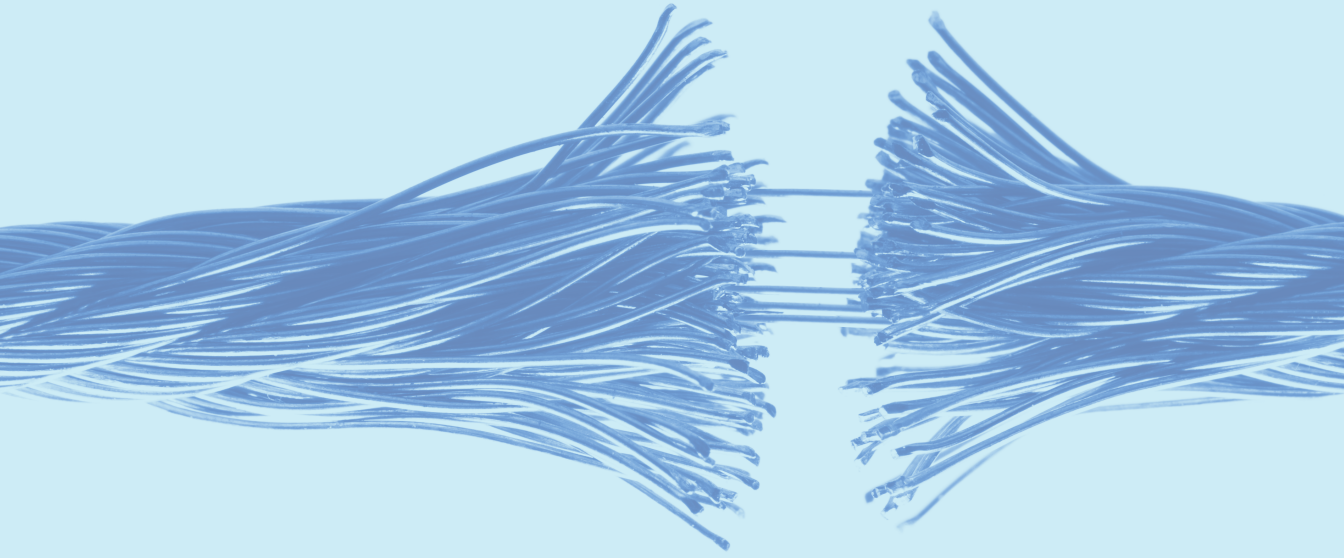


U.S.-CHINA TECHNOLOGICAL "DECOUPLING"

A STRATEGY AND POLICY FRAMEWORK

JON BATEMAN
With Foreword by Eric Schmidt

CARNEGIE
ENDOWMENT FOR
INTERNATIONAL PEACE

U.S.-CHINA TECHNOLOGICAL "DECOUPLING"

A STRATEGY AND POLICY FRAMEWORK

JON BATEMAN
With Foreword by Eric Schmidt

Carnegie Endowment for International Peace
Publications Department
1779 Massachusetts Avenue NW
Washington, DC 20036
P: + 1 202 483 7600
F: + 1 202 483 1840
CarnegieEndowment.org

This publication can be downloaded at no cost at CarnegieEndowment.org.

TABLE OF CONTENTS

ABOUT THE AUTHOR

Jon Bateman is a fellow in the Technology and International Affairs Program at the Carnegie Endowment for International Peace. He previously worked as a senior intelligence analyst, policy adviser, and speechwriter in the U.S. Department of Defense, most recently serving as special assistant to the Chairman of the Joint Chiefs of Staff.

ACKNOWLEDGMENTS

The author is deeply grateful to George Perkovich for his patient guidance and penetrating reviews of this report throughout its development. Special thanks also go to Marjory Blumenthal, Tom Carothers, Mark Chandler, Chris Chivvis, Tino Cuéllar, Doug Farrar, Steve Feldstein, Sarah Gordon, Yukon Huang, Jim Miller, Mike Nelson, Matt Sheehan, Stephen Wertheim, and Tong Zhao for their valuable written feedback on drafts. Conversations with many others—in government, the private sector, academia, and civil society—helped to test and sharpen the report's underlying ideas. Thanks are also owed to Evan Burke, Emeizmi Mandagi, Nikhil Manglik, and Arthur Nelson for research assistance, and to Isabella Furth, Natalie Brase, Jocelyn Soly, and Amy Mellon for editing and design. This report is the author's sole responsibility and does not represent the views of any other person or institution.

The research for and writing of this report were supported by the William and Flora Hewlett Foundation. Editorial production and dissemination were supported by a grant from Schmidt Futures.

ABBREVIATIONS

AI	Artificial intelligence
CBP	Customs and Border Protection
CCL	Commerce Control List
CFIUS	Committee on Foreign Investment in the United States
DHS	Department of Homeland Security
DOD	Department of Defense
EAR	Export Administration Regulations
ECRA	Export Control Reform Act
FCC	Federal Communications Commission
FIRRMA	Foreign Investment Risk Review Modernization Act
IC	Intelligence Community
ICTS	Information and communications technology or services
IEEPA	International Emergency Economic Powers Act

INA	Immigration and Nationality Act
ITAR	International Traffic in Arms Regulations
MEU	Military End User
NSC	National Security Council
PLA	People's Liberation Army
PRC	People's Republic of China
R&D	Research and development
SDN	Specially Designated Nationals
SEC	Securities and Exchange Commission
STEM	Science, technology, engineering, and mathematics
USITC	U.S. International Trade Commission
USML	U.S. Munitions List
USTR	U.S. Trade Representative
WTO	World Trade Organization

FOREWORD

Technology is the engine that powers superpowers. As the chair of the National Security Commission on Artificial Intelligence (NSCAI), I led the effort that ultimately delivered a harsh message to the U.S. Congress and to the administration: America is not prepared to defend or compete in the AI era. The fact is that America has been technologically dominant for so long that some U.S. leaders came to take it for granted. They were wrong. A second technological superpower, China, has emerged. It happened with such astonishing speed that we're all still straining to understand the implications.

Washington has awakened to find the United States deeply technologically enmeshed with its chief long-term rival. America built those technology ties over many years and for lots of good reasons. China's tech sector continues to benefit American businesses, universities, and citizens in myriad ways—providing critical skilled labor and revenue to sustain U.S. R&D, for example. But that same Chinese tech sector also powers Beijing's military build-up, unfair trade practices, and repressive social control.

What should we do about this? In Washington, many people I talk to give a similar answer. They say that some degree of technological separation from China is necessary, but we shouldn't go so far as to harm U.S. interests in the process. That's exactly right, of course, but it's also pretty vague. How partial should this partial separation be—would 15 percent of U.S.-China technological ties be severed, or 85 percent? Which technologies would fall on either side of the cut line? And what, really, is the strategy for America's long-term technology relationship with China? The further I probe, the less clarity and consensus I find.

In fairness, these are serious dilemmas. They're also unfamiliar. "Decoupling" entered the Washington lexicon just a few years ago, and it represents a dramatic break from earlier assumptions. In 2018, for example, I remarked that the global internet would probably bifurcate into a Chinese-led internet and a U.S.-led internet. Back then, this idea was still novel enough that the comment made headlines around the world. Now, the prediction has already come halfway true. Meanwhile, policymakers—who usually aren't technologists—have scrambled to educate themselves about the intricate global supply chains that still link the United States, China, and many other countries.

In 2019, I was appointed to be the chair of the NSCAI, a congressionally mandated bipartisan commission that was charged with "consider[ing] the methods and means necessary to advance the development of artificial intelligence, machine learning, and associated technologies to comprehensively address the national security and defense needs of the United States."[1] I worked with leaders in industry, academia, and government to formulate recommendations that would be adopted by Congress, the administration, and departments and agencies.

We were successful, but this effort did not go far enough. That is why I continue to advocate for major legislation (such as the United States Innovation and Competition Act and the America COMPETES Act), to develop the next phase of implementable policy options (through the recently launched Special Competitive Studies Project), to support bold and ambitious research on the hardest AI problems (via my new AI2050 initiative), and to elevate public discussion (in my latest book, *The Age of AI*, with Henry Kissinger and Daniel Huttenlocher).

Still, there is so much more work to do to secure America's technological future in the context of a rising China. Given the high stakes and dizzying complexity of the challenges, many U.S. leaders are still searching for a mental framework—a set of analytical tools to help them answer the most fundamental questions of strategy and policy. The China Strategy Group, a bipartisan group of thinkers and doers I convened with Jared Cohen in 2020, sought to develop those kinds of frameworks. One of our key findings was that such profound national dilemmas call for deeper analysis by a broader range of independent voices.

That's why I was so pleased to read Jon Bateman's major new report, "U.S.-China Technological 'Decoupling': A Strategy and Policy Framework." Jon is a brilliant thinker who has written an exceptional guidebook and blueprint for U.S. action. His report builds on recommendations outlined by the NSCAI and the China Strategy Group. It's a major achievement, and I strongly hope that policymakers pay attention to it.

There is no shortage of analysis today on U.S.-China tech policy, but Jon's report stands out for its ambition, clarity, and rigor. To start with, he avoids two of the biggest and most common pitfalls: offering hazy strategic ideas without explaining how to implement them,

or cataloging a laundry list of policies without any discernible strategy. Instead, Jon draws a straight line from the heights of American grand strategy to the trenches of agency decisionmaking. With this methodical approach he outlines a smart, achievable agenda for a remarkable range of U.S. national security and economic goals. I particularly appreciated Jon's prolific use of case studies to ground his proposals in technological reality.

Jon is not afraid to stake a position, and some of my favorite parts of his report were those that I disagreed with. He argues, for example, that the military importance of AI may be overestimated—or, at least, that the era of what China calls "intelligentized warfare" is probably still a long way away. I'll take the other side of that bet, but I still found Jon's analysis to be evenhanded and thought-provoking. And at this perilous moment in U.S. history, we simply can't afford groupthink. With calls for a hard "decoupling" getting louder, fewer people are willing to say (or even ask) where it all ends. Jon is one of those people, and I applaud him for it.

The paradoxes of the U.S.-China tech relationship are not going away. The United States will need to continually reassess whether and how to remain interdependent with our major international rival. The decisions will be difficult, the debates heated. Jon's report is among the best guides I have seen and will remain a touchstone for years to come.

Eric Schmidt
Co-founder, Schmidt Futures
Chair, Special Competitive Studies Project
Former CEO & Chairman, Google

EXECUTIVE SUMMARY

A partial "decoupling"[2] of U.S. and Chinese technology ecosystems is well underway. Beijing plays an active role in this process, as do other governments and private actors around the world. But the U.S. government has been a primary driver in recent years with its increased use of technology restrictions: export controls, divestment orders, licensing denials, visa bans, sanctions, tariffs, and the like. There is bipartisan support for at least some bolstering of U.S. tech controls, particularly for so-called strategic technologies, where Chinese advancement or influence could most threaten America's national security and economic interests. But what exactly are these strategic technologies, and how hard should the U.S. government push to control them? Where is the responsible stopping point—the line beyond which technology restrictions aimed at China do more harm than good to America?

The United States cannot afford simply to muddle through technological "decoupling," one of the most consequential global trends of the early twenty-first century.

These are vexing questions with few, if any, clear answers. Yet the United States cannot afford simply to muddle through technological decoupling, one of the most consequential global trends of the early twenty-first century. The U.S. technology base—foundational to national well-being and power—is thoroughly enmeshed with China in a larger, globe-spanning technological web. Cutting many strands of this web to reweave them into new patterns will be daunting and dangerous. Without a clear strategy, the U.S. government risks doing too little or—more likely—too much to curb technological interdependence with China. In particular, Washington may accidentally set in motion a chaotic, runaway decoupling that it cannot predict or control.

Sharper thinking and more informed debates are needed to develop a coherent, durable strategy. Today, disparate U.S. objectives are frequently lumped together into amorphous constructs like "technology competition." Familiar terms like "supply chain security" often fail to clarify such basic matters as which U.S. interests must be secured and why. Important decisions are siloed within opaque forums (like the Committee on Foreign Investment in the United States [CFIUS]), narrow specialties (like export control law), or individual industries (like semiconductors), concealing the bigger picture. The traditional concerns of "tech policy" and "China policy" receive outsized attention, while second-order implications in other areas (such as climate policy) get short shrift. And as China discourse in the United States becomes more politically charged, arguments for preserving technology ties are increasingly muted or not voiced at all.

This report aims to address these gaps and show how American leaders can navigate the vast, perilous, largely unmapped terrain of technological decoupling. First, it gives an overview of U.S. thinking and policy—describing how U.S. views on Chinese technology have evolved in recent years and explaining the many tools that Washington uses to curb U.S.-China technological interdependence. Second, it frames the major strategic choices facing U.S. leaders—summarizing three proposed strategies for technological decoupling and advocating a middle path that preserves and expands America's options. Third, it translates this strategy into implementable policies and processes—proposing specific objectives for U.S. federal agencies and identifying the technology areas where government controls are (or are not) warranted. The report also highlights many domestic investments and other self-improvement measures that must go hand in hand with restrictive action.

THE EVOLUTION OF U.S. THINKING AND POLICY

The U.S. government's interest in technological decoupling has risen dramatically since the mid-2010s. During this period, Beijing's growing strength and more troubling behavior at home and abroad led U.S. leaders to revise their views of China, deeming it America's primary state threat. At the same time, techno-nationalist ideas—depicting technology as an arena for interstate struggle rather than a neutral global marketplace—became ascendant around the world and eventually prevailed in Washington. Together, these two trends produced a new American techno-nationalism focused principally on China. It first took shape during former president Barack Obama's second term, was elevated and implemented under former president Donald Trump, and has been largely embraced by President Joe Biden.

Early U.S. actions were mainly "defensive": restrictive measures aimed at thwarting or containing Chinese technology threats. Export and import controls, inbound and outbound investment restrictions, telecommunications and electronics licensing regimes, visa bans, financial sanctions, technology transaction rules, federal spending limits, and law enforcement actions have more frequently and intensively targeted China. Lately, Washington has increased its

focus on "offensive" measures—positive actions to nurture America's own technological strength, such as investments in research and development (R&D) and education. Yet despite this offensive pivot, defensive measures continue to multiply and raise some of the most acute policy dilemmas. For example, cracking down on illicit Chinese technology transfer at U.S. universities can chill valuable scientific collaboration, and banning Chinese technologies on national security grounds may prompt Beijing (or others) to broaden their own trade barriers.

U.S. policymakers must have a firm grasp of the many different tools used to curb bilateral technology interdependence. 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. To clarify the picture, this report offers a primer on key U.S. defensive authorities and how they have targeted the Chinese tech sector.

Under U.S. law, officials have vast discretion to impose technological decoupling. They need only invoke pliable concepts like "national security" or "the public interest" to restrict how technology products, services, and inputs move between America and China. Most restrictive powers have been used to a small fraction of their full decoupling potential. At the same time, restrictive authorities are fragmented across multiple agencies and policy domains. This combination of great power and great complexity increases the risk that U.S. technology controls will be poorly conceived or work at cross-purposes. It is therefore essential to develop a government-wide strategy that can prevent overreach and align disparate elements into a coherent whole.

CHOOSING A STRATEGY

A U.S. strategy for decoupling should envision the kind of technology relationship that America hopes to have with China, provide a rationale for this vision, and explain how it can be made into reality. A sound strategy would start with a multidimensional assessment of U.S.-China tech ties and their wide-ranging effects on diverse American interests. In fact, a strategy for technological decoupling should consider more than just tech-specific or China-specific concerns. It should be rooted in a larger U.S. grand strategy that reconciles decoupling with other national priorities, from international trade to domestic political stability to global climate change, that might be impacted directly or indirectly. Washington still lacks such a decoupling strategy, even as it continually imposes new tech controls on China.

Leading proposals can be grouped into three general camps. First, a "restrictionist" camp believes that the U.S.-China technology relationship is zero-sum and that it tends to favor

Beijing, necessitating dramatic curtailment of bilateral tech ties. This group—including China hawks, some human rights defenders, and many national security officials—fears U.S. complacency during what it sees as a closing window to prevent China's technological dominance. Second, a "cooperationist" camp perceives U.S.-China tech ties as non-zero-sum and largely beneficial to America, casting doubt on key elements of Washington's decoupling agenda. This group—including many business interests, techno-globalist activists, and some progressives—fears U.S. overreaction, inflated threat perceptions, and excessive confidence in restrictive tools.

Third, a "centrist" camp identifies the U.S.-China tech relationship as complex and uncertain, with both zero-sum and non-zero-sum elements and mixed costs and benefits for both countries. Centrists want focused, finely tuned defensive measures plus large offensive investments. This group—including many mainstream think tank analysts, moderate political figures, and some state and local leaders—fears U.S. incapacity to balance interdependence and decoupling. Key capacity challenges include securing public-private coordination, mapping complex supply chains, and overcoming Washington gridlock, polarization, and bureaucratic clumsiness.

The United States should adopt a centrist strategy. The very existence of a heated debate among these three camps is itself an argument for the careful incrementalism that centrists espouse. We are still in the early years of a radically new phase in U.S.-China relations and only on the cusp of far-reaching global transformations promised by artificial intelligence (AI) and other emerging technologies. These coming changes, although unquestionably significant, remain difficult for present-day observers to assess. Policymakers should play for more time—preserving and expanding American options while the future comes into sharper focus.

The primary effort should be "offensive": new investments and incentives to bolster and diversify innovation pathways, supply chains, talent pipelines, and revenue models in strategic technology areas. The United States has far more influence over its own technological strength than it has over China's, and such investments act as a hedge against multiple scenarios. They can prepare America for full-scope technological decoupling with fewer costs and risks, should that become necessary, or they can position U.S. firms to compete better in a still-globalized technology marketplace.

Because offensive investments are challenging to implement and take a long time to pay off, fast-acting "defensive" restrictions should be used to buy time. Washington should institute controls in technology areas where China seems close to securing unique, strategically significant, and long-lasting advantages. Defensive measures can help to forestall Chinese breakthroughs long enough for U.S. offensive efforts to bear fruit.

However, restrictive tools should be confined to a secondary, supporting role and only used in compelling circumstances. Technology restrictions can be costly (harming U.S.

industries and innovators), imprecise (chilling more activity than intended), and even futile (failing to remedy the relevant Chinese tech threats). Restrictive tools by themselves cannot ensure U.S. technological preeminence over the long haul, but they can and should frustrate Chinese dominance in the short run, preserving competitive opportunities while America regroups and regains momentum in key technology areas.

A centrist strategy of this kind will also help the U.S. government maintain its control over the decoupling process—keeping its pace and scope aligned with American needs. U.S. policymakers have enjoyed the luxury of control during recent years, as Washington took the initiative while Beijing, other governments, and private entities around the world were comparably cautious and reactive in technological decoupling. But as decoupling accelerates, these outside actors increasingly seek to seize initiative for themselves—for example, preempting future U.S. restrictions by acting first to reduce technology interdependence on their own terms. Meanwhile, decoupling has slowly begun to shift power within the United States toward political figures, commercial actors, and national security voices who advocate even stronger restrictive measures.

Restrictive tools by themselves cannot ensure U.S. technological preeminence over the long haul, but they can and should frustrate Chinese dominance in the short run.

These dynamics create risks of unanticipated escalatory spirals. Washington might aim for a modest level of decoupling but end up with something broader, faster, and messier. In a worst-case scenario, the United States could accidentally set in motion a frenzied, ever-intensifying cycle of decoupling that races well ahead of what the nation can afford. A centrist strategy can minimize this risk by ensuring that technology restrictions are targeted and precise. The United States must then communicate this strategic intention, and share more details of specific policies, to help stabilize expectations in China and elsewhere. Such clarity cuts against the grain for U.S. leaders, who like to preserve their own discretion and struggle to make credible commitments across presidential administrations. But in a complex and interdependent global technology landscape, silence or ambiguity may actually cede control to others.

TRANSLATING STRATEGY INTO POLICY AND PROCESS

Any U.S. strategy—whether restrictionist, cooperationist, or centrist—must be translated into policies and processes to guide agency-level decisions. This is no simple task. It requires evaluating a host of technology areas, weighing numerous costs and benefits through the lens of multiple expert disciplines. Meaningful guidance must move past generalities and express clear policy choices, even in the face of uncertainty and a fraught domestic atmosphere. Thus,

although many observers say that technological decoupling should be bounded and partial, there are few comprehensive, detailed proposals for how and where to draw such boundaries.

To develop such guidance, this report unpacks the many U.S. interests at stake and proposes nine policy objectives for technological decoupling. National security objectives include maintaining a military edge over China, limiting Chinese national security espionage, preventing Chinese sabotage in a crisis, limiting Chinese influence operations, and denying support for Chinese or China-enabled authoritarianism and repression. Economic objectives include countering unfair Chinese practices and intellectual property (IP) theft, and competing and leading in strategic industries. Then there are ancillary objectives—non-technology goals that also influence American decoupling policy: obtaining general leverage over China, and shaping U.S. domestic narratives. These nine objectives, although linked, raise many distinct issues and dilemmas. They cannot be treated as interchangeable responses to an undifferentiated mass of "Chinese tech threats"—an all-too-typical approach.

The next step, and the heart of this report, is a careful review of the role U.S. technology controls should play in achieving these policy objectives (see Table 1). Taking each objective in turn, the report weighs the risks and benefits of U.S.-China technological interdependence against the risks and benefits of U.S. government technology controls. This analysis leads to a series of proposed dividing lines—implementable standards for determining which technologies warrant restrictions and which do not. Specific examples help illustrate how these dividing lines would work in practice. Offensive measures essential to each objective are also highlighted. By considering the full gamut of U.S. interests across many different technology areas, the report shows what a centrist decoupling might look like and how agencies could implement it.

This step-by-step process demonstrates several points that bolster the case for a centrist approach. First, the most strategically significant technologies (like 5G telecommunications equipment and semiconductors) are few in number and already subject to strong U.S. government controls. A handful of other technology areas may need tighter China-oriented restrictions—for example, drone swarms, the U.S. bulk power system, and technologies sold to Xinjiang. Yet certain China-focused controls seem counterproductive in a number of other high-profile areas, such as geolocation data, social media platforms, and consumer devices like smartphones. Second, official U.S. policy goals remain dangerously vague and open-ended. To avoid costly and quixotic technology wars, Washington must publicly clarify its vision for the global tech trade and set more achievable ambitions for countering techno-authoritarianism, maintaining a military edge over China, and preventing Chinese espionage, sabotage, and influence operations. Third, offensive policies have the greatest long-term potential for strengthening U.S. technology leadership, competitiveness, and resilience—and thereby achieving security and prosperity. Although technology restrictions are the primary subject of this report, they cannot be the primary focus of policymakers.

Table 1: Overview of Recommended U.S. Policies

	Proposed policy objective	Proposed standard for government tech controls	Illustrative policies	Key offensive measures
NATIONAL SECURITY	**Maintain a military edge over China**	Slow China's acquisition of technologies that could thwart U.S. defense planning objectives.	Consider controls for drone swarm hardware, but review sanctions on Chinese supercomputing organizations.	Speed up U.S. force transformation. Improve defense industrial base information and cybersecurity.
	Limit Chinese national security espionage	Deny China insider access to U.S. personal data it cannot otherwise readily obtain, whose loss would be hard to remedy.	Continue blocking sale of American genetics firms to Chinese entities, but allow sale of firms with geolocation data.	Pass national cybersecurity and data privacy laws. Improve defensive counterintelligence for U.S. government officials.
	Prevent Chinese sabotage in a crisis	Deny China a presence in systems that could disrupt major U.S. military contingencies or cause mass casualties or evacuations.	Reinstate ban on Chinese large power transformers, but narrow and clarify the sweeping ICTS supply chain security rule.	Invest in adversary-agnostic cybersecurity and all-hazards resilience of critical military and civilian systems.
	Limit Chinese influence operations	Prevent China from swinging a federal election or significantly reducing public confidence in elections or pandemic measures.	Permit Chinese ownership and operation of TikTok pending further analysis. Do not force Chinese divestment from U.S. video game developers based on influence threats.	Repair U.S. information ecosystem by regulating platforms, reforming election law, funding education and journalism, and facilitating basic research.
	Deny support for China-enabled authoritarianism and repression	Avoid U.S. complicity in Beijing's repression of minorities. Dissuade China from selling, and others from buying, repressive tech.	Sanction Chinese tech companies that support Xinjiang security operations, but clarify the "surveillance technology sector" authority.	Press Americans, U.S. allies, and others on the use or sale of repressive tech. Model liberal democratic tech policies at home.
ECONOMIC	**Counter unfair Chinese economic practices and IP theft**	Link U.S. technology controls to a comprehensive strategy for the international trade system.	Reconcile U.S. open trade aspirations with America's tech-related trade barriers and claims of a WTO "national security exception."	Cultivate a united front among U.S. allies about the WTO's future and China's role within it.
	Compete and lead in strategic industries	Prevent long-term Chinese dominance of tech industries expected to have the largest economic impact (and some national security nexus).	Maintain controls on 5G telecoms equipment, but generally avoid restricting AI software, smartphones, and Internet of Things on economic grounds.	Increase federal spending on R&D, STEM education and training, and innovation infrastructure. Step up antitrust scrutiny and reforms.
ANCILLARY	**Obtain general leverage over China**	Use technology restrictions as bargaining chips with Beijing in rare cases when they could advance supreme U.S. interests.	Consider leveraging Huawei sanctions to secure Chinese emissions reductions, but not to expand U.S. market access in non-technology sectors.	Build and sustain international coalitions to press China on key U.S. concerns.
	Shape U.S. domestic narratives	Raise domestic awareness about technology threats from China while minimizing politicization.	Use regularized processes instead of executive orders. Empower oversight elements.	Carry out responsible, factual domestic messaging campaigns. Listen to domestic stakeholders.

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]

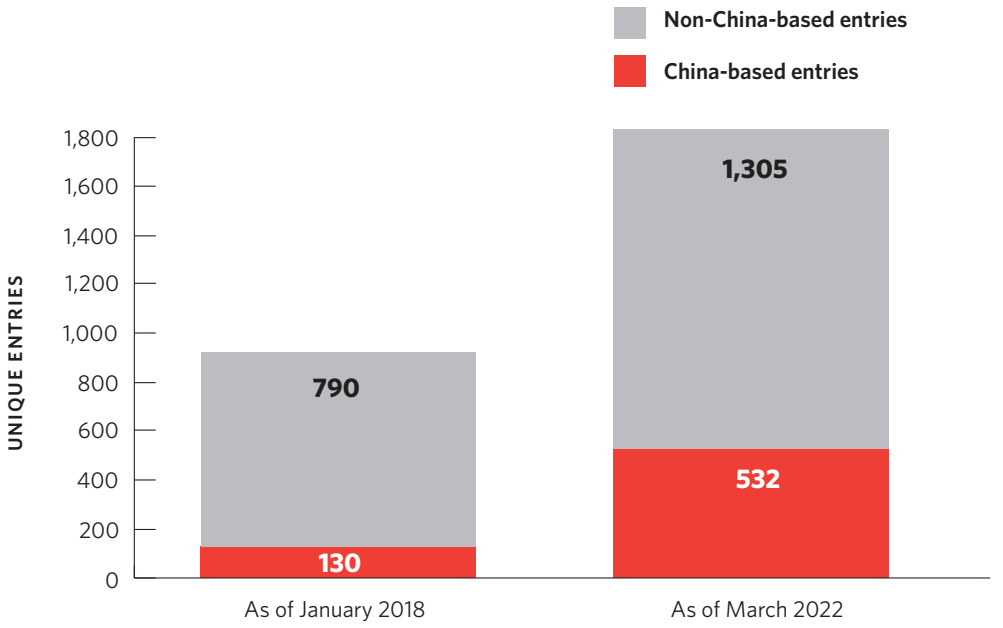
The EAR has multiple components, including a list-based regime called the **Commerce Control List (CCL)**. Each item on the CCL has one or more "reasons for control" that explain the listing's justification and determine which countries it affects. Relatively few reasons for control apply to Canada, 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]

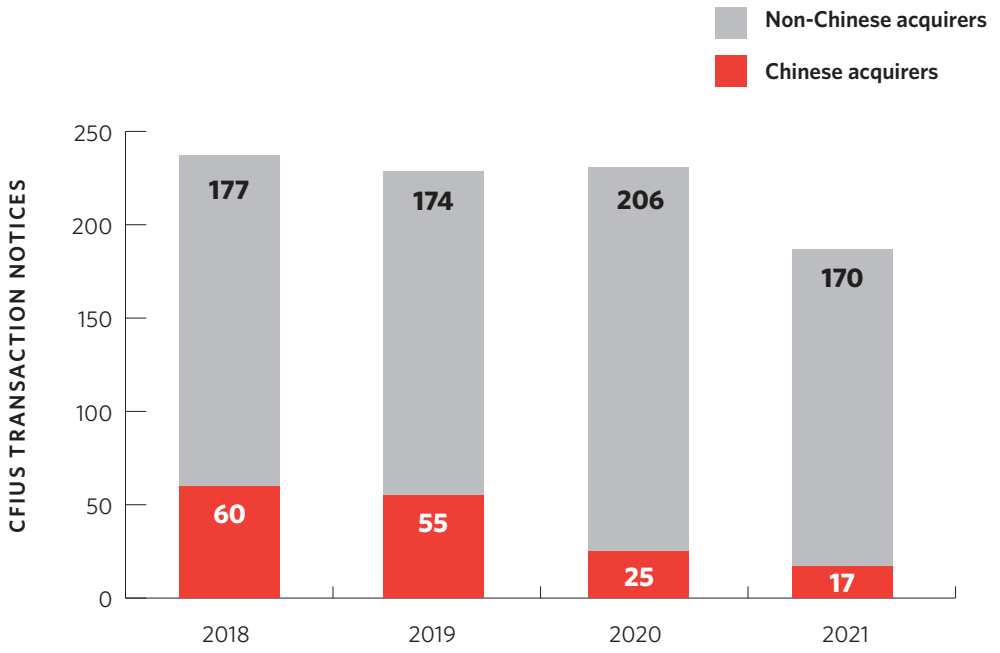
INVESTMENT RESTRICTIONS

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]

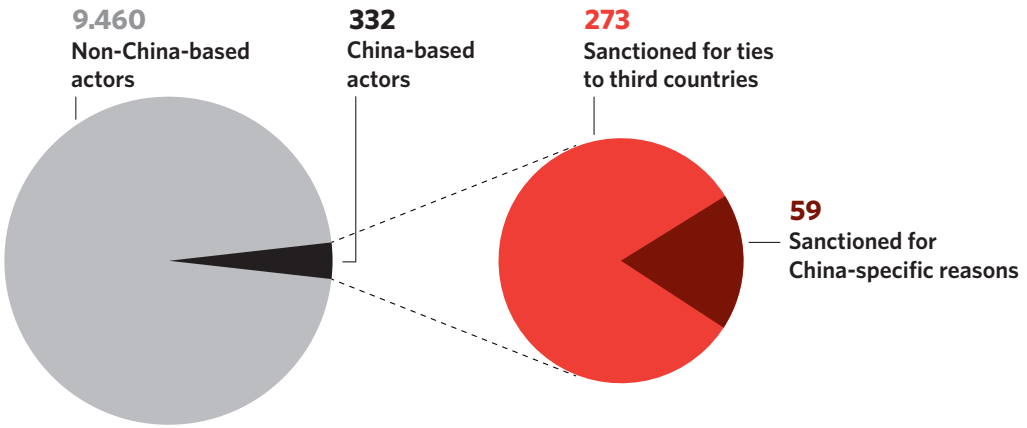
FINANCIAL SANCTIONS

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.

CHOOSING A STRATEGY

The dozens of new U.S. government technology controls aimed at China in recent years did not all have a single, unified objective. Some sought to counter national security threats, some were more economically motivated, and some had ancillary purposes (like domestic or diplomatic gamesmanship) unrelated to technology itself. Yet in public discourse, and even in policy circles, distinct objectives are often left undifferentiated or undefined. Too frequently, U.S. leaders and analysts speak of "countering" or "reining in" Chinese technology threats and risks—highly general formulations that elide key goals and trade-offs.

Untangling this jumble of U.S. objectives is an important first step in developing a coherent strategy. Table 5 describes nine apparent rationales for recent U.S. technology restrictions aimed at China.

The existence of so many distinct policy rationales is not surprising. The United States has many different concerns with China, and technology plays a significant part in nearly all of them. Technology is rightly at the heart of America's China policies. (The corollary idea, that China should be at the heart of U.S. tech policy, is more debatable.) In many cases, these policy rationales overlap and reinforce each other. For example, potential Chinese influence over U.S. telecommunications networks raises multiple fears simultaneously: theft of commercial secrets, tracking of U.S. government officials, injection of disinformation, or subversion of critical infrastructure in a crisis, among other possibilities. Hence the U.S. telecommunications sector was an early target for American restrictive measures, and the global telecoms marketplace remains a central preoccupation of Washington's tech diplomacy.

Table 5: Untangling the Many U.S. Rationales for China-Related Tech Restrictions

U.S. interest area	Rationale	Illustrative policy
National security	Maintaining a military edge over China	Since 2020, Chinese graduate students and researchers with institutional ties to Beijing's "military-civil fusion" efforts have been denied visas.
	Limiting Chinese national security espionage	In 2019, a Chinese company was forced to sell the dating app Grindr because the app's sensitive personal data could be used for intelligence targeting.
	Preventing Chinese sabotage in a crisis	Since 2019, U.S. telecommunications providers have been unable to receive federal subsidies to buy Huawei or ZTE equipment, partly due to sabotage fears.
	Limiting Chinese influence operations	In 2020, Trump ordered a ban on TikTok in part because the app could "be used for disinformation campaigns that benefit the Chinese Communist Party."
	Denying support for Chinese and China-enabled authoritarianism and repression	In 2019, Chinese tech companies, including Hikvision, Megvii, and SenseTime, were placed on the Entity List due to their involvement in Beijing's repression in Xinjiang.
Economic	Countering unfair Chinese economic practices and IP theft	The Trump administration's broad-based tariffs on China—aimed at countering unfair economic practices such as intellectual property theft—applied to many technology goods, including smart devices, flash memory devices, and electronic components.
	Competing and leading in strategic industries	U.S. controls on the export of American technologies to Huawei are especially strict for semiconductors and for any tech that would be used "with or in any 5G devices"—two areas considered strategic by Washington.
Ancillary	Obtaining general leverage over China	Trump described U.S. and allied actions against ZTE and Huawei as leverage in broader trade talks. In the Phase One deal, he used this leverage to gain concessions in non-tech areas like agriculture and financial services.
	Shaping U.S. domestic narratives	Shortly before the 2020 election, the Trump administration released new H1-B visa restrictions that would have significantly affected Chinese high-tech workers.

THE NEED FOR BETTER STRATEGY

However, a long list of policy aims is not the same as a strategy. In fact, it can be anathema to one. Many of these goals are vague and have no clear limiting principle. They can also come into conflict with each other, or with other U.S. national priorities. A good strategy would clarify key objectives and prioritize them. It would also proffer a theory of success—a realistic basis for determining which forms of technological decoupling will actually achieve U.S. aims. So far, Washington has struggled to articulate such a strategy.

Without more strategic *clarity*, decoupling can become overaggressive or incoherent and contrary to U.S. interests. For example, the U.S. military does not need (and cannot achieve) unlimited advantages over China's military in every place, time, and domain. The United States must define its desired "military edge" over China in more specific terms. Likewise, if Washington seeks to rebalance the terms of bilateral economic competition, it should have a desired model of the global economy in mind. Are U.S. policymakers aiming for two largely separate international economic systems, or would China remain integrated within a modified global economy? And is the point to maximize U.S. prosperity and technology leadership, or to minimize China's (which are not the same thing)?

A long list of policy aims is not a strategy. Washington has struggled to clarify key objectives, prioritize them, and proffer a theory of success.

Without a sense of strategic *priorities*, decoupling can cause havoc as one objective smashes into another. Barring Chinese graduate students helps to reduce illicit technology transfer, but it also hampers U.S. technological competitiveness by spurning a key source of skilled labor.[187] Which goal takes precedence? Technological decoupling is fraught with these kinds of costs and risks—and unfortunately, their ripples can spread far beyond the technological realm, affecting seemingly unrelated U.S. goals. For example, harsh U.S. measures against Huawei and TikTok have helped convince many in Beijing that Washington seeks wholesale economic containment. In climate change talks, China may now be even more liable to view proposed emissions reduction targets as a stealth means of stifling its economic growth.

Finally, without a strategic *theory of success*, decoupling may fail to accomplish much of anything good. U.S. efforts to prevent the flow of sensitive technology into China—for example, equipment for manufacturing 5- and 7-nanometer node microchips—require cooperation from many other countries that participate in the supply chain or have access to the same sensitive technology. Without this cooperation, technology controls can be futile and ultimately self-defeating. Which countries, or multilateral institutions, would belong to the U.S. "side" of trusted partners in a given technology area? What mixture of inducement, pressure, and persuasion could succeed in bringing those countries on board and/or reshaping multilateral institutions for this purpose? And when are these diplomatic efforts really worth the payoff?

THE CURRENT U.S. STRATEGY DEBATE

After the chaos and inconsistency of the Trump years, Biden will need a more rational approach—clearly defining U.S. objectives for decoupling and articulating a strategy to

achieve them. This is a high stakes challenge. Technology is a key determinant of American national well-being and power, and a central arena of U.S.-China strategic competition. It is also fraught with risk and uncertainty. Too much interdependence with China could leave the U.S. economy, society, and national security apparatus vulnerable to espionage or subversion, and make America complicit in Chinese technological abuses. Yet too much decoupling could impair the U.S. tech ecosystem, further destabilize the bilateral relationship, and alienate U.S. allies and trading partners caught in the crossfire.

There is heated debate about how the United States should thread this needle. To grossly oversimplify, one can define three general camps (see Table 6).[188]

Restrictionists. First, what might be called a "restrictionist" camp calls for dramatically curtailing U.S.-China technology ties. The harshest proposals come from China hawks like Matt Pottinger (who has advocated expanding U.S. outbound investment restrictions "by at least an order of magnitude"), Derek Scissors (who has recommended far tougher export controls and an "outbound version of CFIUS"), and Senator Tom Cotton (who has proposed a "research blockade" on China, sweeping export controls on high-end semiconductors, secondary sanctions amounting to a "death sentence" for China's "national champions," and revocation of Permanent Normal Trade Relations).[189]

Some human rights advocates also have restrictionist leanings: twenty-four NGOs including Human Rights Watch, Freedom House, and PEN America have called for "a series of escalating actions against technology companies found to be contributing to China's mass surveillance, including by imposing Global Magnitsky sanctions," while *New York Times* columnist Farhad Manjoo suggested that technological and economic integration with China "isn't worth the moral cost."[190] And restrictionist sensibilities seem fairly common within U.S. national security officialdom, particularly in the military and the Intelligence Community (IC). In 2019, Chairman of the Joint Chiefs of Staff General Joseph Dunford expressed "great concern" that U.S. tech firms provide "indirect benefit" to the PLA when they operate and conduct research in China.[191]

Restrictionists tend to define bilateral tech ties as zero-sum: China gains long-term strategic advantages while America reaps only marginal and transitory gains.

As these examples indicate, restrictionists have varied diagnoses of the problems they seek to solve and the appropriate U.S. policy response. One common view holds that Beijing is successfully executing a long-term plan to sap American global strength and attain regional or even global hegemony.[192] Technology is seen as central to China's plans, allowing Beijing to steal U.S. secrets, leapfrog U.S. military capabilities, bolster its own and other countries' repressive capabilities, and more. Restrictionists therefore tend to define bilateral tech ties as zero-sum: China gains long-term strategic advantages

by exploiting U.S. tech industries and systems, while America reaps only marginal and transitory gains, like paying lower prices for China-derived tech goods. Accordingly, restrictionists favor broad-based technological decoupling aimed at denying China meaningful opportunities to draw support from, or establish influence within, the U.S. tech ecosystem. Hal Brands, for example, has proposed that Washington "work with allies to slow Chinese innovation through technological denial policies."[193] Some restrictionists go beyond mere decoupling and argue that U.S. tech controls should be designed to harm and ideally destroy major Chinese tech companies, such as Huawei.

Cooperationists. At the other end of the spectrum, a range of what might called "cooperationist" voices have opposed major elements of Washington's technological decoupling agenda. U.S. business interests often tout the economic and technological importance of maintaining global supply chains and market access to China. For example, Google warned that Huawei's Entity List designation could create cybersecurity vulnerabilities, and the Semiconductor Industry Association has argued that "America's longstanding leadership in semiconductors is put at risk by broad restrictions on U.S. exports of commercial chip technologies to China."[194] Meanwhile, some independent technologists and tech activists—including key pioneers of the early internet—remain vocally committed to techno-globalist ideals and view decoupling as anathema. The World Wide Web Foundation (joined by Amazon, Facebook, Microsoft, Twitter, and others) has warned against "internet fragmentation" and "techno-protectionist initiatives," while the Internet Society believes that "having a government dictate how networks interconnect according to political considerations rather than technical considerations, runs contrary to the very idea of the Internet."[195]

Cooperationists often posit that a twenty-first-century system of open technology collaboration would reproduce the waves of innovation and widely shared global progress said to characterize the late twentieth century. And the United States—with its historically dynamic innovation system—would be well positioned to lead within and benefit from such an environment. They also argue that many technology controls are simply unworkable, given the practical difficulties of predicting technological change and regulating cross-border flows in an already globalized, digitized world.

Cooperationists often posit that the United States would be well positioned to lead and benefit from a twenty-first-century system of open technology collaboration.

Another strain of cooperationism exists among progressives, who caution against overinflating Chinese (and other foreign) threats. Senator Bernie Sanders, for example, has argued that "the growing bipartisan push for a confrontation with China" fuels wasteful spending, militarism, bigotry, and authoritarian populism at home while reducing the likelihood of cooperation on key global issues.[196] Applying this critique to U.S. tech policy, Sanders has described proposed federal investments in semiconductors as a form of corporate welfare.[197]

Others have blamed the China Initiative for fomenting xenophobia and racism toward U.S.-based academics of Chinese nationality or ethnicity.[198] In addition, some progressives cite climate change as an area where U.S.-China technology cooperation must greatly increase, not decrease. More than forty activist groups—including MoveOn, the Sunrise Movement, and the Union of Concerned Scientists—have urged the Biden administration to "speed the [global] transition away from dirty energy economies" by marrying U.S. clean tech with Chinese industrial capacity.[199] (On the other hand, progressive concerns about Chinese human right abuses and untrammeled free trade lead some on the left to favor more tech restrictions.[200])

Centrists. Between the poles of restrictionism and cooperationism lies what might be called a "centrist" camp, which seeks to incorporate the best insights of each side while making more room for complexity and uncertainty. Centrists agree with restrictionists that Beijing poses unique long-term challenges to the United States and that technology is a central risk factor. But, echoing cooperationists, they think that some Chinese tech threats are exaggerated, offset by the benefits of cooperation, and only partially addressable via China-focused governmental restrictions. Centrists generally endorse the overall U.S. shift toward partial technological decoupling and accept that decoupling must progress further to protect U.S. national security and economic security. However, they want new technology controls to be carefully scrutinized; they doubt the viability or wisdom of dividing the world into sealed geo-technological blocs. Centrists view Chinese military aggression as a major possibility and question Beijing's willingness to partner on global issues like climate change and pandemics. Yet they insist that co-existence and collaboration on urgent challenges must still be tried, and so they hope to avoid a technological confrontation that would take bilateral relations to a breaking point. Some centrists emphasize how much we still do not know about China's long-term path and the ultimate impacts of emerging technologies, and therefore recommend hedging strategies to account for multiple possible futures.

A leading centrist statement is the China Strategy Group report co-led by Eric Schmidt and Jared Cohen. It argues that "some degree of disentangling is both inevitable and preferable," yet "we [should] seek to avoid unnecessary and counterproductive levels of separation."[201] Many other centrists can be found in technocratic bastions such as mainstream Washington think tanks and academic policy centers. Stephanie Segal of the Center for Strategic and International Studies developed a cost-benefit framework to assess U.S.-China interlinkages; she found that "existing [U.S. government restrictions] go a long way in protecting national security" and that further decoupling should be "targeted" and rigorously evaluated.[202] Richard Danzig and Lorand Laskai, summarizing a body of research on technological decoupling commissioned by the Johns Hopkins University Applied Physics Laboratory, advocated "an incremental approach rooted in the indeterminacy of the current moment and recognition of the fact that interdependence is likely to continue."[203] Samm Sacks of New America and others have promoted the "small yard, high fence" concept.[204] This popular metaphor, attributed to former U.S. secretary of defense Robert Gates, conveys that

technology controls should be the exception instead of the rule, applying only to the most sensitive and strategic areas.[205]

Centrists have promoted the "small yard, high fence" metaphor to convey that technology controls should apply only to the most sensitive and strategic areas.

The centrist approach to technological decoupling has been embraced by some moderate political figures as well. Senator Chris Coons has also endorsed the "small yard, high fence" metaphor and has proposed "safeguard[ing the] crown jewels of technology" while "strik[ing] the right balance to avoid [full-scale] decoupling of global tech industries between the United States and China."[206] A quiet centrism may also exist at the state and local level. The Carnegie report "Making U.S. Foreign Policy Work Better for the Middle Class," published in 2020, drew on interviews of state and local government, business, labor, and community leaders and middle-income workers in Colorado, Nebraska, and Ohio. Most interviewees "want[ed] the United States to push back more effectively against unfair Chinese trading practices and make investments at home to compete more successfully with China. But otherwise they tend[ed] to see China pragmatically and [were] not inclined to view the geopolitical rivalry as an organizing principle of U.S. foreign policy."[207] (More recent surveys by the Chicago Council on Global Affairs found that the general American public has become "dramatically" more hostile to U.S.-China trade since 2019.[208])

Like the other camps, centrists have diverse policy ideas but tend to unite around a few general principles. First, centrists say that U.S.-China technological decoupling should be selective and targeted. Second, they want decoupling to be coordinated multilaterally. Centrists observe that the United States is a leading, but not exclusive or indispensable, player for many technologies. This means that unilateral U.S. controls are often ineffective, resulting only in self-imposed competitive disadvantages and friction with international partners. Therefore, Washington should work with so-called like-minded countries (in particular, technologically advanced liberal democracies) to create shared policy frameworks.[209]

Third, centrists insist that "defensive" efforts to curb or thwart Chinese technology threats cannot distract from a core "offensive" program to strengthen U.S. and allied technology ecosystems. Washington has only so much influence over the course of Chinese technological advancement, centrists argue, but there is far more the United States can do to improve its own technological strength. Moreover, many of the problems commonly framed as Chinese technology threats are partially, or even mostly, the result of domestic American challenges. For example, supply chain insecurity (a central focus of China-oriented technology controls) stems in part from industrial consolidation and workforce shortages in the United States; disinformation targeting Americans (a growing concern of China tech watchers) is a largely homegrown problem. According to the centrist view, U.S. policy should primarily focus on supporting America's own technology leadership, competitiveness, and resilience. Countering China would be a secondary priority.

Table 6: Three U.S. Camps Offer Competing Strategies for Technological Decoupling

Camp	Beliefs	Adherents
Restrictionists	• U.S.-China tech relationship is zero-sum and tends to advantage China • U.S. has a short window in which to prevent Chinese technological dominance • U.S. should greatly expand tech restrictions aimed at China	• China hawks • Some human rights defenders • Many national security officials
Cooperationists	• U.S.-China tech relationship is non-zero-sum and tends to benefit the U.S. • Americans often inflate China-tech threats • Major U.S. tech restrictions are domestically harmful and internationally destabilizing	• Many business interests • Techno-globalist activists • Some progressives
Centrists	• U.S.-China tech relationship has both zero-sum and non-zero-sum elements with mixed costs and benefits for both countries • More U.S. tech controls are needed but these should be selective, carefully designed, and multilateral • U.S. should focus on nurturing its own technological strength and tech policymaking capacity	• Many mainstream think tank analysts • Some moderate politicians • Some state and local leaders

Implications. This three-camps taxonomy is admittedly crude. Individual people and institutions do not self-identify with these labels and may not agree with them. Each camp is internally diverse and their boundaries overlap and shift. Still, the taxonomy helps to reveal some of the major questions and choices facing U.S. policymakers.

It is clarifying, for example, to compare what each camp sees as the greatest risks for U.S. policy. Restrictionists most fear U.S. *complacency* during a brief window when China's tech-driven dominance can still be prevented. Cooperationists most fear U.S. *overreaction* resulting from inflated perceptions of Chinese tech threats and excessive confidence in restrictive measures. Centrists, hoping to avoid both these perils, most fear U.S. *incapacity* to achieve a successful balance. Key capacity challenges include securing public-private coordination, mapping complex supply chains, and overcoming Washington gridlock, polarization, and bureaucratic clumsiness. Ultimately, U.S. leaders must choose which fears (and hopes) they most identify with.

This taxonomy also gives a rough guide to the changing direction of U.S. thought and policy. Cooperationism was the dominant view when Obama took office, and it still had some currency by the time he stepped down. The Trump administration's policies and rhetoric became increasingly restrictionist over four years—though it sent contradictory signals, and Trump departed before a fully restrictionist vision could be realized. The Biden administration has so far retained much of the Trump policy architecture, while speaking a language that sounds more centrist. For now, the center of gravity in Washington seems to lie somewhere between the centrist and restrictionist positions.

Restrictionists fear U.S. complacency toward Chinese tech threats, while cooperationists fear U.S. overreaction. Meanwhile, centrists fear U.S. incapacity to navigate between both perils.

A CASE FOR A CENTRIST STRATEGY

The debate among restrictionists, cooperationists, and centrists cannot be resolved by a policy paper. Part of what separates these camps are divergent worldviews and values—deep-seated disagreements about American priorities and purposes. The three camps also disagree about more tangible questions, such as how to understand China's capabilities and intentions, what kind of political economy will produce the most innovation in the coming decades, and how much influence the United States will have in shaping global technological choices. The answers to these questions will not be known for decades. For now, strategists and policy experts can only venture their best assessments based on incomplete data and personal beliefs—and, for some, perceived political advantage. Indeed, the biggest drivers of real-world U.S. strategy will probably be political: partisan dichotomies, public sentiment, business interests, media attention, and civil society advocacy.

Despite these limitations, expert analysis can still help to inform and guide political and public dialogues about U.S.-China technological decoupling. Analysts can present the strongest, clearest versions of each strategic position, and continually sharpen and disseminate their ideas in the face of critiques and evolving evidence. In that spirit, below are two brief arguments in support of the centrist position. First, narrow and targeted China-focused technology restrictions can buy time for more positive U.S. investments to bear fruit, while reducing the costs and risks of decoupling. And second, a clearly articulated centrist strategy can help Washington maintain control of the pace and course of technological decoupling, thereby helping to prevent a runaway cycle that moves faster and further than U.S. leaders want.

BUYING TIME

The very existence of a heated debate among restrictionists, cooperationists, and centrists is itself an argument for the careful incrementalism that centrists espouse.[210] We are still in the early years of a radically new phase in U.S.-China relations, and we are only at the cusp of far-reaching global transformations promised by AI and other emerging technologies. These coming changes, while undoubtedly significant, remain difficult for present-day observers to assess. How will China's strategic intentions and technological capabilities change as the country further develops? How will cross-border data flows, new energy tech, or quantum computing reshape the global economy and security environment? How will countries of the world (and multinational companies) align themselves in a more fractured geo-technological landscape? How will the familiar costs and benefits of U.S.-China technological interdependence shift in the coming decades? There is simply no reliable way to answer these questions today. Policymakers should therefore play for time—preserving and expanding American options while the future comes into sharper focus.

Offense and defense. The primary effort should be a positive program to strengthen U.S. and allied technology ecosystems from within (the so-called "offensive" agenda). An offensive program would include new investments and incentives to bolster and diversify innovation pathways, supply chains, talent pipelines, and revenue models in strategic technology areas.

Such investments make sense regardless of how U.S.-China technology relations develop over time. If the United States ultimately concludes that full-scope technological decoupling has become necessary, then offensive investments will have prepared America to separate with fewer costs and risks. But if American leaders eventually decide to maintain substantial tech ties with China, then the offensive measures will have positioned U.S. firms to compete more effectively in a globalized technology marketplace. Moreover, many offensive investments are worth making for their own sake, irrespective of the China challenge. Even if China did not exist, concerted efforts to strengthen the U.S. technology base would still help boost American productivity and economic dynamism.

Offensive investments like education and R&D take a long time to pay off. Conversely, "defensive" measures—government restrictions aimed at thwarting Chinese technological advancement or influence—are fast-acting and readily implemented. They should therefore be used to buy time for the offensive agenda to bear fruit. Specifically, Washington should impose new controls in technology areas where China seems close to securing unique, strategically significant, and long-lasting advantages. In such circumstances, defensive measures can help to forestall Chinese breakthroughs long enough for the United States to regroup and regain technological momentum.

Defense is not risk-free, however. U.S. tech controls can be costly (harming U.S. industries and innovators), imprecise (chilling more activity than intended or desired), and even fu-

tile (failing to substantially remedy the relevant Chinese tech threats). And these side effects can be hard to predict, measure, and control. That is why restrictive tools should be confined to a secondary, supporting role and only used in compelling circumstances. Restrictive tools by themselves are incapable of ensuring U.S. technological preeminence over the long haul, but they can and should be used to frustrate Chinese dominance in the short run. The right U.S. technology controls can help to preserve competitive opportunities while American offensive efforts better position the country to succeed and lead in key technologies.

Fast-acting and readily implemented "defensive" restrictions can buy time for "offensive" investments, like education and R&D, to bear fruit.

Comparing technology areas. Consider 5G telecommunications equipment. The United States and many other countries have been in the process of purchasing large-scale 5G infrastructure that will likely operate for many years, providing the supplier country with a long-lasting technological beachhead as well as durable economic and political influence. Until 2019, Huawei and ZTE appeared set to secure Chinese dominance of the global 5G telecoms marketplace—occupying, for the foreseeable future, some of the most strategic terrain in cyberspace.[211] Although no U.S. company competed on a one-for-one basis with Huawei or ZTE, multiple U.S. national security and economic interests were nevertheless at risk: protecting secrets, preventing sabotage, blunting the global influence of an adversary, and more. This was a closing window of opportunity if there ever was one, and a clear impetus for defensive measures.

In response, the United States imposed a barrage of restrictions on ZTE and even more on Huawei: the Entity List, the Covered List, the Non-SDN Chinese Military-Industrial Complex Companies List, the Section 889 blacklist, the special foreign direct product restrictions, the "remove and replace" rule, federal indictments of Huawei and its CFO, and visa bans for certain employees, among other actions.[212] Washington also waged a unique diplomatic campaign (branded for a time as "The Clean Network") to dissuade third countries from buying Huawei and ZTE 5G equipment.

These moves were reasonably successful: several major countries opted not to purchase Chinese 5G gear, improving the market position of European competitors.[213] Most important, an open 5G architecture called O-RAN was given precious time to develop as a serious alternative, reducing the prospects of Chinese vendor lock-in and creating new openings for U.S. firms.[214] Meanwhile, Washington took active steps to manage the costs of its telecoms decoupling efforts. It has paid for small U.S. carriers to replace Huawei and ZTE equipment, helped finance certain third-country purchases of Western-made 5G gear, allowed U.S. chipmakers to retain some Huawei business, and drafted legislation to infuse the U.S. semiconductor sector with new federal funds.[215]

5G telecommunications equipment provided an especially compelling case for U.S. restrictions, because the United States faced a closing window of opportunity to prevent Chinese dominance of a strategic technology. But each technology area has a different strategic profile, and few of them will present as clear-cut a case for so many restrictive measures. AI software, social media platforms, smartphones, drones, Internet of Things devices, routers, advanced batteries, semiconductors, cloud services: they all have distinct national security implications, economic impacts, marketplace dynamics, supply chains, and innovation trajectories. In many cases, strong new U.S. government technology controls could do more harm than good.

Balancing global challenges. One reason for caution is the existence of other urgent crises, beyond Chinese tech threats, that compete for Washington's resources and attention and can sometimes clash with technological decoupling. Even as the United States engages in bilateral power struggles with China (and other state adversaries), it faces global and domestic challenges that are arguably still more daunting and have their own closing windows of opportunity. At a global level, COVID-19 exemplifies the perils of today's interconnected world. Contagions—in the form of infectious diseases, financial crises, or cyber catastrophes—loom on many fronts, requiring new forms of collective action across geopolitical divides.[216] The most obvious of these enormous threats is climate change.

While decoupling might seem like a solution to excess interconnectedness, global challenges cannot be solved without deep global cooperation. If Washington and Beijing cannot come together with others to address shared risks, then any U.S. national accomplishments may be washed out by a rising tide of global calamity. It is imperative that U.S. government policies toward China—including tech policy—address these larger problems and avoid making them worse.

Even as the United States engages in bilateral power struggles with China, it faces global and domestic challenges that are arguably still more daunting and urgent.

For example, Washington should think twice before walling itself off from Chinese clean energy technology such as solar cells, wind turbines, and advanced batteries. Granted, some Chinese clean tech companies have benefited from unfair practices like intellectual property theft, and the United States has powerful motivations to protect and nurture its own industries in these emerging strategic sectors.[217] Yet the world has years, not decades, to avoid catastrophic and irreversible climate damage; any delays in the deployment of low-carbon-intensive infrastructure would require powerful justifications.[218] By the same token, U.S. sanctions on Beijing's national tech champions should avoid inflicting so much Chinese economic pain that bilateral climate cooperation breaks down. In September 2021, China's climate envoy made the not-unreasonable case that climate "cannot possibly be divorced" from other friction points: "The U.S. side hopes

that climate cooperation can be an 'oasis' in China-U.S. relations, but if that 'oasis' is surrounded by desert, it will also become desertified sooner or later."[219]

Balancing domestic challenges. Domestically, the U.S. political system is floundering, its social cohesion fraying, and its economic promise hollowing for too many people. These trends have complex, multi-decadal causes but have dangerously accelerated in recent years. It was only a year ago that the United States suffered an abortive insurrection, and most experts believe that American democracy remains unstable. U.S. policymakers must therefore focus much of their attention on the home front, even at some risk to traditional national security priorities such as addressing Chinese tech threats.[220] For example, the U.S. government's ongoing crackdown on Chinese graduate students and researchers cannot be allowed to trigger a mass exodus of Chinese undergraduates, who pose little security risk yet pay billions of tuition dollars, in effect subsidizing educational opportunity for many Americans.

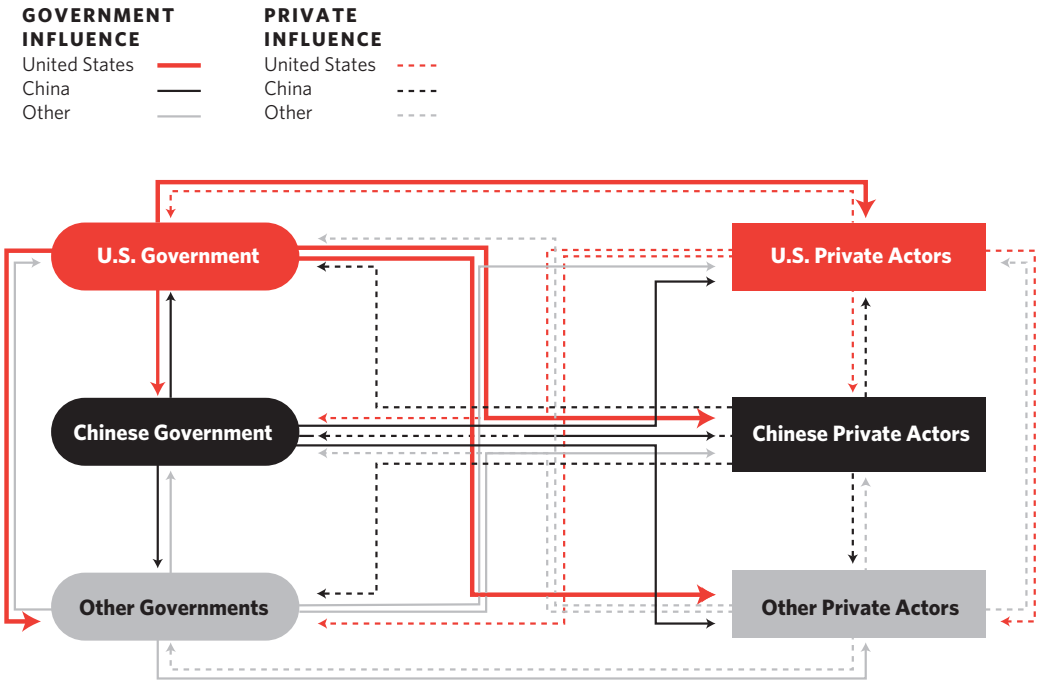
In sum, an overaggressive technological decoupling can set back other national priorities that may matter more or come to a head sooner. This does not negate the risks of U.S.-China technological interdependence, which are real and will likely grow in years ahead. But the United States must balance the troubling possibilities of tomorrow against the lethal dangers of today. This means buying additional time for U.S. leaders to assess geotechnological developments, juggle domestic and global crises, and implement long-term investments in American technological strength. Select defensive measures can extend these timelines—helping to lay the groundwork for greater technological independence in the future, should it become needed, even as most U.S.-China tech ties are allowed to endure for now. Balancing in this way can help hedge against multiple scenarios, from full-scope decoupling to relative technological integration.

MAINTAINING CONTROL

Time is one of two decisional resources that Washington must conserve as it manages technological decoupling. The other key resource is control over the decoupling process—the ability to set its pace and scope so that decoupling aligns with American needs. Granted, the U.S. government has never had total control. Beijing maintains its own long-standing limits on foreign technology; other governments have significant influence on global supply chains and markets; and companies around the world make private calculations about cross-border investments and deals. Nevertheless, the distinct wave of technological decoupling that began in the mid-2010s was initially of Washington's design—set in motion by the U.S. government's purposeful, albeit ill-coordinated campaign of China-oriented restrictions. Other actors have been comparably reactive (maneuvering in response to U.S. policy) and cautious (often seeking to conserve the status quo ante). This kept the U.S. government in the driver's seat, letting American officials advance decoupling as they saw fit while stopping short wherever they perceived risks to U.S. interests.

That privileged position could not last for long. As decoupling progresses, various foreign and domestic actors have increasingly sought to seize initiative for themselves—seeking to shape the decoupling process rather than remain at the mercy of U.S. government policy. These dynamics, explored below, create a risk of feedback loops: each new U.S. technology control strengthens the incentives for others to retaliate in kind, or to get ahead of the next Washington restriction, which accelerates decoupling beyond what U.S. officials intend. If Washington fails to monitor and manage these escalatory dynamics, it could accidentally set in motion a frenzied, ever-intensifying cycle of decoupling that races well past what America can afford.

Figure 4: The U.S. Government Is Just One of Many Actors Shaping Technological Decoupling



Source: Author's elaboration.

Preemptive action by outside actors. The first kind of feedback loop involves outside actors seeking to anticipate and preempt future rounds of U.S. technology restrictions. Now that U.S.-China technology decoupling is well underway, companies, universities, investors, and other actors around the world want to avoid being caught in the maelstrom. This means not making significant long-term commitments that could be vulnerable to collapse if the U.S.

government decided to impose new technology controls. In essence, these actors could "self-decouple" now, on their own terms, rather than risk a more abrupt and forceful U.S. government mandate later. The more restrictive measures that Washington imposes, the more outside actors will look to stay ahead of the curve. The consequences could potentially snowball, causing much more extensive technological decoupling than the U.S. government intends.

Companies and foreign governments could "self-decouple" now, on their own terms, rather than risk a more abrupt and forceful U.S. government mandate later.

A vivid example came in July 2020, when the Justice Department announced the indictment of six Chinese researchers for hiding their affiliations with the PLA. Following these *six* indictments, *more than one thousand* other Chinese researchers reportedly left the United States. "The breadth and depth of the exodus was not expected," an anonymous U.S. official told the *Washington Post*.[221] James Mulvenon, who has written extensively on China tech threats, told the newspaper that "he does not believe there were 1,000 active PLA-linked researchers in the United States but said it is possible many researchers affiliated with state institutes and universities left over the last year because they feared they might lose their fellowships." In other words, the U.S. government failed to anticipate that its small action would trigger a huge counterreaction, disrupting vast amounts of legitimate research activity. In the end, the Justice Department dropped charges against five of the six defendants. Still, it claimed to have "advanced our deterrence objectives," citing the mass exodus of Chinese researchers as a positive development.[222] The whole episode casts significant doubt on Washington's ability to predict and adequately weigh the collateral consequences of its China-tech actions.

Chilling effects from vague restrictions. The episode also illustrates a more general problem: vague or opaque U.S. government restrictions can chill far more technological activity than policymakers intend. There are many impediments to designing precise U.S. controls. Major "technologies" that Washington seeks to protect (such as AI, 5G, microelectronics, and drones) are really high-level constructs and systems-of-systems built from multiple interlinked technology families. Their smaller subelements (for example, advanced batteries that might power drones or electric cars) have complex global supply chains and innumerable uses and users. Agencies struggle to divvy up this mass of technological interconnections into clean administrative categories. And their criteria for doing so—premised on such notions as "national security" and, increasingly, "economic security"—are poorly conceptualized and highly contested. Early-stage technologies pose particular regulatory challenges because their future impact can only be guessed.

In the face of these uncertainties and administrative dilemmas, U.S. government agencies often take what they view as a cautious approach. They announce broad, open-ended authorities that would permit—but not require—a sweeping range of new government

technology restrictions. The government can then apply these authorities on a case-by-case basis, deliberating in secret and weighing a host of variables. This approach maximizes flexibility: enforcement can be dialed up or down based on new data, circumstances, and political imperatives. Its ambiguity also makes it harder for adversaries to identify and exploit loopholes in Washington's decisionmaking framework. Examples of this approach include CFIUS reviews, enforcement of the Commerce Department's new ICTS supply chain security rule, the licensing process for many export-controlled items, and designations under many sanctions authorities.

U.S. agencies often announce broad, open-ended restrictive authorities they can then apply on a case-by-case basis, deliberating in secret and weighing a host of variables.

However, too much discretion can ultimately be self-defeating. A major risk is that outside stakeholders see these opaque technology control regimes as risky and unpredictable, thereby chilling activity that could otherwise benefit the United States. Consider the Trump administration's visa ban for Chinese graduate students and researchers affiliated with Beijing's "military-civil fusion" programs; the ban left many key terms undefined, including what affiliations would be disqualifying. The policy's ambiguity generated widespread confusion about its scope and impact. A rigorous analysis by Georgetown's Center for Security and Emerging Technology tentatively "suggest[ed] 3,000 to 5,000 as a reasonable range for the annual number of students affected," calling this "a low-confidence estimate" and warning that the real number "would be much larger" if "military-civil fusion" was interpreted more broadly than the report assumed.[223] (The study was "unable to assess" the impact on Chinese nonstudent researchers due to a lack of publicly available data.) Today, more than eighteen months after the policy was announced, there is still no official public account of its key parameters.

Confronting this uncertainty, many Chinese graduate students and researchers can be expected simply to avoid applying to U.S. universities. Many U.S. universities will likewise avoid admitting or hiring certain Chinese applicants—even in cases where there was no national security risk and a visa might actually have been granted. (U.S. officials have offered rough estimates of visa revocations and denials, but have not yet publicly addressed potential chilling effects.)[224] Moreover, such dynamics can become self-reinforcing. Chinese graduate students and researchers diverted from the United States will go somewhere else instead, and eventually these alternate academic paths could become popular or even default options. The net result could be large, long-term reductions in American access to top academic talent.

Chinese government retaliation. Another feedback loop stems from Beijing's retaliation against U.S. technology controls aimed at China, which creates a risk of lengthy tit-for-tat reactions or escalatory spirals. So far, Beijing's responses have generally been reciprocal.[225] For example, it established an "unreliable entities list" following increased U.S. use of the Entity List, and Beijing imposed new technology export controls after related moves by

Washington.[226] But future responses could be more damaging. Many in Beijing believe that the United States is intent on destroying the Chinese technology ecosystem, and Chinese domestic narratives about tech competition have become increasingly nationalistic.[227] A particularly harsh U.S. restriction, or the overall accumulation of controls, may cause China to step up its responses or broaden them into new areas. Alternatively, Beijing might overreact due to misperceived U.S. intentions.

Retaliation by China could put pressure on Washington to respond in kind, risking a repetitive cycle that takes decoupling further or faster than the United States initially envisioned. For example, the U.S. order for ByteDance to divest from TikTok was followed, less than a year later, by China's pressure on ride-hailing company DiDi to de-list from the New York Stock Exchange.[228] Although Beijing probably had multiple motivations for reining in DiDi, it publicly cited data security concerns, mirroring Washington's main justification for the TikTok order. Beijing's abrupt exercise of power over DiDi aggravated U.S. leaders' worries that Chinese companies fail to disclose regulatory (and other) risks and are in Beijing's thrall. Several senators seized upon the episode to promote an accelerated timeline for de-listing all Chinese companies from American exchanges under the Holding Foreign Companies Accountable Act.[229] These moves and countermoves illustrate how easily escalatory spirals could be set in motion.

China has many cards to play if it chooses to step up its retaliation for U.S. tech restrictions. For example, it could dissuade or bar Chinese undergraduates from attending U.S. universities, depriving the United States of billions of dollars in tuition revenue at a time when many American institutions of higher learning are struggling financially.[230] It could impose controls on the rare earth metals required for many important technologies, which China nearly monopolizes.[231] It could further limit the activities of U.S. tech companies operating in China, bar or unwind U.S. investments and joint ventures, or ban the purchase of certain U.S. tech products. And if Beijing seeks to respond outside of the technology domain, the possibilities are open-ended.

These Chinese retaliation options illuminate vulnerabilities that U.S. leaders should try to address over time. For now, however, they are realities of interdependence. They highlight the damage America could suffer if decoupling gets out of hand and is no longer being controlled by Washington. Granted, China would also suffer in the process, so a measure of deterrence almost certainly exists. Nevertheless, history is replete with examples of destructive, seemingly irrational cycles of international escalation. A responsible U.S. strategy for technological decoupling must account for and mitigate this risk.

Domestic political dynamics. Finally, U.S. technology controls can shape domestic politics in ways that encourage ever-stronger restrictions in the future. Politically speaking, China-related controls—like other kinds of U.S. sanctions and restrictions targeting adversaries—are easy to impose and hard to reverse. Congress has also repeatedly stepped in

to turn discretionary executive measures into permanent statutory requirements. The result is a one-way ratchet, gradually limiting the policy space of each successive administration.

Biden, for example, has so far opted to retain many Trump policies that were highly controversial when first instituted—including the China tariffs and the unique foreign direct product rule applied to Huawei. Biden also allowed Trump's sweeping ICTS regulation to come into effect, surprising multiple business groups that had called the rule unworkable. Although Biden may actively support some of these measures, politics are probably a factor in others. The *Wall Street Journal* reported that "administration officials [were] concerned that blocking or diluting the [ICTS] rule would send the wrong message about the new administration's approach to China, potentially fueling criticism that it [was] taking a weaker approach."[232]

The economic impact of U.S. government technology restrictions can also ripple into the political arena. For example, a U.S. import ban on certain Chinese tech products could economically weaken the American resellers of those products. If those resellers ultimately exit the marketplace, that would mean fewer voices advocating for bilateral tech cooperation. Conversely, hawkish voices tend to thrive in a restrictive and securitized environment. Palantir, whose data products are used by the U.S. national security establishment, has emerged as a strong advocate of technological decoupling.[233] Washington's drive to counter China tech threats creates business and political opportunities for companies like Palantir, potentially fueling the rise of a well-connected decoupling lobby. There is already a long American tradition of defense and national security contractors exerting influence over public policy—for example, by supporting political candidates and thinkers who warn of foreign threats and advocate muscular U.S. responses. Technology controls aimed at China could unleash similar dynamics, as a subset of U.S. tech companies will benefit from such restrictions and work to entrench or expand them.

In sum, Washington might aim for a moderate level of technological decoupling but end up with something broader, faster, and messier. The risks are serious and demand a strategic response. The United States must preserve the ability to adjust the decoupling process upward or downward—keeping its pace and scope aligned with American needs. That means U.S. technology restrictions should be kept as targeted and precise as possible to minimize the risk of unwanted escalation. Moreover, Washington must communicate its intentions clearly and convincingly to multiple audiences. It should openly clarify its strategic objectives, and even some specific policy criteria, to reassure companies, universities, and foreign governments—including China—of its intentions. This degree of clarity cuts against the American grain: U.S. political and national security leaders like to preserve their own discretion, and they struggle to make credible commitments across presidential administrations. But in a complex and interdependent global technology landscape, too much silence or ambiguity may actually cede control to others.

TRANSLATING STRATEGY INTO POLICY AND PROCESS

The previous chapter argued for a centrist technological decoupling strategy in which U.S. government restrictions play a small but important role. Government tech restrictions by themselves cannot ensure U.S. technological preeminence over the long haul, but they can sometimes frustrate Chinese dominance in the short run. The United States should therefore focus its restrictions on a select set of technology areas where China verges on securing unique, strategically significant, and long-lasting advantages. This would buy time for longer-term investments in American technological leadership, competitiveness, and resilience to succeed—helping the United States address the full range of its tech challenges, including those that only partially relate to China. Carefully tailoring and communicating these restrictive policies would also help Washington preserve its influence over the pace and scope of technological decoupling, reducing the likelihood of a damaging runaway process. A balanced approach to the U.S.-China technology relationship would provide American leaders with maximum options during an era of strategic uncertainty and flux. It would also improve the odds of bilateral cooperation on urgent global challenges, like climate change, and preserve space to address pressing domestic crises.

Not everyone will agree with this strategy. Restrictionists may find it naïve, and cooperationists may consider it dangerous. So much the better; American policymakers need to hear robust debate, especially in this early phase of technological decoupling. Responsible voices from all three camps should continue weighing in on the most fundamental questions: In what ways does today's U.S.-China technology relationship help or hurt America—in the technology arena, and beyond? How will this cost-benefit calculus change over time, and

how should the United States balance its present and future needs amid inherent uncertainty? Meanwhile, how can Washington maintain control of the technological decoupling process and prevent triggering a more severe, violent break than it intends? Strategies should be judged by the clarity, factual grounding, and analytical rigor of their answers to these questions.

THE NEED FOR PRACTICAL GUIDANCE

Once a strategy is established, it must then be translated into policies and processes to guide U.S. government decisions. Without a practical set of standards, even the best strategy can result in inconsistent and ad hoc decisionmaking. In particular, the U.S. government must devise ways to determine which technology areas require China-related restrictions and which do not. While restrictionists, centrists, and cooperationists have varying appetites for technological decoupling and China-oriented controls, they must all face a version of this line-drawing problem when turning their high-level visions into tangible policy.

Meaningful guidance must move past generalities and express clear choices. That means describing what different federal agencies should do with specific authorities that they have. It is no simple task. Analytically, it requires evaluating a host of technology areas and weighing numerous costs and benefits through the lens of multiple expert disciplines. Politically, the charged tenor of China discourse in the United States makes American leaders and analysts reluctant to publicly cheerlead any form of bilateral technology cooperation, even where the benefits outweigh the costs. Thus, while many observers say that technological decoupling should be bounded and partial, there are few comprehensive, detailed proposals for how and where to draw such boundaries.

Any strategy for technological decoupling must face a line-drawing problem when turning its high-level vision into tangible policy.

The easy part is identifying the highest-risk, most strategically sensitive technology areas where U.S. government controls are clearly desirable. 5G telecommunications equipment and semiconductors are two well-known examples. The United States has already imposed substantial restrictions in both areas, and experts broadly support them even while debating key details. The hard part, often, is naming lower-risk areas—technologies where continued U.S.-China interdependence would be permissible and actually beneficial to American interests. But Washington needs real limits to bound the decoupling process and prevent a costly, self-destructive overreach. The more clearly such limits can be articulated in practical policymaking standards, the more effectively the U.S. government can make decisions and manage the expectations of other governments and private actors worldwide.

BREAKING DOWN THE POLICY PROBLEMS

This report takes a step-by-step approach to develop useful policy guidance. It begins by breaking down the many U.S. interests at stake into nine distinct policy objectives for technological decoupling. National security objectives include maintaining a military edge over China, limiting Chinese national security espionage, preventing Chinese sabotage in a crisis, limiting Chinese influence operations, and denying support for Chinese or China-enabled authoritarianism and repression. Economic objectives include countering unfair Chinese practices and intellectual property theft, and competing and leading in strategic industries. Then there are ancillary objectives—non-technology goals that also influence American decoupling policy: obtaining general leverage over China, and shaping U.S. domestic narratives. These nine objectives, although linked, raise many distinct issues and dilemmas. They cannot be treated as interchangeable responses to an undifferentiated mass of "China tech threats"—an all-too-typical approach. Of course, real-world decision-making often involves weighing multiple policy objectives simultaneously.

Technological decoupling can serve many distinct U.S. policy objectives. These cannot be treated as interchangeable responses to an undifferentiated mass of "China tech threats."

The next step, and the heart of this report, is a careful review of the role U.S. technology controls should play in achieving these policy objectives. Taking each objective in turn, the report weighs the risks and benefits of U.S.-China technological interdependence against the risks and benefits of U.S. government technology controls, in line with the overall (centrist) strategy described above.[234] This analysis leads to a series of proposed dividing lines—implementable standards for determining which technology areas warrant U.S. government restrictions and which do not. Specific examples help to illustrate how these dividing lines would work in practice. Finally, there are brief discussions of "offensive" (domestic self-improvement) measures critical for achieving each policy objective. While technology controls are the primary subject of this report, they must not become the primary focus of policymakers.

Because U.S. policymakers face complex dilemmas, these recommendations would require further vetting and debate by implementing agencies. They would also need refinement to a higher level of detail. While this report's proposals aim to be specific and actionable, agencies need to draw still finer distinctions in real-world policymaking. For this reason, many of the recommendations lay out analytic processes that agencies should follow—questions to ask, objectives to prioritize, and standards to apply—rather than firm outcomes. Case studies illustrate how these processes might play out in specific technology areas, though agencies would need to arrive at their own conclusions based on internal expertise (including classified information) and outside perspectives.

Reasoned deliberation does not always determine actual U.S. policy, of course. Political imperatives, unexpected crises, and bureaucratic quirks all play a role. But it is essential for Washington to develop strong decisionmaking processes to inform the use of China-oriented technology controls. Good processes push high-level U.S. officials to consider key issues earlier, more frequently, and in a more focused, structured way than would otherwise happen. They frame policy dilemmas for principals and help to clarify questions that require resolution by the president. Over time, high-quality government deliberations also teach the permanent national security apparatus—the many thousands of staffers and outside analysts who shape conventional thinking in Washington—to ask better questions about technological decoupling.

MAINTAINING A MILITARY EDGE OVER CHINA

RISKS OF INTERDEPENDENCE

America's most senior military officers and civilian defense leaders in both parties have grown increasingly alarmed by China's advancing military capabilities. Unclassified U.S. intelligence assessments describe the PLA as slowly but steadily transforming itself "from a defensive, inflexible ground-based force charged with domestic and peripheral security responsibilities to a joint, highly agile, expeditionary, and power-projecting arm of Chinese foreign policy that engages in military diplomacy and operations across the globe."[235] U.S. forces, by comparison, have deferred some of their own modernization programs and declined in readiness across many areas since 2001, partly due to a preoccupation with counterterrorism and counterinsurgency. Even after the Afghanistan withdrawal, America's enormous and highly capable military remains spread thin across a number of global missions—whereas the PLA has been optimizing for a few key objectives in its local theater. Together, these trends have led the Pentagon to warn of a diminished "competitive edge" over China.[236]

Technology plays a key part in China's military catch-up. Beijing has made major strides in modernizing its conventional hardware and nuclear weapons systems—aided, at times, by cyber and traditional espionage. Looking ahead, many U.S. analysts are especially worried about the PLA's incorporation of emerging digital technologies such as AI and quantum computing. China believes that AI, in particular, will eventually enable "intelligentized warfare"—a more rapid, precise, and dispersed form of combat intended to paralyze enemy forces and decisionmakers.[237]

Because AI and so many other militarily relevant technologies are dual-use, the PLA seeks technical support from Chinese companies and universities under the banner of "military-civil fusion." Seamless fusion remains more aspiration than reality; however, Beijing is working to break down bureaucratic barriers and enhance incentives for private support to the military.[238] It also has many legal and extra-legal tools to compel such cooperation for high-priority military programs. This makes the U.S. defense establishment leery of technological cooperation between American and Chinese businesses or universities. The Pentagon fears that Beijing will leverage such links to acquire military-relevant technology, whether through licit means (such as joint ventures) or illicit means (like hacking).[239]

RISKS AND LIMITATIONS OF DEFENSIVE MEASURES

The need to maintain a military edge over China offers powerful justification for U.S. technology controls. But what sort of controls can achieve American military needs at acceptable overall cost to the U.S. national interest? A narrowly tailored set of restrictions makes the most sense for several reasons. First, although AI and other emerging, dual-use technologies may someday become key factors in the U.S.-China military balance, that day is probably a long way off. The coming wave of military-technological advances will likely produce a marathon competition that lasts many years or even decades. This means the United States should prioritize the long-term sustainment of American innovative capacity rather than the short-term curtailment of Chinese military advances. Technology controls that durably set back PLA modernization would be worthwhile, but restrictions that degrade America's own technology base while only briefly disrupting Chinese progress would be counterproductive.

It will likely take many years or even decades before AI and other emerging, dual-use technologies become key factors in the U.S.-China military balance.

To gauge the near-term role of AI in U.S.-China military competition, consider a potential confrontation in the Taiwan Strait occurring in the next few years—the central worry of today's U.S. defense leaders. According to most analysts, the outcome of a Chinese incursion would likely hinge on such traditional factors as the PLA's competence in amphibious assaults, the readiness of Taiwan's defensive forces and the willpower of its civilian population and leaders, and the U.S. military's regional force posture and rules of engagement.[240] AI would certainly not be decisive. A recent analysis of Chinese military contracts found that, "like the United States, China's most promising AI applications so far seem to be for back-office tasks like intelligence analysis and predictive maintenance."[241]

At what point will military AI become important enough to swing a battle between U.S. and Chinese forces? The National Security Commission on Artificial Intelligence—

the leading mainstream assessment—placed this risk "in the coming decades."[242] And how likely is it that Chinese AI would one day be sufficient to offset U.S. military advantages in other areas? The commission was appropriately cautious, simply noting that Beijing "believes" this could happen. DOD's most recent public report on the Chinese military also hedged on whether, how, and when emerging technologies like AI or quantum computing might affect real-world combat. The report rightly gave more weight to less exotic developments, such as China's ballistic and cruise missile advancements, its anti-satellite capabilities, its increasingly realistic joint exercises, and other modernization efforts.[243] Of course, the era of AI warfare will come eventually and the U.S. military must work hard to prepare for it. But the longer this technology competition lasts, the less likely it is that U.S. restrictions will hold Chinese advances at bay.[244]

Second, the Pentagon's "competitive edge" concept is notably vague and open-ended, making it a poor guide for determining which technologies merit U.S. government restrictions.[245] Nearly all technology has some military application, and the U.S. military sees itself "competing" with China in innumerable ways and places—from combat contingencies in the Indo-Pacific to steady-state information operations and defense diplomacy in Africa and Latin America. Controlling all the technologies relevant to such competition would mean a total amputation of U.S.-China tech ties—choking the American economy that funds defense spending, and degrading the U.S. innovation base that supports military capability development.

DOD has never actually called for full-scope decoupling; in fact, the DOD-aligned JASON group of scientific advisers has argued that international technical cooperation is vital to American interests.[246] Yet U.S. military leaders have sometimes flirted with more restrictionist ideas—for example, generically opposing Americans' involvement in the Chinese AI sector.[247] Such ideas, if pursued to their logical conclusion, could lead to broad-based technological decoupling.

Finally, the U.S.-China rivalry is not just military in nature, and Washington will likely rely more on economic and diplomatic tools in the years to come. That is because the current U.S. military "competitive edge" over China, diminished as it is, probably cannot be sustained. China has natural geographic advantages in its home theater, whereas U.S. forces must operate costly and vulnerable expeditionary bases and logistics lines. China's defense budget will probably keep growing faster than American spending, which is projected to stay flat or rise slowly in real terms.[248] The technologically inferior PLA can close many existing gaps at a faster pace than the U.S. military can create new ones. And for many military scenarios, such as a Taiwan Strait confrontation, Beijing will be more invested in the outcome and more politically capable of absorbing losses than Washington.

Of course, the United States should take all reasonable measures to mitigate these military disadvantages. But a detailed study by the RAND Corporation found that "as long as

the Chinese economy continues to grow faster than that of the United States and Beijing continues to make military modernization a priority, the challenges facing U.S. military planners in Asia will grow more severe over time."[249] This means that other tools of U.S. national power will be crucial for managing China's rise—something Beijing itself appears to recognize.[250] Thus, Washington should avoid technology restrictions that yield immediate yet modest military gains but inflict larger, longer-term economic and diplomatic costs on the United States.

RECOMMENDED POLICIES AND PROCESSES

The Defense Department must focus and prioritize its concerns about Chinese tech. Specifically, DOD should identify future PLA technology milestones that would tangibly change military outcomes over a concrete time horizon. This rigor would help federal regulators design more targeted technological controls that achieve military needs while minimizing harm to other national interests.

A good starting point would be DOD's China-related defense planning scenarios—a classified set of priority missions that might include, for example, helping to defend and/or resupply Taiwan.[251] For each planning scenario, DOD could seek to identify what potential new PLA technological capabilities would most significantly increase the likelihood of U.S. mission failure. The time horizon being considered would shape the nature of DOD's analysis. DOD could make fairly concrete predictions about what technologies will matter most during the next five or ten years, because U.S. and Chinese operational concepts will not drastically change during that time and most key technologies either already exist or have been theorized. To assess military-critical technologies on a longer timeline, DOD would need to make more speculative predictions, such as how early-stage technologies may mature over decades, and what the American and Chinese militaries of the future will look and fight like. Proposed controls on early-stage technologies should therefore meet a higher threshold of criticality and undergo more rigorous vetting.

DOD should use its defense planning scenarios to identify future PLA technology milestones that would tangibly change military outcomes over a concrete time horizon.

Although DOD has formidable internal expertise in offices such as the Strategic Intelligence and Analysis Cell, its assessments should draw generously from the insights of independent technologists, military analysts, and China experts to avoid myopia and groupthink. Existing channels for engaging outside experts, like the JASON group, may need to be expanded or supplemented to account for the difficulty of making long-term technology predictions and the need to consider implications for a wide range of U.S. interests beyond

defense. The Intelligence Community should also provide an independent check on DOD's assessments. Once military-critical technologies have been identified, intelligence analysts should assess the likelihood of the PLA actually acquiring these technologies and effectively fielding them over different time horizons. Analysts would also evaluate China's relative dependence on foreign tech transfer, as opposed to its indigenous ability to develop the same technologies.

Regulators would then consider the efficacy of potential technology controls, and an interagency review led by the National Security Council (NSC) would evaluate second- and third-order impacts, such as economic and diplomatic implications. Interagency review has long been the norm for many kinds of technology controls. But given the growing importance of dual-use technology, private sector–led "spin-on" innovation, and globalized supply chains, the NSC should assess whether current deliberative processes are sufficiently comprehensive and inclusive.

CASE STUDIES

Drone swarms. Drone swarms are a potential example of militarily significant technology that might merit new U.S. technology restrictions. Many military analysts worry that large swarms of cheap, autonomous, self-coordinating drones could neutralize U.S. military advantages over China.[252] They fear that China could deploy these drone swarms to overwhelm and destroy large, expensive, relatively immobile American assets like aircraft carriers. If that fear is well-grounded, then China's development and successful fielding of this technology could swing the balance of a strategically consequential battle.

Still, U.S. technology controls would only make sense if they could be effective in protecting America's military edge. China's world-class commercial drone industry is mostly indigenous, reducing the U.S. government's influence over Chinese advancements. In late 2020, the Trump administration added DJI, the global market leader in drones, to the Entity List based on human rights violations. David Benowitz, an industry analyst and former DJI official, identified several U.S.-origin parts that DJI would need to replace following this designation. Still, he predicted the move would not "severely impact" the company.[253]

Swarming, an aspect of drone technology that remains in development, could have distinct chokepoints for U.S. controls to target. Key hardware components of drone swarms, like high-fidelity short-range communication equipment, might perhaps be controllable (assuming China does not already lead in these areas). Some software components, however—like computer vision algorithms—would be harder to control because they are intangible, under development by many international companies, and often based on openly published academic research.

Xiaomi. The final days of Trump's presidency offered a vivid example of poorly designed technology controls, when DOD designated the consumer electronics giant Xiaomi as a "Communist Chinese Military Company." This status, a forerunner of Biden's Non-SDN Chinese Military-Industrial Complex Companies List, would have prohibited Americans from investing in the company. DOD's justification was shockingly thin. It highlighted Xiaomi's plans to invest in 5G and AI—two broad, loosely defined technology areas that most global companies are pursuing—and the fact that Xiaomi was once publicly recognized by a Chinese ministry. Xiaomi later won a court injunction after a federal judge found the company did not meet the legal criteria for designation and DOD "could not identify *any* transfers of technology from Xiaomi to the PRC."[254] Biden has since reversed this designation and overhauled the underlying regulatory process, placing the Treasury Department in charge.[255]

Broad technology categories like "AI," "Big Data," or "the Internet of Things" are not appropriate targets for military-related technology restrictions. They are too ubiquitous to control, and too generic to meaningfully assess for military impact. Unfortunately, the U.S. government does not always recognize this. The Commerce Department's new ICTS supply chain rule requires special scrutiny for any China-related technology "integral to: (A) Artificial intelligence and machine learning; (B) Quantum key distribution; (C) Quantum computing; (D) Drones; (E) Autonomous systems; or (F) Advanced Robotics."[256] These are diverse and capacious categories. They can be a starting point for further analysis, but U.S. government decisionmaking must be far more granular.

Broad technology categories like "AI," "Big Data," or "the Internet of Things" are too ubiquitous to control and too generic to meaningfully assess for military impact.

Supercomputers. Supercomputers provide another case study that illustrates the complexity of U.S. efforts to control military-relevant technology. The U.S. government has long sought to prevent the Chinese military from acquiring powerful supercomputers due to their important role in advanced cryptography and in the design and development of nuclear weapons, missiles, and other military systems.[257] For decades, Washington relied on export controls of finished supercomputers, permitting their sale to China only if they would not be used for military purposes.[258] But U.S. restrictions have recently broadened. The United States now uses its Entity List to target entire Chinese organizations involved in supercomputing—restricting them from obtaining a wide range of U.S. components and other goods, not just supercomputers themselves.[259]

Although these initial designations focused on organizations owned or controlled by the PLA, they have sprawled since 2015.[260] Today the Entity List covers nearly all major players in the Chinese supercomputing ecosystem, including high-performance chip designers, supercomputer manufacturers, and supercomputer operators.[261] According to the Commerce

Department, these organizations have varying ties to the PLA. Secretary of Commerce Gina Raimondo explained that "supercomputing capabilities are vital for the development of many—perhaps almost all—modern weapons and national security systems, such as nuclear weapons and hypersonic weapons."[262] But that is hardly all, or even most, of what some of these entities do. Like supercomputing organizations around the world, they also support biomedical research, weather forecasting, electric grid management, oil and gas exploration, and countless other benign activities.[263]

On one level, this increasing use of the Entity List makes sense. China has transitioned from purchasing foreign supercomputers to building its own, so U.S. technology controls will be more effective if they target the latter process instead of the former.[264] Yet the change in U.S. regulatory tools has also implied a subtle but important de facto shift in U.S. policy toward China's technological development. Before, Washington specifically opposed Beijing's military use of supercomputers. Now, it effectively opposes Chinese supercomputing as a whole—a general-purpose technology with innumerable civilian uses. The U.S. government has yet to publicly comment on this shift, which could have second- and third-order implications. It might stymie scientific cooperation on climate modeling, for example, or help motivate Beijing to restrict American access to some general purpose technology that China dominates. The Biden administration should carefully review its semiconductor restrictions to ensure that it has fully considered their implications beyond the military sphere.

KEY OFFENSIVE POLICIES

While senior defense leaders should continue to inform civilian regulators of the critical technologies they believe warrant government controls, other ways of maintaining the American military edge over China deserve more time and attention. First, DOD should accelerate its efforts to modernize and transform U.S. forces to counter the PLA. This work—which includes developing more survivable and cost-effective systems, becoming more adept at incorporating private sector innovations, designing new warfighting concepts for near-peer battle, and moving forces into and within the Indo-Pacific—has been underway since late in the Obama administration. However, it remains far from complete and faces enormous bureaucratic and congressional obstacles.[265] The U.S. military edge over China will depend more on this task than on any other governmental effort, including technology restrictions.

The U.S. military edge over the PLA will depend more on the modernization and transformation of American forces than on technology restrictions targeting China.

Second, the Department of Defense and the Department of Homeland Security (DHS) should redouble their efforts to shore up cybersecurity and information security in the military and among defense

contractors specifically. The immediate priority would be to counter the most proven and most damaging Chinese intelligence collection techniques—namely, remote hacking, human agent recruitment, and open-source research. Although the Pentagon in recent years has significantly tightened the cybersecurity requirements in its procurement rules, the defense industrial base remains vulnerable.[266]

LIMITING CHINESE NATIONAL SECURITY ESPIONAGE

RISKS OF INTERDEPENDENCE

The Federal Bureau of Investigation currently describes China's intelligence activities as "the greatest long-term threat to our nation's information."[267] The bureau has thousands of active counterintelligence cases relating to China and opens multiple new cases daily.[268] Although Beijing's theft of intellectual property and other economically valuable data remains the primary concern, Chinese national security espionage is also harmful. China's intelligence agencies have stolen a significant volume of U.S. military secrets in recent years, including aircraft designs.[269] They have penetrated U.S. political campaigns to gain insight into future American policymaking.[270] And they have compromised America's own espionage networks, reportedly helping to expose and disrupt U.S. intelligence activities in China—a top American collection priority—and elsewhere.[271]

Classified U.S. national security secrets are shielded by a robust system of technological, physical, and personnel controls. As a result, China often first seeks out sensitive unclassified data that it can later exploit to acquire classified information. In particular, U.S. officials assess that China assembles and analyzes large quantities of Americans' personal information to identify potential targets for intelligence collection or other subterfuge. Some U.S. intelligence officials believe such techniques have enabled Beijing to quickly identify undercover personnel from the Central Intelligence Agency around the world and monitor or disrupt their activities.[272] U.S. agencies also cite the risk that China could use sensitive medical, financial, or other personal information to blackmail or co-opt American officials.[273]

China's intelligence targeting of American officials has become a major justification for U.S. tech restrictions. After all, U.S.-China technological ties provide the Chinese government with additional opportunities to harvest Americans' personal data (just as these ties may give Washington ways to collect on Chinese targets). Beijing could, for example, pressure a Chinese tech company to share its private data on American users. Chinese companies are legally required to comply with such requests, and according to U.S. intelligence officials, these companies already help to process bulk data in the possession of Chinese intelligence agencies.[274] For example, U.S. officials have publicly alleged that Huawei "has the capability secretly to access sensitive and personal information in systems it maintains and sells," and that "information from Huawei routers has ultimately ended up in hands that would appear to be the state."[275]

RISKS AND LIMITATIONS OF DEFENSIVE MEASURES

These risks provide some basis for limiting Chinese companies' presence in U.S. information systems. However, restrictive measures may always not be very effective in thwarting Chinese theft of Americans' personal data, for the simple reason that Beijing seems to prefer other ways of acquiring that data. When American officials describe China's most successful and damaging bulk collection efforts to date, they usually point to the devastating hack of the U.S. Office of Personnel Management and the compromises of Marriott, Equifax, and Anthem. But these were all remote cyber operations; none apparently required any Chinese insider access to U.S. systems, companies, or supply chains.[276]

In fact, sensitive personal information about Americans can be bought outright from U.S. or foreign data brokers. U.S. journalists have vividly demonstrated how easy it is to obtain geolocation and other data to identify and track prominent Americans.[277] The U.S. military and Intelligence Community reportedly use similar techniques to track foreign targets, so there is every reason to believe that Beijing does the same.[278] Then there is simple data scraping from the open internet, which is apparently one of Beijing's most effective espionage techniques. According to U.S. prosecutors, China has successfully recruited multiple Americans to spy for Beijing based on information in these targets' public LinkedIn profiles. William Evanina, then director of the National Counterintelligence and Security Center, said in 2019 that LinkedIn was China's "ultimate playground for collection."[279] (Although LinkedIn announced last year that it would leave the Chinese market, that won't stop Beijing from scouring Americans' own LinkedIn pages.[280]) The major digital espionage

China's most successful known bulk collection efforts were all remote cyber operations. They required no insider access to U.S. systems, companies, or supply chains.

risks, then, stem from pervasive gaps in U.S. cybersecurity and data privacy law, policy, and implementation. Chinese tech companies' presence in American markets and supply chains seems like a secondary threat at most.

Before instituting sweeping measures to deny China any access to Americans' personal data on national security grounds, it is also worth considering targeted actions to protect the relatively few U.S. citizens with access to classified information. The government has significant influence over its own employees and contractors, enabling Washington to discourage or even bar them from using Chinese technologies deemed to be high-risk. For example, the U.S. military already bans TikTok from government-owned devices. The military has even "urged troops and their dependents to erase the app from personal phones"; if necessary, this could become a condition for maintaining a security clearance.[281] Protecting undercover agents is a more complicated task. But U.S. spy agencies have already implemented new tradecraft and operational security innovations to offset China's digital counterintelligence techniques—the kind of cat-and-mouse game that has occurred throughout the history of espionage.[282]

RECOMMENDED POLICIES AND PROCESSES

"Personal data" is not a useful or controllable category. Instead, the U.S. Intelligence Community should work to identify those categories of personal data that would provide the greatest marginal benefits to Chinese spy agencies. Regulatory agencies would then consider technology restrictions aimed specifically at this data, while accepting higher levels of risk for other types of data.

Regulators should protect the personal data with greatest marginal benefits to Chinese spy agencies, while accepting higher levels of risk for other types of data.

The Intelligence Community analysis would need to consider China's preexisting intelligence capabilities and its access to functionally equivalent personal data on Americans. It would also examine the U.S. government's ability to detect and mitigate different kinds of personal data theft. If Washington can learn of certain Chinese data theft quickly and implement effective response plans (for example, by readjusting official travel patterns or refreshing the cover identities used by intelligence officers), that category of data may need less protection. Finally, the IC should consider the overall significance of the U.S. personnel described by the data, and the likely harm to U.S. national security from China's improved ability to track, recruit, or disrupt these people. While all Americans' personal data deserves fundamental protections, extra-stringent restrictions should have special justification—just as the IC generates costly cover identities for some intelligence officers and not others. For example, data on enlisted U.S. military members in

non-sensitive positions would certainly have some intelligence value to China, but it may not be critical enough to justify broad-based restrictions on China's involvement in the U.S. tech sector.[283]

Because U.S. government data is already controlled to varying degrees, the Intelligence Community would primarily look to identify sensitive but unclassified personal data held by companies and other private parties. For a useful benchmark of the sensitivity of privately held data, the IC could ask whether the data would be considered classified if owned by the U.S. government. For example, U.S. national security agencies maintain large caches of employee data in unclassified, internet-connected systems (like the Defense Travel System) that are inherently more vulnerable to Chinese hacking than classified systems.[284] The existence of such systems suggests that Washington believes the practical benefits of internet connectivity can often outweigh the risks of Chinese espionage. This is a reasonable calculation. Regulators should not require private companies to take more onerous precautions than U.S. agencies themselves take for equivalent categories of government-held data.

CASE STUDIES

Genetic data. Genetic information is an example of personal data that could warrant restrictive measures to prevent Chinese government access. In 2020, the Treasury Department issued new regulations empowering CFIUS to review covered transactions that involve "sensitive personal data" of more than 1 million individuals.[285] The definition of sensitive personal data includes genetic data. Compared to other types of personal information, genetic data is less widely distributed and harder for Beijing to obtain. China could conceivably use genetic information to identify and physically track U.S. government officials—including undercover officers—as they move around the world.[286] Because someone's genetic information cannot be changed, a breach would have lifelong consequences and be difficult to remediate.[287]

Geolocation data. In other cases, the "sensitive personal data" regulation seems overly broad. Geolocation data is also considered sensitive under the Treasury rule. Yet because Americans' geolocation data can be easily purchased from online data brokers, CFIUS screening probably cannot prevent China from acquiring such data. Meanwhile, the possibility of CFIUS review could cause substantial economic harm to U.S. businesses. There are entire industries, including the mobile app ecosystem, where relatively small American companies might have geolocation data on 1 million or more individuals. The potential need to file voluntary CFIUS notices, and the opaque and time-consuming nature of CFIUS review, could chill a great deal of investment activity while doing little to protect Americans from Chinese espionage.

The Grindr episode illustrates both the possibilities and limitations of U.S. efforts to stop Chinese companies from acquiring different kinds of personal data on Americans. In 2019, CFIUS forced a Chinese company to unwind its purchase of the dating app Grindr.[288] Grindr has a large American user base, likely including many U.S. officials, who privately share information about their HIV status and sexual activities with the app. Such information has great value for Chinese intelligence targeters, will remain relevant to them for decades, and cannot be found in many other places online. The CFIUS action therefore made sense, because it blocked one of China's clearest paths to acquiring a unique cache of personal data with clear national security value. On the other hand, the forced divestment probably did little to secure other types of personal data, such as geolocation. A 2021 Norwegian government report revealed that Grindr's new American owners routinely share users' "IP address, GPS location, age, and gender," though not sexual or health information, "with a very large number of third parties."[289] It would be a trivial task for the Chinese government to get similar information from data brokers.

Stayntouch. Trump's 2020 executive order on Stayntouch provides another cautionary case study. Circumventing the normal CFIUS process, Trump required a Chinese company to divest from Stayntouch, a cloud-based service that helps hotels manage their properties.[290] Stayntouch has access to data on hotel guests, and its software can even be used to access guest rooms. This likely raised the specter of China using Stayntouch software to gain historical or real-time knowledge of U.S. government officials' travels, a clear counterintelligence threat. That said, Stayntouch is used by only 500 hotels worldwide; American officials might be able simply to avoid these hotels.[291] By comparison, Marriott alone has 7,642 properties.[292] Without aid of any insider access, Chinese hackers had persistent access to Marriott's Starwood network for *four years* and stole data on *500 million guests*, including reservation and travel information as well as personal data such as passport numbers.[293]

The contrast between Stayntouch and Marriott shows the limits of CFIUS as a tool for protecting Americans' personal data. While a small number of high-value data sources can be protected through China-focused restrictions like investment screening, most other kinds of personal data cannot feasibly be secured this way. Unfortunately, U.S. officials have not always made such distinctions. The Trump administration, in particular, often lumped all types of personal data together regardless of sensitivity, uniqueness, or controllability. Then secretary of state Mike Pompeo in 2020 described a "project of real scale" in which "we are now evaluating *each instance* where we believe that U.S. citizens' data . . . crosses Chinese technology."[294]

App bans. In Trump's last days as president, he signed an executive order banning Alipay, WeChat Pay, and six other Chinese apps. Rather than point to specific kinds of data these apps collected from Americans, Trump described a generalized threat of "Chinese connected software applications" that can "[access] personal electronic devices such as smartphones, tablets, and computers"—in other words, nearly all Chinese software. And he cited, as a

favorable precedent, India's recent ban of "more than 200 Chinese connected software applications throughout the country"— a blunderbuss barrage from New Delhi that seemed motivated more by a desire to retaliate for recent border skirmishes than by any careful, app-specific security review.[295]

Pompeo and Trump are no longer in office, and Biden has rescinded the app bans. But the fact that such bans were even attempted, and the limitless logic used to justify them, has already sent a chilling message to the global software industry. Meanwhile, loose talk about "Americans' data" can still be heard across the political spectrum. Evanina, a former career professional, testified last year that approximately "80 percent of American adults have had *all of their personal data* stolen by the [Chinese Communist Party], and the other 20 percent most of their personal data"—a head-scratchingly vague and implausible claim that has nevertheless become widely quoted.[296]

Video games. Under Biden, CFIUS has reportedly continued its investigation of Tencent's ownership stakes in Riot Games and Epic, two video game developers.[297] A former civil servant in charge of CFIUS reviews under Obama and Trump explained these investigations to *Bloomberg*: "When you're talking about massive amounts of data, there's probably something for the committee to look at." He went on to add that: "The question then becomes[:] is the risk high enough that it actually warrants forcing deals apart."[298] In other words, a large universe of activities must be reviewed, with fine policy distinctions being made after the fact, behind the scenes, on a case-by-case basis. This strategy, typical of the American national security establishment, risks casting a chill over huge swaths of commercial transactions. A more targeted and rigorous approach is needed.

In June 2021, Biden signed an executive order on "Protecting Americans' Sensitive Data from Foreign Adversaries."[299] This order singles out the threat from China and tasks agencies with making "recommendations to protect against harm from the unrestricted sale of, transfer of, or access to United States persons' sensitive data, including personally identifiable information, personal health information, and genetic information, and harm from access to large data repositories by persons owned or controlled by, or subject to the jurisdiction or direction of, a foreign adversary." A formal process for grappling with these problems is a welcome improvement on the previous, ad hoc approach. But the ultimate value of this process will depend on whether key terms from Biden's order can be given more specific, tightly focused definitions. "Sensitive data," "personally identifiable information," and "large data repositories" are vague concepts that could easily lead to overreaching governmental controls. These concepts should be refined to include only the highest-priority data, as outlined above.

KEY OFFENSIVE POLICIES

The U.S. government has many opportunities to protect Americans' personal data from Chinese intelligence, beyond imposing restrictive measures aimed specifically at China. Above all, Congress should establish national data privacy and cybersecurity standards. Many experts have called for federal legislation to replace the weak smattering of sector-specific and state-level rules.[300] With new mega-breaches and data abuses routinely coming to light, it is clear that many U.S. companies lack adequate incentives to protect Americans' private information. National cybersecurity and data privacy standards would be adversary-agnostic, aiming to stop any malicious actor from wrongfully purchasing or stealing sensitive personal data. By addressing the underlying problem—that Americans' personal data is very easy to obtain—such standards would do more to thwart Beijing's intelligence collection than most China-centric measures.

National cybersecurity and data privacy standards, although adversary-agnostic, would do more to thwart Beijing's intelligence collection than most China-centric measures.

The U.S. government can also take specific precautions to protect its own officials. While all Americans have an interest in preventing Beijing from accessing their personal data, the most acute national security threat is Chinese intelligence targeting those with classified information—a much narrower category. In response to this growing threat, U.S. agencies have significantly increased their China-related counterintelligence activities. Still, the scope of the problem described by U.S. officials calls for even more resources. The government should step up its monitoring and disruption of Chinese intelligence operations, provide more frequent and detailed defensive counterintelligence briefings, and hand down new guidance or restrictions for officials' use of higher-risk online spaces like LinkedIn, among other possibilities. Targeted counterintelligence programs, while often not sufficient on their own, can help advance U.S. policy objectives without many of the costs and risks that come with broad-based technology restrictions.

PREVENTING CHINESE SABOTAGE IN A CRISIS

RISKS OF INTERDEPENDENCE

The Biden and Trump administrations both have warned that China could sabotage critical U.S. systems during a bilateral crisis and that technological interdependence heightens this risk.[301] Beijing has the legal and political tools to compel private Chinese companies to offer up any privileged access they may have to software or hardware systems used in the United States. Such access could facilitate actual attacks, as well as threats (either explicit or implicit), against U.S. infrastructure. During peacetime, China's interest in stable commercial and diplomatic relations generally outweighs any benefits of digital sabotage or saber-rattling. But in extreme circumstances, like the cusp of war, China would have strong reason to consider all its options. There are two broad scenarios.

In extreme circumstances, Beijing would consider digital sabotage to paralyze the U.S. military or dissuade American leaders from confronting China forcefully.

First, China could attempt a counterforce operation to paralyze the U.S. military and prevent American units from responding to a bilateral crisis. For example, Beijing might want to stop key U.S. military assets from promptly reinforcing or resupplying American or allied forces abroad. The scenario has parallels with Japan's 1941 surprise attack on Pearl Harbor, which sought to buy time for Tokyo to act freely in the Pacific.[302] In a modern digital version of such an attack, China could try to subvert unclassified and/or commercially operated infrastructure that the U.S. military relies

on—such as core telecommunications systems, private logistics companies, off-base electric power sources, undersea cables, commercial satellites, and cloud services.

Second, Beijing could carry out a countervalue operation that harms U.S. civilians, hoping to demoralize them and thereby dissuade American political leaders from confronting China forcefully. This might involve disruptions of the U.S. power grid, financial sector, healthcare systems, emergency services, telecommunications, or transportation networks. Britain briefly tried (and soon abandoned) a countervalue strategy at the outset of World War I, seeking to exploit its centrality in international communications and financial networks to isolate the German economy and force Berlin to quickly sue for peace.[303] A Chinese version of this gambit could cause significant blowback—harming the Chinese economy and turning Chinese tech companies into international pariahs, among other consequences. But in a major crisis, Beijing might discount or accept this risk, seeing digital subversion as less dangerous and provocative than more overt forms of disruption.

The danger posed by these scenarios is difficult to assess. On the one hand, they are premised on a hypothetical, high-stakes crisis that may never come to pass. China's calculus for when and how to exploit its companies' access to adversary systems is unknown; Beijing's concern for Chinese firms' commercial reputations may create a state of deterrence. And the ultimate impact of any Chinese sabotage is uncertain, in part because U.S. critical infrastructure systems are so complicated and decentralized. On the other hand, the long-term risk of such a crisis seems to be trending upward as bilateral relations deteriorate. And all governments, including the United States, are willing to exploit domestic companies for national security purposes under various circumstances. Finally, a crisis is no time to test the consequences of critical U.S. system outages.

RISKS AND LIMITATIONS OF DEFENSIVE MEASURES

U.S. restrictive measures can help to reduce the risks of actual or threatened Chinese technological sabotage. But such measures also have practical limits. Understanding these limits can help to focus U.S. action on the most important areas while preventing futile and costly overreach elsewhere.

To begin with, Beijing's counterforce and countervalue options in a crisis do not all require insider access to U.S. systems. According to the U.S. Intelligence Community, "China can launch cyber attacks that, at a minimum, can cause localized, temporary disruptions to critical infrastructure within the United States."[304] Such cyber attacks most frequently involve remote hacking; built-in backdoors are rare. In extremis, China could also do things like physically cutting undersea cables (including those that are not operated by or connected to China), disrupting U.S. satellites (through physical or cyber means that do not require

supply chain access), or ordering intelligence agents or co-optees inside the United States to carry out physical sabotage of critical infrastructure (whether Chinese-made or otherwise). Some of these actions are potentially deniable. In other words, U.S. tech restrictions can curb a few of China's sabotage options, but it isn't clear that PLA military planners need or prefer those particular options.

Technology controls also cannot eliminate China's low-tech or no-tech sources of leverage over the United States. During peacetime, Beijing's demonstrated coercive tool kit includes halting key exports, imports, and people-to-people exchanges in an effort to inflict economic damage.[305] Such actions do not necessarily target technology industries or rely on technological links. Instead, China has previously targeted sectors (including agriculture, tourism, and education) where it can impose asymmetric economic costs and maximize political pressure on a rival country's government. Again, more extreme options also exist. At the threshold of war, Beijing could choose to seize U.S.-owned assets in China or carry out mass arrests of American citizens. Such leverage points are inherent to a U.S.-China relationship; they cannot be eliminated so long as the two countries do business.

The fact is that any bilateral relationship provides both countries with some access to and influence over the other. Unless the United States seeks a Cold War–style separation from China, Beijing will retain significant avenues for coercion and disruption. Of course, Washington wants to design a relationship that maximizes U.S. leverage over China while minimizing Chinese leverage over America. This is a fine aspiration in theory, but often unattainable in practice, especially in the long run. One-sided dynamics will become harder to sustain over time as China continues to grow in economic heft and international influence relative to the United States.[306]

Any bilateral relationship provides both countries with some influence over the other. Barring a Cold War–style separation, Beijing will retain significant avenues for coercion and disruption.

Finally, potential Chinese sabotage should be placed in the context of other threats to U.S. infrastructure.[307] While American policymakers worry about what Beijing might do in future crises, a diverse array of non-Chinese actors have already caused actual disruptions to U.S. infrastructure during peacetime, or demonstrated the capability to do so. In 2021, a criminal ransomware attack led to the lengthy shutdown of America's largest petroleum pipeline, helping trigger fuel shortages throughout the East Coast.[308] The year prior, a domestic suicide bombing near an AT&T facility in Nashville caused prolonged telecommunications outages across multiple states.[309] Russia has twice caused power outages in Ukraine, and in 2014 it emerged that unknown cyber actors had severely damaged a German steel mill.[310]

The biggest threat to critical infrastructure, arguably, comes from non-intentional disruptions. Episodes like the Texas freeze (2021), Hurricane Maria (2017), and the Northeast blackout (2003) illustrate a basic problem: First, inadequate investments in infrastructure capacity, maintenance, and resilience create systemic fragility. Then, semi-random shocks—such as weather events, demand surges, equipment malfunctions, or counterfeit parts—destabilize the system and lead to large-scale outages.[311] Non-intentional infrastructure failures have been far more frequent and damaging than intentional wrongdoing by any actor. Non-intentional disruptions might even happen to coincide with an international crisis and thereby hamper U.S. military forces, although such a convergence is unlikely.

Unfortunately, China-focused restrictions can sometimes divert resources from broader efforts to shore up U.S. critical infrastructure against all hazards. Consider a hypothetical federal mandate to remove all Chinese equipment from the electrical grid. To pay for this expensive initiative, utilities would need to defer other planned investments in security and resilience, raise rates on consumers and businesses, or secure large government subsidies. Congress recently bumbled through a very similar situation. In March 2020, it passed a law requiring U.S. telecoms to "remove and replace" Huawei and ZTE equipment due to national security concerns.[312] Small rural carriers warned that this unfunded mandate would "devastate" them financially. Congress eventually provided subsidies to offset carriers' costs, but it took nine months and a fortuitous legislative vehicle—the $900 billion COVID-19 relief package—to do so.[313] Meanwhile the industry was forced to endure what one top lobbyist described as a lengthy "cliffhanger," during which two small carriers shut down.[314]

To be sure, U.S. policymakers cannot ignore the risk of China sabotaging American systems in a crisis. The risk is real, and technological interdependence provides Beijing with additional means (though perhaps lower motivation) to subvert U.S. infrastructure. Washington should take targeted, cost-effective actions to address the problem. But restrictive measures should focus on the highest-risk areas, where Chinese technological influence within the United States could grant Beijing a particularly effective capability to paralyze key U.S. forces or coerce U.S. political leadership at a critical moment. Even then, technology controls should be aligned with a comprehensive national plan to protect U.S. critical infrastructure from all digital and physical hazards.

RECOMMENDED POLICIES AND PROCESSES

The U.S. government should identify the most consequential Chinese sabotage scenarios, map the specific technological dependencies that would enable them, and design targeted controls to curb such risks.

The Department of Defense should take the lead on counterforce analysis. Approved defense planning scenarios can serve as the starting point. For each planning scenario, DOD

could list the individual U.S. military assets or networks essential to achieving mission objectives, perhaps based on Time-Phased Force Deployment Data.[315] It could then determine where these military assets have critical dependencies on unclassified and/or commercial U.S. networks. Finally, DOD could evaluate such networks for the presence of Chinese-origin software or hardware that Beijing could exploit to alter military outcomes. The acid test would be whether Chinese technological sabotage could significantly increase the likelihood of U.S. mission failure.

While DOD is leading the counterforce analysis, DHS should assess countervalue sabotage. To build a set of scenarios, DHS might start with existing frameworks such as the National Critical Functions—a list of fifty-five government and private sector activities "so vital to the United States that their disruption, corruption, or dysfunction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof."[316] These functions include such elemental tasks as "Manage Hazardous Materials," "Generate Electricity," and "Provide Positioning, Navigation, and Timing Services." DHS could survey major stakeholders for each function to identify Chinese commercial presence in the supply chain that could be exploited for disruptive purposes. This could leverage and complement the department's ongoing Systemic Cyber Risk Reduction Venture, which has a similar purpose but is not China-specific.[317]

DHS should set a high threshold of criticality before it recommends that regulators impose new China-related technology controls. It might, for example, consider only those sabotage scenarios that could plausibly exert a coercive effect on U.S. political leadership during a crisis. This would likely involve mass casualties and/or mass evacuations. As a point of comparison, the Federal Emergency Management Agency's National Threat and Hazard Identification and Risk Assessment provides a list of seven scenarios with that level of severity, including earthquakes, hurricanes, space weather events, and concurrent natural disasters.[318] To justify new government technology controls, a Chinese countervalue sabotage scenario might need to threaten damage on the same order of magnitude.

Any Chinese sabotage scenario should be vetted for plausibility. The Intelligence Community could provide an independent assessment that considers China's technology subversion capabilities, military doctrines, and national leadership intentions during the expected lifecycle of the U.S. systems at issue. In assessing China's plans and intentions, intelligence analysts should consider what other counterforce or countervalue options Beijing may have in a crisis, and whether Chinese leaders may be deterred by the risks of economic blowback or U.S. reprisals.

CASE STUDIES

Bulk power. The Trump administration's regulation of bulk power systems was a good example of tailored tech restrictions designed to thwart Chinese sabotage. In May 2020,

Trump signed an executive order restricting usage of bulk power equipment sourced from "foreign adversary" countries such as China.[319] Bulk power systems are ideal targets for sabotage because their failure can cause massive electricity outages that cannot easily be remediated. Large power transformers, for example, can take more than twenty months to replace.[320] These transformers are increasingly—though not exclusively—sourced from China and contain smart components potentially susceptible to manipulation.[321]

Trump's action focused specifically on counterforce scenarios. The administration assessed that the PLA "is equipped and actively planning to undermine" the bulk power system and that "such attacks are most likely during crises abroad where Chinese military planning envisions early cyber attacks against the electric power grids . . . in the U.S. to prevent the deployment of military forces and to incur domestic turmoil." Accordingly, the Department of Energy applied the ban on Chinese bulk power equipment only to "Defense Critical Electric Infrastructure"—that is, civilian-owned or -operated power infrastructure serving certain military facilities designated by DOD as "critical to the defense of the United States."[322]

The Department of Energy was right to bar China from supplying highly critical, difficult-to-replace bulk power equipment that directly supports military operations.

The Department of Energy was right to impose this restriction on a select subset of highly critical, difficult-to-replace equipment that directly supports military operations. However, Biden has rescinded the new rule and asked the Energy Department to consider what, if anything, should replace it.[323] The department invited public comment on potential approaches, including whether it should issue a new, even broader ban to cover countervalue scenarios and other types of power infrastructure. Any such expansion should remain focused on a very high threshold of sabotage impact and be rooted in rigorous cost-benefit analysis.

ICTS supply chain security rule. Not every U.S. action aimed at preventing Chinese technological sabotage has been so targeted. A particularly troubling case is the Commerce Department's new rule on ICTS supply chain security, which was first developed by the Trump administration, then allowed by Biden to come into effect in March 2021. Like the bulk power regulation, this rule warns that China and other foreign adversaries could sabotage the U.S. supply chain—"fully or partially shutting down critical networks or functions at key times," among many other cited dangers.[324] But the ICTS supply chain rule is far more sweeping in its scope and implications.

The ICTS rule allows the Commerce Department to review and ban virtually any China-sourced technology that is widely used in the United States. The potential scope of review includes—but is not limited to—all software (including mobile apps and web apps), internet hosting services, home networking devices, and Internet of Things devices used by or process-

ing data on more than 1 million Americans.[325] Considering the U.S. population and the scale of many digital markets, this is a low threshold. A transaction need not have any connection to critical infrastructure sectors or critical national functions to trigger review. The law firm Morrison & Foerster observed that "almost any ICTS-related activity in the United States connected to China is now subject to regulatory review by the U.S. government."[326]

Covered transactions are not automatically banned. Instead, the rule establishes a review system analogous to CFIUS. The Department of Commerce, in consultation with other agencies, will judge each transaction using a wide range of factors, including the likelihood and severity of potential harms and the efficacy of mitigation options, to determine whether "undue or unacceptable risks" exist. The publicly stated decisionmaking criteria are quite vague. Biden and the Commerce Department have taken laudable initial steps to clarify and refine these criteria, but it remains to be seen what implementation will actually look like. If Commerce follows the standard model of U.S. national security regulation (exemplified by CFIUS), it will either develop a more detailed list of internal criteria, or else make decisions on an ad hoc basis.[327] Both options would leave outside stakeholders—such as U.S. businesses—in the dark.

U.S. national security officials and political leaders traditionally prefer opaque regulatory processes for several reasons. By declining to commit publicly (or sometimes even privately) to a detailed and predictable decision framework, they seek to maximize the U.S. government's enforcement discretion. The all-encompassing ICTS supply chain rule means that Washington can adjust its interpretation from day to day based on its evolving needs and beliefs. Trump's Commerce Department also explained that clearer public criteria "would [have] allow[ed] foreign adversaries to pinpoint certain types of ICTS Transactions that would more easily escape Departmental oversight and, therefore, threaten U.S. national security."

Biden should substantially narrow the ICTS rule, instituting a clear and high threshold for technology bans and declaring specific safe harbors for noncritical tech areas.

But too much discretion comes with costs of its own, especially when a large portion of the U.S. digital economy and global technology supply chain is at stake. Without more clarity and predictability, some U.S. businesses will simply choose to avoid China-related technology transactions, including many that pose little national security risk and are economically beneficial. Likewise, global investors will pull back support from some projects—many of them benign—whose viability depends on a long-term U.S.-China technology supply chain.[328] The Biden administration should substantially narrow the ICTS supply chain rule, instituting a clear and high threshold for technology bans and declaring specific safe harbors for noncritical technology areas. It should also continue working to develop and publicize a more detailed and explicit set of enforcement criteria, along the lines suggested throughout this report.

In its current form, the ICTS supply chain rule is an invitation for overuse—if not by this administration, then by a future one. For example, restrictionist politicians and national security analysts have long campaigned for broad-based bans on computers, printers, and other devices sold by the Chinese companies Lenovo and Lexmark. The proposed bans would apply even in lower-risk settings, like noncritical state and local government offices.[329] Banning these cheap IT commodities would make it harder for cash-strapped public entities to address more pressing cybersecurity concerns, such as ransomware. Yet the ICTS supply chain rule provides a clear regulatory basis for such a ban, setting the stage for a concerted lobbying push in the future.

KEY OFFENSIVE POLICIES

The U.S. government has numerous options for directly bolstering the cybersecurity and resilience of critical military and civilian systems, which would mitigate not only the risk of Chinese sabotage but also other serious threats, like weather-related outages. With the electrical grid, for example, the Federal Energy Regulatory Commission could apply stronger mandatory cybersecurity standards to a larger number of entities and enforce them more vigorously.[330] The Department of Energy could establish a strategic reserve of large power transformers.[331] Congress could allocate federal money to shore up grid vulnerabilities.[332] Investments in disaster recovery capabilities at the federal, state, and local levels would also help mitigate the economic and societal damage caused by infrastructure outages once they occur. Any of these efforts might be expensive, so the federal government could focus first on a small subset of assets, like Defense Critical Electric Infrastructure, that face greatest risk from Chinese sabotage.

LIMITING CHINESE INFLUENCE OPERATIONS

RISKS OF INTERDEPENDENCE

U.S. officials have become increasingly vocal in warning of Chinese government efforts to influence American politics and society.[333] Several trends underlie this concern. First, Russia's interference in the 2016 U.S. presidential election brought much greater attention to the overall threat of foreign influence. Subsequent events, particularly the COVID-19 "infodemic" and the U.S. Capitol insurrection, further highlighted the fragility of America's political-informational ecosystem and its susceptibility to damaging manipulation.

At the same time, a more assertive China has increasingly sought to shape political narratives beyond its borders, especially on China-related issues. Much of this activity is overt—including Beijing's "wolf warrior diplomacy," its nationalistic state-sponsored media, and its punishment of foreign companies whose speech offends the Chinese Communist Party. But some efforts are covert—ranging from traditional influence (for example, cultivating agents within foreign political circles) to modern digital techniques (for example, fabricating armies of fake social media accounts that harass and vilify dissidents).[334]

China's foreign influence efforts have often focused closer to home, on targets such as Taiwan and Australia.[335] Nevertheless, in 2021 the U.S. Intelligence Community assessed that "Beijing has been intensifying efforts to shape the political environment in the United States to promote its policy preferences, mold public discourse, pressure political figures whom Beijing believes oppose its interests, and muffle criticism of China on such issues as religious freedom and the suppression of democracy in Hong Kong."[336] According to

the IC, China "considered but did not deploy influence efforts intended to change the outcome of the [2020] US presidential election."[337] Beijing apparently judged that the risks outweighed the benefits. This calculus may well change in the future, particularly if U.S.-China relations continue to deteriorate.

U.S. policymakers worry that Beijing could pressure the makers of popular Chinese apps like TikTok or WeChat to support covert influence campaigns that target Americans.

U.S. policymakers worry that Beijing could pressure the makers of popular Chinese apps like TikTok or WeChat to support covert influence campaigns that target Americans. Such a campaign might involve artificially promoting and/or suppressing certain content, perhaps leveraging the apps' capability to microtarget specific audiences. WeChat—which is popular among the global Chinese diaspora—already censors topics such as the Tiananmen Square massacre and the Falun Gong religious movement.[338] TikTok has acknowledged doing the same, but claims that it stopped in 2019.[339]

RISKS AND LIMITATIONS OF DEFENSIVE MEASURES

In theory, these concerns could justify major U.S. government restrictive measures such as app bans. In practice, however, there are good reasons for U.S. policymakers to think twice. To begin with, social media–based influence operations by China and other foreign governments may not actually be very effective. Researchers have struggled to find strong evidence that such operations can measurably alter their targets' beliefs and actions over time. A meta-analysis by Princeton University found only one high-quality empirical study on the question.[340] That study examined efforts by Russia's Internet Research Agency during the 2016 U.S. presidential election and found no effect on American Twitter users' political beliefs.

Although future research may identify stronger causal effects, it is worth keeping in mind the difficulties of large-scale public persuasion. To swing a U.S. presidential election, for example, Chinese influence actors would need to sway the small number of persuadable voters, or alter the turnout of voters, in battleground states. But Beijing would face stiff competition along the way. A Chinese influence campaign would be operating amid a cacophony of other voices—including political candidates and parties, community leaders, activists, traditional media commentary, and authentic citizen views—that dominate online as well as TV, radio, print, and word-of-mouth discourse. Domestic voices tend to have far more resources (billions of dollars are spent during a presidential election cycle), greater political sophistication, and thicker networks than even the most well-crafted foreign personas.

Just as domestic actors are the predominant voices in American politics, domestic players are also the main sources and amplifiers of political disinformation. Before TikTok entered

the American market, U.S.-based platforms like Facebook, Twitter, and YouTube already provided fertile ground for false, polarizing, and destructive political discourse. While these platforms have taken many actions to address influence operations, the problem seems to be growing even faster.[341] Fundamentally, user-generated content is produced on a scale that overwhelms existing content moderation tools, and platforms lack the financial and political incentives to undertake wholesale product redesigns to reduce the spread of harmful content. Market power is one part of the problem. The size of some major platforms helps to insulate them from pressure by users, advertisers, political leaders, activists, and employees to take stronger action against influence operations and other damaging content.

In this context, competitive pressure from Chinese apps like TikTok may have beneficial effects. TikTok is the most significant competitive threat to emerge in the American social media landscape in years. As such, its presence might help spur U.S.-based platforms to take stronger action against disinformation and other influence operations to burnish their reputations among advertisers, users, and outside stakeholders. Indeed, American activists and NGOs concerned about harmful online content have begun to explicitly compare TikTok's efforts against those of U.S.-based platforms.[342] This suggests that TikTok's presence has helped to intensify a reputational contest among platforms that could, if combined with regulatory and other pressure, raise the bar for responsible policies and practices by all players.

Slow-rolling efforts to shape Americans' general views of China and China-related policy are more readily detected and countered without resort to government tech controls.

A sound U.S. policy on Chinese influence operations would place companies like TikTok in the context of the larger American political-informational ecosystem. Seen in that light, Chinese tech companies play a limited and, perhaps, not entirely harmful role. Restrictive measures to counter Chinese influence operations should therefore be carefully vetted and focus on the highest-impact, most plausible threats.

RECOMMENDED POLICIES AND PROCESSES

Washington has a variety of tools to combat Chinese influence operations, but it should reserve technology restrictions such as app bans for the most serious risks. These would include the risk that China successfully alters a national election outcome or greatly reduces public confidence in an election. Potential influence operations with life-and-death consequences, such as those that markedly increase vaccine hesitancy during a pandemic, would also justify strong controls. However, long-term influence operations on less sensitive topics can often be managed in other ways. The bulk of Chinese influence activity in the United States seems aimed at shaping Americans' general views of China and China-related policy.[343] These slow-

rolling persuasion campaigns, while troubling, are no emergency. They are more readily detected and countered without resort to government controls.

It is unclear whether China currently has the ability to achieve any of the most dangerous influence outcomes, such as swinging an election. The U.S. government should conduct a careful, fact-based assessment to guide its use of technology controls. The Intelligence Community can help by estimating the Chinese government's capability and willingness to subvert Chinese commercial technology to influence Americans. But a China-focused intelligence assessment is only part of what policymakers would need. U.S. policymakers must also understand the American political and societal factors that would determine whether Chinese influence operations ultimately succeed or fail. This analysis would be crucial to properly size up the threat and weigh policy responses, yet the Intelligence Community and other government agencies lack the authority and expertise to conduct such an assessment.

To supplement the IC's analysis, the president could convene an outside advisory group of political scientists, communications experts, influence operations researchers, and technologists, perhaps under the aegis of the National Academies of Sciences, Engineering, and Medicine. This panel would examine the U.S. domestic environment's susceptibility to Chinese digital influence operations. For example, it might consider whether and how such operations could effectively persuade key voting constituencies or influence their turnout, considering factors like the partisan balance in swing states and the responsiveness of various constituencies to targeted digital campaigns. A government-sponsored analysis of this kind would need to be carefully designed to prevent real and perceived impingements on Americans' civil liberties.[344]

CASE STUDIES

TikTok. The most significant U.S. restrictions aimed at thwarting Chinese influence operations were Trump's executive orders attempting to ban TikTok and force its sale. These orders—which have never been implemented—were not justified based on publicly available evidence about influence threats. While Trump vaguely claimed that TikTok could "be used for disinformation campaigns that benefit the Chinese Communist Party," his administration offered no analysis of how effective these campaigns might be.[345]

Biden rescinded the TikTok ban. He replaced it with a new mechanism, the Commerce Department's ICTS supply chain security rule, to evaluate any Chinese software and hardware popularly used in the United States. Later, he published "a criteria-based decision framework" to help guide the Commerce Department's review of so-called "connected software applications" such as TikTok.[346] However, officials have not publicly confirmed whether TikTok is currently being investigated under the ICTS process.[347]

The Department of Commerce should carry out such a review, if it has not already started one. Biden's criteria offer a helpful starting point but should be refined to more specifically assess TikTok's threat as a medium for Chinese influence operations. Outside experts should draw on the best data and science to answer key questions including: whether TikTok's user base contains a large number of swing state voters; whether political content on TikTok content appears highly influential with a critical mass of those voters; whether corporate firewalls cannot reliably prevent Beijing from hijacking the platform in an undetected way during the course of an election; and whether the threat of Chinese influence operations via TikTok outweighs any benefits that TikTok may have on U.S. political discourse, including from competitive pressures on American tech platforms.

Long-term influence. Beyond TikTok, many proposals to limit Chinese influence capabilities in the United States do not focus on high-consequence, time-critical processes like elections. Instead, there is often worry that Beijing may gradually sway Americans' views about China-related policies. Confucius Institutes (Chinese public diplomacy initiatives embedded in U.S. universities) are frequent bogeymen, as is Chinese influence over U.S. entertainment sectors, like filmmaking and sports. CFIUS is reportedly in talks with Chinese tech giant Tencent about its ownership stakes in major U.S. video game developers.[348] At some point, relationships between Chinese tech companies and U.S. streaming platforms—like Netflix-Baidu and HBO-Tencent—will likely come under scrutiny. But none of these arrangements seem to represent the kind of urgent influence threat that justifies forceful U.S. government controls.

KEY OFFENSIVE POLICIES

While the U.S. government should continue to monitor and disrupt Chinese influence activities, its top priority must be restoring health to America's domestic information ecosystem. Washington must recognize that disinformation flourishes due to deep-seated and largely homegrown trends—in American politics, society, economy, and law—that have co-evolved over decades and become mutually reinforcing. Key factors include the TV and online media landscape (segmenting Americans into ideological echo chambers), social media business models (maximizing user engagement and enabling microtargeting), and political party dynamics (such as geographic sorting, gerrymandering, and primary election rules). Large-scale progress in combating disinformation would require profound national reforms in these and other arenas. The goal would

The top priority must be restoring health to America's domestic information ecosystem. This would disincentivize the production, amplification, and consumption of disinformation from all sources—not just China.

be to disincentivize the production, amplification, and consumption of disinformation from all sources—not just China.

True reform would be an extremely daunting task. The federal government's role in combating disinformation is poorly defined and heavily constrained by laws, norms, and political obstacles. Its tools are often tactical in nature (like sanctions) and oriented toward foreign threats (as with the Foreign Agents Registration Act). Federal overreach could actually worsen political distrust or create harmful precedents that future administrations could abuse. In fact, some of the most dangerous disinformers have been federal officeholders and candidates.

That said, experts have proposed a raft of policy ideas that the U.S. government could either implement or help to coordinate. These include strengthening regulation of online platforms; reforming campaign finance, election advertising, and redistricting laws; funding media literacy education; creating new public-private grant programs for journalists; and funding and facilitating basic research on influence operations.[349] Such policies have not been rigorously tested. In fact, there is very little empirical evidence about the impacts of influence operations or the effectiveness of countermeasures.[350] Still, improving the U.S. domestic information environment would be much more effective in curbing Beijing's influence operations than any China-specific measures. Moreover, these policies would help to address domestic disinformation, a far more serious problem.

DENYING SUPPORT FOR CHINESE AND CHINA-ENABLED AUTHORITARIANISM AND REPRESSION

RISKS OF INTERDEPENDENCE

Technology has enabled disturbing escalations and expansions of China's authoritarian and repressive policies, prompting American policymakers to step up U.S. tech restrictions in response. Washington's main concerns are twofold.

First, Beijing has spent years pioneering wholly new kinds of mass digital surveillance and censorship within China—including the Great Firewall, social credit systems, and ubiquitous AI-powered digital camera networks, to name just a few well-known examples. These systems are more fragmented and spottier than sometimes portrayed. Nevertheless, China's techno-authoritarian innovations have managed to expand the modern frontiers of social control, alarming Americans concerned with Chinese human rights and civic freedoms.[351] In particular, tech has helped to power Beijing's worst recent abuses, such as the ongoing campaign to marginalize Uyghurs and eliminate their culture, which Washington rightly calls genocide and crimes against humanity.[352] Mass facial recognition and biometric collection have become tools of ethnic profiling against Uyghurs, while Chinese drones have helped Xinjiang security forces to manage mass detention operations.

China's techno-authoritarian systems, while more fragmented and spottier than sometimes portrayed, have nevertheless expanded the modern frontiers of social control.

Second, many U.S. policymakers believe that Beijing is proactively exporting this techno-authoritarian model to other countries.[353] For example, Chinese digital surveillance and censorship systems have been sold to repressive regimes like Zimbabwe and Venezuela, with the latter receiving "a commercialized version of China's 'Great Firewall.'"[354] Washington fears that a "China model" of techno-authoritarianism will not only spread among authoritarian countries, but may also influence hybrid regimes and illiberal democracies, exacerbating and entrenching the global democratic recession.

Such an outcome would threaten U.S. interests (as well as American values), because Washington derives much of its geopolitical influence from the assumption of like-mindedness among governments and publics in democratic countries. More fundamentally, Biden argues that the fate of America's own democracy is bound up with that of democracy abroad, and he has rhetorically staked his national security strategy on that premise.[355] This linkage may motivate a broadening of U.S. efforts to combat global techno-authoritarianism, particularly in countries that purchase systems from America's chief rival, China.

A number of experts dispute the narrative that China purposefully exports techno-authoritarianism. They argue that Chinese foreign tech sales are driven more by the "pull" from governments who demand repressive tools than by any "push" from Beijing.[356] However, the strength of Beijing's "push" may grow over time, if China (like the United States and other historical great powers) comes to see a network of like-minded regimes as vital to its global interests. Moreover, even a mere "pull" from third countries, when eagerly satisfied by China, can pose challenges to U.S. agendas of human rights and democracy promotion around the world.

Initiatives like the Digital Silk Road help to spread Chinese hardware, software, and services, whose architectures embody Beijing's preference for a more controllable, government-led internet.[357] Western democracies, in contrast, promote international tech standards and governance models more compatible with free expression and civil society. To be sure, the United States and its allies have also provided substantial technology to friendly authoritarian regimes, from general cloud services to boutique hacking software.[358] Yet multiple democracies are taking tentative steps to reduce this complicity—for example, by cracking down on the reckless proliferation of advanced hacking tools.[359]

The development of Chinese techno-authoritarianism, and Beijing's more general authoritarian turn under President Xi Jinping, has prompted Washington to revisit its traditionally laissez-faire approach to China's human rights problems. After the 1989 Tiananmen Square massacre, the United States initially sought to condition the overall bilateral trade relationship on improvements to China's human rights record. But the Bill Clinton administration "ultimately abandoned this direct linkage" in favor of permanent most-favored-nation status, hoping that economic engagement would open up China politically (while benefiting

America economically).[360] Afterward, for nearly twenty years, the United States dealt with Chinese human rights abuses by levying very targeted punishments that did not jeopardize economic ties. For example, it imposed visa restrictions and sanctions on a handful of Chinese officials involved in the repression of Tibet and Falun Gong. It has also funded civil society and human rights activities in China, including software designed to circumvent internet censorship.

But recent U.S. technology restrictions reflect a tougher policy on Chinese human rights, with more economic bite. The Trump administration punished some of China's most prominent and successful tech firms, including SenseTime, Megvii, Hikvision, iFLYTEK, and Dahua, for their activities in Xinjiang—the first time that human rights violations had ever been cited in Entity List designations.[361] Likewise, Biden and Congress have cracked down on Chinese imports from Xinjiang, including tech products such as cell phones and solar cells, due to forced labor concerns.[362] The solar cell restrictions, in particular, will have widespread impact across the solar industry.[363] In addition, the U.S. government has announced sanctions and visa restrictions for certain Chinese tech companies and their employees involved in support to the Nicolás Maduro regime in Venezuela and other "regimes engaging in human rights abuses globally."[364]

RISKS AND LIMITATIONS OF DEFENSIVE MEASURES

Unlike past U.S. efforts to punish Chinese human rights abuses, these latest technology controls have had tangible economic consequences, resulting in canceled deals and rerouted supply chains.[365] Still, the recent restrictions represent just a small fraction of the broad-based China tech restrictions that some are advocating in the name of human rights and democracy. U.S. policymakers should understand this slippery slope before they slide much further.

Although recent U.S. government restrictions have focused primarily on Xinjiang, and Washington officially disavows any intent to impose sweeping reforms on China's larger political order, an emerging and politically diverse strain of thought argues for more expansive and assertive U.S. efforts to liberalize Chinese politics.[366] From the right, leading former Trump administration officials argue that the problem with China is its Marxist-Leninist ideology, and that Washington must therefore wage a Manichean struggle against Beijing's official thought system.[367] From the left, some human rights promoters believe that America's economic relationship with China "isn't worth the moral cost" and that U.S. leaders should mount

An emerging and politically diverse strain of thought argues for stronger U.S. efforts to liberalize Chinese politics. Policymakers should understand this slippery slope before sliding much further.

a "sustained effort" to "[counter] China's dictatorial apparatus."[368] From the center, national security voices such as the Atlantic Council's "The Longer Telegram" have called for the United States to aggravate "internal fault lines of domestic Chinese politics in general and concerning Xi's leadership in particular"—that is, to help effectuate Xi's removal from power.[369]

These ideas have growing influence, and they could well push U.S. tech policy down a perilous path. Human Rights Watch, for example, has asserted that "human rights abuses in China exist, and persist, in part because the US and others haven't insisted on holistic progress, and haven't imposed a price in response to them."[370] It therefore signed a letter with twenty-three other NGOs, including Freedom House and PEN America, advocating "a series of escalating actions against technology companies found to be contributing to China's mass surveillance, including by imposing Global Magnitsky sanctions."[371] But the premise is likely mistaken: the United States probably can't impose a price severe enough to deter the vast bulk of Chinese human rights violations. As a result, these "escalating actions" would have no clear stopping point.

Much of Beijing's techno-authoritarianism is a logical outgrowth of the Chinese political system itself—a system the United States cannot change and can barely seem to influence. The Chinese government seeks to preserve the Communist Party's power at all costs, and the Party stands for a rigid, domineering vision of the Chinese social order. So long as these facts remain true, Beijing will continue developing and employing technologies to achieve its authoritarian ends. Moreover, the indigenous Chinese technology base provides Beijing with ample capability to do so. This means that no amount of U.S. pressure is likely to compel China to relax the basic components of its domestic technological repression. At most, U.S. technology controls can impose modest costs and delays in specific cases where China currently relies on foreign components, such as advanced semiconductors.[372]

Meanwhile, a zealous U.S. campaign against the basic apparatus of Chinese techno-authoritarianism could inflict serious costs on the United States. It would likely devastate bilateral diplomatic ties, making cooperation on global issues more difficult and military conflict more likely. It would also be difficult to contain. Consider that virtually all Chinese tech companies contribute in some way to mass surveillance via the operation of draconian statutes such as China's Cybersecurity Law and National Security Law. In fact, Beijing's system of mass surveillance and control is suffused throughout the entire Chinese economic and societal structure. Chinese tech and non-tech companies alike send sensitive data to the state, participate in censorship activities, implement various social credit systems, and generally seek to anticipate and demonstrate allegiance to Xi's sociopolitical edicts.[373] Aggressive attempts to thwart Chinese mass surveillance, censorship, or techno-authoritarianism may well lead toward technological and economic divorce.

The United States probably has more room to address China's sales of repressive technologies to foreign governments. Some of these governments are less deeply authoritarian than

China and/or easier for Washington to influence due to specific bilateral relationships. Direct engagement should be tailored to the individual circumstances and motivations of third-country governments. Even then, the U.S. government should expect to encounter strong resistance in any global campaign to roll back techno-authoritarianism. U.S. democracy promotion efforts have historically struggled during periods when they were comingled and conflated with larger geopolitical campaigns, such as the Cold War and the War on Terror.[374] American strategic competition with China presents a similar problem for today's U.S. democracy promoters.

RECOMMENDED POLICIES AND PROCESSES

The United States is right to respond to the novel and serious twenty-first-century challenge of techno-authoritarianism, but it must also avoid embarking on an overambitious crusade with high risks and few rewards. U.S. policy on Chinese domestic techno-nationalism should focus on the most egregious abuses. Rather than waging a quixotic battle against entrenched Chinese policies like mass surveillance and internet censorship, Washington should keep working to punish and stigmatize Beijing's targeted repression of Uyghurs and other minority groups. Such groups do not benefit from what the Chinese Communist Party considers to be its authoritarian social compact, and they often seek to remain outside of it. In partnership with other countries, U.S. pressure might make some difference on Chinese repression of minorities. But if it does not, America can at least limit its moral complicity.

To implement this policy, the State Department and the Intelligence Community should collaborate with outside groups to identify Chinese technology systems that support Beijing's targeted efforts to repress minority groups. The Departments of Commerce and Treasury, and other agencies, could then compile the major ways that these Chinese systems rely on direct or indirect American support, including U.S. exports (of finished technology, raw inputs, or non-technology goods and services) and financing. Regulators would then consider which of these support flows can be feasibly controlled, based on the U.S. government's ability to trace their movement into and inside of China.

U.S. responses to Chinese "export" of techno-authoritarianism should depend on the "importing" country, the nature of the technology transaction, and the mixture of "push" and "pull" motivations at play.

U.S. responses to Chinese "export" of techno-authoritarianism should look different depending on the "importing" country, the nature of the technology transaction, and the mixture of "push" and "pull" motivations at play. When third countries are specifically seek-

ing out repressive tools and deem Chinese technology to be the best available, Washington can consider using sanctions and other restrictive measures as part of a broader dissuasion campaign aimed at both sides of the transaction—recognizing that the prospects of success will often be low.

When third countries are instead seeking general purpose technologies and the United States is concerned that Chinese products have authoritarian governance models embedded within them, Washington should focus on fostering the development of compelling Western alternatives. The U.S. government could, for example, help its companies better compete with China on costs, or double down on traditional American advantages such as reliability, security, technical assistance, and noncorruption. Restrictive measures could then buy time for these positive efforts to produce competitive alternatives to Chinese tech. Finally, there will likely be countries that pursue hedging strategies—intentionally dividing purchases between Chinese and Western technologies—to maximize their political and economic leverage and autonomy. Hedging countries are difficult to sway; U.S. tech policy might draw insights from other domains, such as arms and civilian aircraft sales, where hedging occurs.[375]

CASE STUDIES

The majority of Trump- and Biden-era technology controls related to Chinese human rights have wisely focused on ethnic repression in Xinjiang. This includes almost all of the Entity List designations of tech companies, for example.

DJI. In a few cases, however, the justifications were vague. In December 2020, the Department of Commerce designated four Chinese entities that "have enabled wide-scale human rights abuses within China through abusive genetic collection and analysis or high-technology surveillance, and/or facilitated the export of items by China that aid repressive regimes around the world, contrary to U.S. foreign policy interests."[376] "Abusive genetic collection" may refer to Xinjiang, but the Commerce Department did not say this. Notably, one of the four companies was the drone manufacturer DJI, which was presumably designated for its "high-technology surveillance" in China or its sales to repressive regimes.

DJI supported Xinjiang security operations as of 2017–2019, though publicly available information is scant and somewhat dated.[377] By declining to specify what exactly DJI had done (and when) and failing to reference Xinjiang, the Trump administration undermined the strength of its stand and allowed for speculation that human rights may have been a pretext. The U.S. government has many other concerns about DJI, including the potential military and intelligence applications of its products and the company's dominant market share in a growing industry where American companies have struggled to break through.[378]

Fortunately, the Biden administration has begun to stake a clearer position on DJI's human rights record. Its December placement of DJI on the Non-SDN Chinese Military-Industrial Complex Companies List indicated that DJI "has provided drones to the Xinjiang Public Security Bureau, which are used to surveil Uyghurs in Xinjiang."[379] This specificity helps to give businesses and governments around the world more stable expectations about the intention behind U.S. human rights policy and the planned use of restrictive tools. Ideally, the U.S. government would take the further step of outlining when DJI's problematic conduct occurred and how the firm could demonstrate reform over time to earn removal from these lists. It may be that DJI and other Chinese companies have no intention of undertaking such reforms or of publicly disavowing human rights abuses that Beijing downplays or denies. However, establishing the general terms of an off-ramp for sanctioned Chinese companies could help Washington clarify its redlines and demonstrate that its human rights concerns are sincere.

Xinjiang. The Biden administration should continue looking for and restricting other traceable forms of American support for China's technological repression in Xinjiang. The newly signed Uyghur Forced Labor Prevention Act is a good first step: it requires importers of goods from Xinjiang to prove those goods were not derived from forced labor, thereby making forced labor less profitable for Chinese companies and the Chinese government.[380] To complement these import restrictions, Washington should further curb the flow of American technologies or tech inputs into Xinjiang. Good candidates for control may include technologies that require significant customization or technical support (including patches and updates), because ongoing vendor-customer relationships can provide a platform to verify Chinese end users and end uses. Other possibilities include enterprise software or heavy "smart" equipment sold to Xinjiang-based entities.[381]

Surveillance sector. A handful of U.S. human rights–oriented tech restrictions have not focused on Xinjiang or other particularly egregious Chinese abuses. Biden's version of the Non-SDN Chinese Military-Industrial Complex Companies List allows designation of companies operating in China's "surveillance technology sector."[382] This undefined term could conceivably cover an enormous range of Chinese companies. The Treasury Department did try to clarify that it "expects to use its discretion to target" three kinds of Chinese companies: those supporting surveillance "that occurs outside of the PRC," those enabling "surveillance of religious or ethnic minorities," and those "otherwise facilitat[ing] repression or serious human rights abuse."[383] While the first two categories make sense, the final catch-all requires narrowing and clarification. For example, the Treasury Department's initial designations—of Hikvision and Huawei—failed to cite any specific human rights abuses or even explain which enforcement category they fell under.[384] (Subsequent designations of SenseTime, DJI, Megvii, and several other Chinese tech companies did provide relevant details on the firms' involvement in targeted surveillance of Uyghurs.[385])

Without more clarity on the intent behind this authority, the U.S. government may find itself adding an ever-larger and more diverse set of Chinese companies to its restrictive lists. Consider that in 2019, the House of Representatives voted 407 to 1 to require sweeping export controls of virtually all technologies "critical" to Chinese social control, surveillance, and censorship.[386] The Senate version of the bill that eventually became law omitted this provision.[387] Still, the initial House vote indicates broad support in Washington for an expansive and potentially costly campaign against China's entire techno-authoritarian model—not just the worst abuses.

Summit for Democracy. During the Summit for Democracy in December 2021, the Biden administration announced several new initiatives related to technology and human rights. While the initiatives were generally sound, they nevertheless demonstrated a continued reluctance to clarify U.S. policy objectives in this area. First, the United States joined with Australia, Denmark, and Norway to launch the Export Controls and Human Rights Initiative, aimed at "prevent[ing] the proliferation of software and other technologies used to enable serious human rights abuses."[388] The meaning of this initiative depends entirely on how "serious human rights abuses" is interpreted—a term that Washington has so far not defined.

Is Washington content to "affirm" existing and emerging democracies with their partnership and consent? Or does it seek actively to subvert and weaken authoritarian regimes?

Second, the White House announced a series of "grand challenges" to spur innovation in what it called "democracy-affirming technologies."[389] These technologies include censorship circumvention software, which the United States has long supported. Still, it is odd to brand such software as "democracy-affirming" rather than, say, "counter-authoritarian": its primary users are seeking to elude their own authoritarian governments, not "affirm" democratic ones. The new language has the effect of masking a major U.S. policy dilemma: is Washington content simply to "affirm" existing and emerging democracies, with these governments' partnership and consent? Or does the United States seek actively to subvert and weaken authoritarian regimes? The latter goal, while instinctually appealing to many in Washington, could be disastrous if applied to China and should not be used to justify significant bilateral tech restrictions.

KEY OFFENSIVE POLICIES

Washington retains a variety of traditional tools for addressing China's authoritarianism and repression, to include démarches, advocacy in international forums, and moral and material support for Chinese dissidents (especially those living abroad), in addition to targeted sanctions against companies and officials involved in the worst abuses. While these are unlikely

to deter Beijing's domestic techno-authoritarianism to any large degree, they are sometimes the best options available.

There is more the United States can do to combat techno-authoritarianism at a global level, including in places where China supplies repressive technologies. First, the U.S. government could further crack down on America's own witting and unwitting transfer of potentially harmful technology products, services, and know-how to human rights abusers. For example, Washington could be more parsimonious in licensing the export of advanced hacking services; better monitor the conduct of U.S. companies granted such licenses; and place postemployment restrictions on former U.S. government officials and contractors who have had access to classified American cyber operations techniques.[390] Second, the United States could more intensively press its allies on their sale (as with Israel, Italy, and Germany) or use (as with Saudi Arabia and the United Arab Emirates) of authoritarian technologies, whether sourced from China or elsewhere. The recent Entity List designation of Israel's NSO Group was a long-overdue step in this regard and has already had some positive effects.[391]

And third, America can better model pro-democracy, pro–human rights technology policies at home, thus earning the credibility to serve as a global leader on these topics. For example, U.S. federal agencies could hold transparent and inclusive discussions with civil society groups and other affected communities on difficult emerging issues such as law enforcement use of facial recognition. The White House Office of Science and Technology Policy recently announced a broad initiative along these lines, aimed at developing a "Bill of Rights for an Automated Society."[392] The practical impact of this "Bill of Rights" will depend on its successful implementation in federal rulemaking and legislation.

COUNTERING UNFAIR CHINESE ECONOMIC PRACTICES AND INTELLECTUAL PROPERTY THEFT

RISKS OF INTERDEPENDENCE

Technology is increasingly at the heart of America's many complaints about unfair and illegal Chinese economic practices.[393] For example, Washington argues that Beijing's extensive and opaque subsidy regime—which includes preferential government financing and procurement contracts—has helped Chinese tech giants like Huawei reach their dominant market positions. Another long-standing sore point is Chinese government discrimination against foreign firms in such areas as regulatory enforcement, licensing, and market access; American tech companies are the most likely of all U.S. firms in China to perceive such discrimination.[394] Likewise, China's practice of pressuring foreign companies into sharing trade secrets and intellectual property with Chinese corporate partners has disproportionate impact on U.S. companies built around specific technology rights, know-how, and data. And the list goes on.

As these examples illustrate, the technology sector is a major *target* of unfair Chinese economic practices. Technology can also *enable* China to obtain unfair advantages in all sectors. For example, the Chinese government carries out large-scale cyber espionage for the benefit of domestic firms, and it shields Chinese companies from accountability when they conduct their own cyber espionage. The U.S. government classifies these policies as unfair trade practices, and it worries that American technological links to China—for example, through the digital supply chain—provide additional access points for Chinese cyber thefts.

Although "unfairness" may be in the eye of the beholder, Washington sees China as violating specific bilateral and multilateral commitments, including WTO rules—that is, Beijing's own promises.[395] Unfortunately, the United States has had only limited success in resolving these issues via formal trade dispute mechanisms and direct diplomacy. Beijing remains strongly committed to its economic strategies, and international trade obligations are difficult to apply and enforce in these kinds of cases. With frustration mounting, Washington has begun to take more unilateral measures, including curbs on the flow of technology to and from China.

U.S. officials have pointed to several ways that technology controls help combat unfair Chinese practices. First, they can serve as a punishment meant to induce changes in Chinese behavior. When Trump implemented tariffs on large categories of Chinese goods—including tech products like smart devices, flash memory devices, and electronic components—he said he was imposing costs for China's intellectual property theft and seeking concessions at the bargaining table.[396] Second, technology restrictions can aim to counteract the benefits China receives from unfair practices and thus equalize the economic competition, in much the same way that countervailing duties offset foreign subsidies. Commerce Secretary Gina Raimondo once told Congress that the Entity List—which prevents designated Chinese companies from obtaining U.S. technologies, ostensibly for national security reasons—can "level the playing field for the American worker."[397] Finally, technology controls can reduce China's opportunities to act unfairly. For example, the U.S. government has strongly discouraged American telecoms from using Chinese equipment, in part so that Beijing cannot leverage this equipment to steal U.S. intellectual property.

RISKS AND LIMITATIONS OF DEFENSIVE MEASURES

However, U.S. government tech restrictions can also create risks for Washington's trade agendas with China and other countries. In particular, U.S. efforts to counter unfair Chinese practices might themselves be deemed unfair or violate international trade rules. Trump's tariffs offer a recent example. Though he imposed them in the name of countering illegal Chinese intellectual property theft, a WTO panel ruled in 2020 that one large tranche of Trump's tariffs was itself illegal.[398] The United States thus faces a dilemma. If it sticks to formal trade dispute mechanisms and nonconfrontational direct diplomacy, then Beijing's systemic trade abuses will likely continue. But if Washington reaches instead for more powerful unilateral tools, like tariffs and government tech controls, then it could end up destabilizing the very global trade order that it professes to be enforcing and protecting. And the WTO's further erosion or collapse might well leave U.S. leaders with less ability than before to curb unfair Chinese practices. Washington has an excellent record of winning WTO cases against China—although the most serious and systemic trade issues, like subsidies and intellectual property theft, have proven hardest to address in that forum.[399]

Washington's China trade dilemma involves more than just technology, and Trump has not been the only president to face it. The Obama administration took issue with several WTO appellate rulings, including those seen as overly accommodating to China. In response, Obama blocked the appointment of multiple WTO appellate judges—an unprecedented and controversial series of interventions.[400] Trump escalated this practice, eventually blocking all WTO appellate appointments and thus denying the body a quorum.[401] Biden has affirmed the Trump policy—in effect, halting the appeals process for all countries until the WTO resolves U.S. concerns with the process and substance of dispute settlement.[402] Washington's goal is to force reforms of what it sees as a broken system that tolerates unfair Chinese practices (among other problems), but its tactics risk weakening the system further.

Nonconfrontational diplomacy probably cannot stop Beijing's systemic trade abuses. But more powerful unilateral tools could destabilize the global trade order.

While the United States plays hardball with the WTO dispute system, its barrage of new China-oriented tech controls may also test the limits of WTO substantive principles. At their core, these principles bar trade barriers that discriminate by national origin.[403] Many recent U.S. tech restrictions would seem to clash—in spirit, if not in letter—with that idea. Consider executive orders or regulatory actions whose terms apply exclusively to China, such as the Non-SDN Chinese Military-Industrial Complex Companies List, the Section 889 blacklist, and Trump's attempted bans on TikTok, WeChat, Alipay, and other Chinese apps. Other U.S. tech controls, like the FCC's Covered List, are technically not focused on any specific country but have so far been used almost exclusively against Chinese firms. The Commerce Department's ICTS supply chain security rule and the Trump Energy Department's bulk power system regulation applied just to China and a handful of other designated "foreign adversaries." Meanwhile, CFIUS and the Entity List are not explicitly tailored to China, yet China has become a primary focus of enforcement. All these tools function as trade barriers by placing substantial limits on Chinese companies' ability to buy technology from, sell technology to, or otherwise transact with Americans.

To U.S. leaders, such policy tools are familiar, accepted, and fully compatible with the international trade system. The United States continues to cite its long-standing position that national security–related restrictions fall outside of WTO scrutiny.[404] Although most other countries (including U.S. allies) do not accept the existence of such a broad exception, they have traditionally declined to press the point, because the U.S. government historically did not impose many such barriers.[405] Yet Washington's self-restraint is now loosening, in large part due to concerns about China and its technology. In the tech domain alone, Washington has greatly increased the number and scope of trade, investment, and other economic restrictions in just the last few years. Meanwhile, U.S. officials in both parties flirt openly with an expanded definition of "national security" that encompasses "economic

security." If the American "national security exception" becomes an "economic security exception," it would virtually negate the WTO framework.

Already, foreign governments have seized on the precedents created by U.S. actions to assert their own national interests. Since 2016, Japan, Russia, the United Arab Emirates, and Saudi Arabia have all for the first time cited an American-style national security exception in WTO disputes.[406] Beijing could take the same path, using the United States' own position to justify Chinese policies (like market access restrictions) that Washington fervently protests.

The United States must think hard about its endgame for bilateral and global trade, in the technology sector and beyond. In a best-case scenario for Washington, its tough tactics somehow push Beijing (and other countries) to accept strong, enforceable new trade rules that rein in unfair Chinese practices. This would be a monumental achievement: negotiations on new WTO trade rules have stalled for the last two decades, and the United States would now be negotiating from a position of reduced global influence, amid heightened tensions with a strategic competitor. In a worst-case scenario, the WTO system collapses under the weight of U.S.-China economic conflict. Although Washington would still have other bilateral and multilateral trade agreements to fall back on, China and other nations would likely institute new economic and national security–related trade barriers that harm the United States.

Some amount of risk-taking by Washington makes sense. The status quo should not be idealized: open trading principles are far from fully implemented and sometimes more honored in the breach, particularly by China. The United States therefore has strong reason to implement measures it thinks will protect American economic interests and add to pressure for structural reforms. It also has reason to believe that the WTO system will merely bend, not break, under this pressure. The system has survived for decades despite numerous international disputes and changing geo-economic and geopolitical dynamics. U.S. tech controls have so far not sent bilateral trade ties with China (let alone the larger WTO system) into a death spiral.

Still, the United States must tread carefully. If present trends continue, American technology restrictions aimed at China will significantly broaden and intensify in the coming years, further raising the stakes. Some of the rhetoric heard in Washington—including limitless notions of "economic security," or the brute goal of "destroying" China's most prominent companies—directly contravenes international trading principles and implies a dangerous reckoning in the future. Worse, these risks often go unacknowledged: U.S. officials and analysts are rarely willing to describe America's China-oriented tech restrictions as trade barriers that skirt the line of national discrimination. By avoiding this issue, they sidestep fundamental questions: Are U.S. actions compatible with today's international rules? If not, what new rule set would Washington propose? Would other nations agree to these new

rules? And if China and others began to leverage any new rules for their own advantage, would Americans still benefit in the end?

RECOMMENDED POLICIES AND PROCESSES

The use of technology controls to address unfair Chinese economic practices should be nested within a comprehensive U.S. strategy for shaping the international trading system as a whole. China would be a major but not exclusive focus of this strategy. The overall goal would be to describe a desired U.S. end-state for international trade. Fundamental questions include whether Washington should seek to reinforce WTO open trading principles or partially roll them back, and what new kind of rules the United States might prefer instead. For example, what would be the desired parameters of an internationally approved "national security exception"? At its heart, a U.S. strategy should deal with practical questions such as which other major nations could be feasibly brought on board, and what enforcement mechanisms could realistically achieve and sustain the American vision over time.

Due to the complexity of international trade and its sweeping implications for all U.S. interests, the process for developing a comprehensive trade strategy should be inclusive. For example, the NSC might share leadership of this process with the National Economic Council and the Domestic Policy Council to ensure that its outcome serves the domestic needs of the American people. USTR and the State Department would be important but not dominant voices. The Intelligence Community could vet the likelihood of various scenarios, including a successful effort to reform the international trade system, as well as alternative futures such as the unintended degradation or collapse of the system. The final strategy, once ratified by the president, would guide how regulatory bodies such as the Commerce Department, Treasury Department, and CFIUS evaluate the purpose, benefits, and risks of technology controls aimed at combating unfair Chinese economic practices.

CASE STUDIES

The Biden administration has taken some positive steps toward an international trade strategy, but it has not yet publicly addressed the core policy dilemmas. In May 2021, U.S. Trade Representative Katherine Tai delivered a report to Congress articulating Biden's official trade policy agenda.[407] It promised a major focus on combating unfair Chinese economic practices, especially those that "threaten our technological edge [and] weaken our supply chain resiliency." Although Trump's government had said the same thing, the Biden report rightly called for "a comprehensive strategy and more systematic approach than the piecemeal approach of the recent past." To that end, it announced that "the Biden

Administration is conducting a comprehensive review of U.S. trade policy toward China as part of its development of its overall China strategy."

This review culminated in October with a major speech by Tai on China. Tai criticized China for "pour[ing] billions of dollars into targeted industries and continu[ing] to shape its economy to the will of the state"—citing solar cells and semiconductors, among other examples.[408] She vowed to "directly engage with China on its industrial policies." Tai addressed the WTO that same month, reaffirming America's commitment to the body while calling for unspecified institutional reforms in several key areas.[409]

Tai's report affirmed that "opening markets and reducing trade barriers are fundamental" goals. Yet it made no mention of Chinese tech companies recently cut off from U.S. markets, suppliers, or investors.

Tai's statements contained laudable objectives and welcome messages. Nevertheless, they still elided basic tensions in the U.S. approach. The report to Congress, for example, affirmed that "opening markets and reducing trade barriers are fundamental to any trade agenda." Yet it made no mention of the many ways that Washington has sought to curb technology trade with China. It said nothing about Huawei, ZTE, DJI, Hikvision, or other Chinese tech companies recently cut off from U.S. markets, suppliers, or investors. It was silent on the growing use and expanding scope of restrictive tools like the Entity List, CFIUS, export controls, and IEEPA. It omitted any discussion of America's position on the WTO national security exception and the rise of copycat claims by other countries.

Such omissions aren't unusual in public (or even private) U.S. government strategy documents. The Biden administration probably wants to reserve discretion at the negotiating table and to avoid taking controversial stands before they prove necessary. The important thing for now is that senior U.S. officials deliberate on these basic dilemmas in a structured way. While some technology restrictions are appropriate and sustainable responses to unfair Chinese practices, there must be an anticipated stopping point. The Biden administration should fully understand the risks involved, think about its endgame, and eventually signal its intentions to China and other trading partners. Simplistic invocations of "unfairness" or "U.S. national security interests" will no longer suffice to navigate these choppy, uncharted waters.

KEY OFFENSIVE POLICIES

Tech controls or no tech controls, Washington lacks any easy path to stop unfair Chinese economic practices. Such practices are highly beneficial to Beijing and hard for outsiders to monitor, let alone deter. Successive U.S. administrations have protested and pushed back with little success. To change these dynamics, Washington needs to amass significant leverage over China, then use some combination of bilateral and multilateral talks—including at international forums like the WTO—to secure and enforce an agreement with Beijing.

Trump made one attempt to accomplish this, using unilateral tariffs for leverage, but he botched the negotiations by settling for market access concessions rather than seeking major structural reforms. Biden is taking the smarter, albeit slower approach of trying to cultivate a united front among U.S. allies and trade partners (while holding onto Trump's tariffs as a bargaining chip). For example, the recently established U.S.-EU Trade and Technology Council has developed an ambitious multilateral agenda to coordinate policy on a number of key issues relevant to Chinese technology and decoupling.[410] And Washington has been using multilateral fora like the G7, the G20, and the WTO to discuss "market distortions and other unfair trade practices" by China.[411]

Time will tell whether Biden's approach yields concrete results. America's European and Asian allies have so far proven less inclined than the United States to squarely confront Beijing over its unfair practices. In the end, Washington may need to make concessions of its own to China (and others) as part of the negotiating process. If China remains obstinate, then Washington will face difficult choices about the future of international trade.

COMPETING AND LEADING IN STRATEGIC INDUSTRIES

RISKS OF INTERDEPENDENCE

As China's technological prowess grows, U.S. officials worry that China could come to lead and possibly dominate the most economically significant tech industries of the future. This concern is not about China's *unfair practices* per se; it is about *unfavorable outcomes* for U.S. competitiveness. The distinction is often glossed over, yet it is crucial. Even on a level playing field, China could potentially outcompete the United States in some tech industries. This troubles American policymakers, most of whom have only known an era of peerless technological leadership by U.S. companies. They now see China catching up (or even moving ahead) in the technology areas expected to matter most for twenty-first-century economies.

China has already become the global leader in 5G telecommunications equipment (a crux of the future digital backbone), as well as commercial drones, Internet of Things devices, mobile payments, solar cells, and smart cities, among other technology areas. And where China does not lead, it is often a world-class competitor—for example, in AI (the most-hyped of all emerging technologies), smartphones, electric vehicles, and much more. While unfair economic practices have contributed to China's success, they do not tell the whole story. China ranks first globally in STEM graduates and second in R&D spending.[412] Its geographically concentrated tech hubs have revolutionized supply chain and manufacturing integration. And government tech policies like Made in China 2025 and the Digital Silk Road, although often misunderstood and overestimated in the West, nevertheless demon-

strate Beijing's national focus on technology strategy—a relative weak point for the United States in recent decades.[413]

If China halted all unfair practices tomorrow, its tech industry would still likely represent the most significant challenge to U.S. technology leadership and global competitiveness since the rise of Japan in the 1980s.[414] Of course, China's challenge might fade over time, just as Japan's did. China could experience a bursting debt bubble, or a "middle income trap," among other potential causes of technological stagnation. But Washington has little ability to predict, let alone influence, such developments. If the current trajectory continues, the United States will have several problems on its hands.

If China halted all unfair practices tomorrow, it would still likely represent the most significant challenge to U.S. technology leadership since Japan in the 1980s.

At the most basic level, losing America's technological edge in major industries would mean fewer U.S. jobs, lower GDP, reduced tax revenue, and other macroeconomic setbacks. It would also diminish the global influence that America derives from its technology leadership. For example, U.S. dominance of digital platforms has provided unparalleled intelligence collection opportunities and helped to project certain American political and cultural values into foreign societies. It also provided the Biden administration with concrete leverage to shape and secure a recent global tax agreement.[415] Loss of American technological dominance would lessen those forms of power and influence. Moreover, it would weaken the so-called "national security innovation base," a Washington term for the American tech industry's special role in generating new U.S. military and intelligence capabilities.[416] No country wants to fall behind in these ways, and the United States is particularly reliant on its technological leadership as a source of economic and national security advantages.

Still, the United States could survive and even thrive despite a loss of dominance in some important tech areas—so long as it remains relatively competitive overall. The more serious threat is that China itself becomes so technologically dominant that American companies are largely frozen out of many important markets. U.S. leaders worry that China's technology gains could become strongly self-reinforcing, paving the way toward just this kind of dominance.[417] Certain tech markets—5G telecommunications equipment is a prime example—have high barriers to entry, significant first-mover advantages, and deep linkages to many other sectors. In such cases, China's early leadership could enable its companies to lock in global market share and seek to dominate related or adjacent industries. Once Chinese firms secured strong enough positions, they and the Chinese government could use unfair practices, like predatory pricing and exclusionary deals, to further entrench their advantages.

These worries have driven U.S. policymakers to try to curb bilateral tech ties that Washington sees as helping China catch up with or overtake the United States—especially in the most economically important technology areas, where long-term leadership is at stake. Two laws passed in 2018 illustrate this trend.

The Foreign Investment Risk Review Modernization Act (FIRRMA) calls for CFIUS to scrutinize transactions involving "a country of special concern that has a demonstrated or declared strategic goal of acquiring a type of critical technology or critical infrastructure that would affect United States leadership in areas related to national security."[418] This is a clear mandate to thwart Made in China 2025, Beijing's strategic technology development plan. Likewise, the Export Control Reform Act (ECRA) instructs the Commerce Department to limit exports of "emerging and foundational technologies." Although these categories remain undefined, Made in China 2025 has served as a starting point for U.S. government analysis.[419] Technically, both FIRRMA and ECRA describe national security as their sole focus. But economic considerations helped spur Congress to act and will certainly influence future regulatory actions.

RISKS AND LIMITATIONS OF DEFENSIVE MEASURES

Preventing China from seizing control of key tech industries is a worthy policy goal. The United States should not underwrite its own economic dislocation if it can avoid doing so. Nevertheless, there is risk of overreach—particularly if Washington views technology controls as the primary means of maintaining its own preeminence, rather than as stopgap measures to thwart Chinese dominance so that other American investments have time to take root. U.S. policymakers should keep several points in mind.

First, the "cure" of government technology controls can sometimes be as harmful as the "disease" of aggressive Chinese competition. Export controls, Entity List designations, and similar restrictions reduce American companies' sales to China, cutting the revenue available to plow back into R&D. Visa bans, deemed export curbs, and supply chain security requirements restrict U.S. access to Chinese talent and subcomponents, imposing higher costs and greater delays on American innovators. Inbound investment restrictions limit U.S. firms' opportunities to raise capital from and achieve corporate synergies with Chinese entities. If U.S. controls are unilateral, then European and Asian rivals can gain competitive advantages over American firms. Moreover, China can and will retaliate against significant restrictive measures.

For these reasons, trade groups like the Semiconductor Industry Association, the Business Roundtable, the National Association of Manufacturers, and the Information Technology Industry Council have sought to limit the use of ECRA and similar new authorities.[420] Although trade associations have narrow vested interests that can diverge considerably from

the national interest, the coalitions raising these concerns have been notably broad-based and diverse. They include a set of groups that represent "all major research universities and medical schools in the United States," which collectively warned that "overly broad or vague controls will result in unnecessary restrictions that will stifle scientific progress and impede research."[421]

Second, technology controls can conflict with Washington's stated objective of fair, rules-based economic competition, as described earlier. WTO rules do not allow a country to curb trade in certain industries just because they are seen as economically important. In fact, this runs directly counter to WTO principles. If the United States publicly embraces an economic strategy of restricting trade in important tech industries, then China and other countries will step up protections of their own "strategic" industries (whether tech or non-tech). Although the WTO system urgently needs reforms, U.S. leaders have not yet articulated a credible vision for reform or a plan for gaining agreement from China and other major trading partners.

Third, it is not easy to identify economically strategic technologies that merit governmental controls. The U.S. government has historically struggled to make accurate, useful predictions about what innovations will be important in the future and to draw administrable lines around fuzzy technology areas.

In the 1990s, economic competition from Japan spurred the U.S. government and outside groups to produce a number of so-called critical technology lists to help inform policymaking.[422] Defining "criticality" proved to be a major challenge, given the many different U.S. interests impacted by technology. In part for this reason, the lists were usually too broad (naming whole fields of practice, such as "programming languages") and/or too long (some had over 100 items) to be useful in policymaking. In hindsight, it is also apparent that many items designated as critical turned out not to be, while some technologies excluded from the lists wound up having vast economic impact. For example, the 1995 White House list cited "virtual reality software" (still a marginal industry today) as critical, but omitted personal mobile devices (a then-extant technology that has since revolutionized global communications).[423] Critical technology lists ultimately failed to have much policy impact, and the effort was abandoned in the 2000s.

The Trump administration sought to revive this moribund tradition by publishing a "critical and emerging technologies list" in October 2020.[424] Unfortunately, this list reflected many old pitfalls. It was vague and equivocal in defining the criteria for inclusion—at one point saying the listed technologies were critical to overall U.S. national security and/or economic advantages, then later calling them critical merely for U.S. government agencies. Although the list was manageable in size (just twenty items), the individual entries had sweeping scope: "Energy Technologies," "Communication and Networking Technologies," "Data Science and Storage," "Medical and Public Health Technologies," "Biotechnologies,"

and so on. And its publication so late in a presidential administration meant that Trump's list, like others before it, lacked clear policymaking relevance.

The U.S. government should develop more detailed and robust internal processes for evaluating the economic consequences of emerging technologies.

The Biden administration refreshed this list in February 2022.[425] The new categories of critical and emerging technologies do not differ much from Trump's, though Biden's version helpfully elaborates on each category by defining multiple subcategories. Still, the list's selection criteria and policymaking purpose remain unclear. Does it name technologies that "may be critical to U.S. national security," or merely those with "the potential to further" it? Both formulations are given. National security, meanwhile, is defined as including "economic prosperity and opportunity"—a defensible framing that nevertheless clouds the specific rationale behind each entry's inclusion, making it harder to use the list as policy guidance. In fact, the White House emphasized that "*this list should not be interpreted as a priority list for either policy development or funding*."[426] Yet it also recommended that agencies consult the list when designing "measures that respond to threats against U.S. security" and "initiatives to research and develop technologies"—that is, policy development and funding.

Washington does not necessarily need (and probably shouldn't try to create) a singular list of all technologies critical for every U.S. national interest. But it does need something beyond what it has now. Routine policy actions like export control listings and CFIUS investigations already require some predictions of future technological importance, despite the inherent difficulties. Yet formally, these policy tools have an exclusive focus on national security concerns, with economic interests left as a potential but largely undefined (and sometimes unspoken) consideration. The U.S. government should develop more detailed and robust internal processes for evaluating the economic consequences of emerging technologies, so that agencies can tailor controls to critical areas where China threatens to secure dominance.

RECOMMENDED POLICIES AND PROCESSES

Government technology controls should play a specific, limited role in the U.S. quest to maintain economic leadership and competitiveness. The president should instruct regulatory agencies to institute restrictive measures only when necessary to hold off looming Chinese dominance in defined strategic industries, thus buying time for other positive American investments to bear fruit. Implementing this guidance would involve creating a formal governmental process to conduct (or oversee) geo-economic analysis of technologies. A new process would need to avoid replicating 1990s-era mistakes while also adapting to today's geostrategic, technological, and governance realities. Fortunately, scholars and

independent analysts have offered a number of useful recommendations and lessons for policymakers.[427]

One approach would be for geo-economic assessments to identify technologies that rate highly across three dimensions: economic value, defensibility, and urgency of control. Each of these dimensions can be defined and measured in various ways. For example, highly economically valuable technologies might include those set to become top exports (as semiconductors are now), to produce the largest companies of the future (as with today's digital advertising sector), or to have powerful second- or third-order effects on many other industries (like clean energy or advanced batteries).

Highly defensible technologies would have strong winner-take-all qualities, meaning that a market leader could capture disproportionate gains and then defend its position for long periods, perhaps due to network effects (as in today's social media market) or high barriers to entry (as in telecommunications equipment). Frameworks for evaluating technological defensibility can be found in antitrust economics and venture capital investing, among other domains. Finally, technologies in urgent need of control are those where a window of competitive opportunity could soon close. Washington might assess whether technological and market developments during the next five to ten years could enable China to achieve and lock in long-term dominance.

If the United States publicly announces an official process for identifying and controlling economically strategic technologies, China and other countries would likely accuse the United States of a flagrant assault on WTO principles. Therefore, the U.S. government should seek to maintain its tradition of requiring that new technology controls have a national security justification, even if, internally, the initial impetus for considering a control is economic competition. Ideally, new controls should be framed as continuations of historic U.S. policy, to include American claims of a WTO national security exception; new precedents should be created only when necessary. The U.S. framework for identifying economically strategic technologies should probably remain confidential or classified.

CASE STUDIES

5G. The Trump administration was right to identify 5G telecommunications equipment as a major target for technology restrictions. Countries all over the world are making or planning massive investments in such equipment, and deployment is expected to drive many ancillary innovations in areas such as autonomous vehicles, the Internet of Things, and mobile apps. Because these are generational investments, market leaders like Huawei have an opportunity to establish firm footholds in the purchasing countries. And the purchases are all happening within a short time frame as countries race to deploy 5G, meaning the window of opportunity will close within the next few years.[428]

Semiconductors. Semiconductors are also a strategic industry: they rank among the most important technologies by overall sales and are essential to almost all modern activity, while the most advanced semiconductors will drive next-generation technological applications like machine learning. Yet U.S. semiconductor firms also rely on China for much of their revenue, and most experts believe China still remains about a decade behind the United States and its allies in key aspects of semiconductor design and manufacturing.[429] U.S. government controls on this sector should therefore be carefully targeted.

The United States should restrict China from accessing only the most advanced semiconductor technology, while allowing sales of commodity chips to help maintain U.S. market share and fund R&D. The Trump administration was right to press the Netherlands to prevent export of extreme ultraviolet lithography systems to China.[430] These would facilitate manufacture of 5- and 7-nanometer node chips and thus help China to leap well ahead of its current capabilities. At the same time, the Biden administration was also right to grant U.S. firms licenses to sell automotive chips—considered commodity items—to Huawei.[431] A more difficult case was Trump's tightening of rules for so-called deemed exports, in effect requiring more scrutiny for Chinese nationals working in the U.S. semiconductor industry.[432] Although the costs and benefits are difficult to independently assess, it makes sense in principle to prioritize protection of critical, cutting-edge intellectual property and trade secrets in the semiconductor sector.

Consumer devices. However, very few technologies sold in large quantities to individual consumers should be subject to government control on the grounds of economic criticality. Smartphones, laptops and desktop computers, Internet of Things devices, consumer-grade drones, home network hardware, gaming systems, and most mobile apps should be relatively unrestricted on economic grounds. These industries are generally commoditized or will likely become so in the near future. They typically feature gradual, incremental shifts in technology, pricing, and market share over time—not defensible moats or closing windows of opportunity for one country to gain enduring dominance. For example, the Biden administration should not add Honor, a smartphone maker spun off from Huawei, to the Entity List, as it is reportedly considering.[433] Republican members of Congress have urged the designation, but their vague argument seems premised on the spurious notion that Honor operates "in a strategic sector."[434]

AI. Artificial intelligence is frequently described as economically strategic—perhaps more often than any other technology area. Evangelists claim that AI will transform all other industries and become a primary determinant of competitive success. Even if this is true, competitive advantages in many aspects of AI do not appear to be very defensible. Foundational know-how proliferates widely (due to open, international academic ecosystems) and would be difficult to control (due to the relative ease of stealing or copying algorithms and training data), compared to more physically embodied trade secrets like semiconductor manufacturing equipment.[435] Thus, U.S. government efforts to control AI research or software would often be ineffectual.

While China is quickly progressing in AI capabilities, there is also no clear sign that it verges on somehow dominating the industry. China does have certain advantages, including its ability to pool large stores of data with less concern for privacy and its access to massive, cheap sources of labor for data cleaning and preparation. Yet the United States still produces higher-quality AI research and has better access to data from key Western markets. At best, China seems capable of developing a modest lead in certain subdisciplines, like facial recognition, where Chinese advantages seem most relevant.[436] But any such lead would be neither comprehensive (across all AI applications) nor permanent (foreclosing future U.S. competition).[437]

AI does appear to have some strategic terrain—bottlenecks in the AI value-chain where one nation might gain outsized advantages and seek to exclude its competitors. Semiconductors, discussed earlier, are one example. Another is the pool of high-end scientific and engineering talent. While the overall AI field is large, many of the most promising breakthroughs have come from a few individuals and companies, such as Alphabet's DeepMind.[438] Concentrating this talent together in one ecosystem seems to create disproportionate innovative benefits—although the effect is likely temporary, as AI innovations often proliferate widely within a few years. Thus, the United States should focus first and foremost on attracting the best AI talent and avoid decoupling the labor pool. This means ensuring that U.S. visa restrictions do not drive away top Chinese AI researchers from American universities and companies, unless a clear national security threat exists.

KEY OFFENSIVE POLICIES

America's ability to compete against China will depend much more on the health of the U.S. innovation ecosystem (so-called "offense") than on any attempt to thwart or impede Chinese technological progress ("defense"). There are at least three major categories of offensive opportunities.[439]

First, Congress should greatly increase the amount of federal R&D spending. Such spending was historically pivotal in creating what we now know as Silicon Valley, but has atrophied in recent decades.[440] The draft U.S. Innovation and Competition Act and America COMPETES Act, although not without problematic elements, mark important steps toward committing greater federal resources to R&D. Second, Congress should invest more in the social and physical infrastructure that supports technological innovation and access. Examples include STEM education (at all levels), STEM workforce training, a national research cloud, and rural broadband.[441] Third, the Justice Department and the Federal Trade Commission should continue stepping up their antitrust scrutiny of the tech sector, and Congress should move forward with intelligent statutory reforms to promote competition. These would help ensure that the U.S. tech sector remains dynamic and innovative.

OBTAINING GENERAL LEVERAGE OVER CHINA

Technology itself is not always the sole concern animating U.S. tech policy. In the China context, U.S. leaders have sometimes used the technology relationship as a pawn in wider bilateral negotiations. For example, the Trump administration used its Entity List designations of ZTE and Huawei to help advance broader trade talks with China. During the talks, Trump rescinded the ZTE designation as a personal gesture to Xi, and held out the prospect of sparing Huawei during subsequent negotiations.[442] Yet Trump did not use these chits to secure major concessions on tech-related issues like intellectual property protection. He accepted relatively weak commitments on those issues and instead bargained for China to buy more U.S. agricultural products and grant market access to American financial services firms. In a roundabout way, Trump used the leverage of technological controls to move China on unrelated matters.

The Entity List designations of ZTE and Huawei, and the attempted ban and forced sale of TikTok, suggested a template. These episodes taught U.S. policymakers that they held the power of life and death over certain Chinese tech companies, and that Beijing prizes these companies enough to bargain over their fate. Given how much Washington wants from China in numerous domains, and how few reliable tools the United States has for bringing Beijing to the table, there is strong temptation to use technology controls as a bargaining chip in non-technology-oriented negotiations.

It is hard enough to design a U.S. tech policy that succeeds on its own terms. This can become virtually impossible if tech issues become entangled with unrelated objectives.

This kind of maneuver should be rare, however. Because U.S.-China technology ties are so important and sensitive in their own right, there are few other issues salient enough to justify their use as a bargaining chip. Doing so risks adding even more pressure to an increasingly fragile technology relationship. It is hard enough to design an American tech policy that succeeds in addressing the complex set of challenges and opportunities that China represents. This can become virtually impossible if tech issues become entangled with, and subordinated to, unrelated policy objectives.

RECOMMENDED POLICIES AND PROCESSES

The president should instruct regulatory agencies, diplomats, and trade negotiators not to use China-related technology restrictions as leverage for unrelated matters, barring exceptional circumstances. Biden should consider exceptions only when they are likely to advance a handful of supreme priorities, such as combating climate change. Before making an exception, the president should ask the Intelligence Community and his negotiating team about the odds that doing so would help win valuable concessions from Beijing.

CASE STUDIES

Phase One trade talks. Trump's maneuvers in trade talks with China illustrate both the promise and the peril of using technology controls as general bilateral leverage. ZTE was originally placed on the Entity List in 2016 for violating U.S. sanctions against Iran and North Korea. So when Trump later granted the company a reprieve to advance his trade talks with China, domestic critics argued that he had compromised U.S. national security.[443] The gambit did make sense in theory. The Phase One trade talks provided a rare opportunity to address structural issues in the U.S.-China economic relationship—a prospect of surpassing value to the American people. By comparison, unyielding enforcement of sanctions on Iran and North Korea was relatively unimportant.

Trump's maneuvers in trade talks with China illustrate both the promise and the peril of using technology controls as general bilateral leverage.

In the end, though, Trump squandered whatever leverage these tactics gave him. He chose to focus his Phase One deal on minor matters like the trade deficit, while neglecting more central grievances such as Chinese subsidies and forced technology transfer. The Entity List maneuver therefore accomplished little—except that it caused China and many other observers to see the list itself as a tool of realpolitik, not a legitimate national security instrument.

Climate change. The Biden administration may face its own decision points in climate change negotiations with China. China has already made some recent climate commitments, but much more work remains. Given the paramount importance of addressing climate change, Biden should consider whether defensive technology measures could serve as bargaining chips—tightening restrictions to increase U.S. leverage, or loosening them to facilitate a deal. The Justice Department, for example, agreed in September 2021 to resolve charges against Huawei CFO Meng Wanzhou, allowing her to leave Canadian custody and return to China. Two Chinese scholars told the *South China Morning Post* that the move would make Beijing more willing to cooperate on climate and other issues.[444] Weeks later, the United States and China signed a new bilateral climate agreement.[445]

KEY OFFENSIVE POLICIES

Washington is right to seek leverage over Beijing, though the best and most appropriate sources of leverage will vary depending on the issue at hand. In general, the United States will have the strongest leverage when it can rally multiple major countries to its side. The Biden administration has therefore tried to build coalitions of allies and partners on such issues as China's human rights record, its cyber operations, and more. Granted, building and sustaining these international coalitions is a challenging task. Compared to the United States, most other countries—even close U.S. partners such as the Five Eyes, the European Union, Japan, and South Korea—tend to be more accommodative toward China. Biden can help set America's China-related global diplomacy on the right course, but these diplomatic challenges will likely outlast his administration.

SHAPING U.S. DOMESTIC NARRATIVES

China-related technology controls can be used to shape American public discourse and political narratives. There are both legitimate and dubious reasons for doing so.

First, U.S. leaders sometimes use announcements of new technology restrictions to raise domestic awareness about tech threats from China and thereby shock complacent private actors into more careful behavior. For context, the government does not directly control most of the U.S.-China technology relationship. On a day-to-day basis, American businesses and academic institutions choose when and where to cooperate with Chinese counterparts, weighing risks and benefits according to their own tolerances. When private stakeholders do not seem to fully appreciate the risks of technological cooperation with China, U.S. government restrictions can be a powerful messaging tool. Of course, the government should first try to communicate directly with these stakeholders and share appropriate evidence about specific threats.

Second, and more questionably, U.S. leaders sometimes institute China-related technology controls as part of domestic political gamesmanship. Anti-China measures are often popular. U.S. politicians may see them as opportunities to burnish national security and populist credentials, especially during election season. Even the most enlightened U.S. leaders will sometimes have mixed motives. From a policy perspective, this is worrisome. Parochial political concerns should never motivate something as serious as technological decoupling. The government should institute guardrails to minimize this behavior.

RECOMMENDED POLICIES AND PROCESSES

Executive branch agencies should adhere to regularized procedures for evaluating technology controls wherever possible. In many cases, regulatory agencies have long-standing internal processes and statutory constraints, such as the Administrative Procedure Act, overseen by the courts. In other cases, broad presidential powers (like IEEPA) can be wielded quite freely, including as a way to circumvent normal decisionmaking by agencies. These shortcuts should be reserved for exceptional situations, such as when the government must act immediately. And when the government creates new decisionmaking processes, such as the new ICTS supply chain security review regime, it should anticipate and account for potential abuse.

The development of China-related technology controls should adhere to regularized procedures and get special attention from federal oversight elements.

At the same time, oversight elements across the federal government should give special attention to China-related technology controls, given the high policy stakes and the substantial risk of politicization or mismanagement. Congressional committees of jurisdiction and inspectors general at key agencies—particularly the Departments of Commerce, Defense, Treasury, and State and the Intelligence Community—should identify technology controls as a top oversight priority. To rally the oversight community, the Government Accountability Office should add technology controls to its High Risk List of federal activities "with vulnerabilities to fraud, waste, abuse, and mismanagement, or in need of transformation."[446] The list already includes entries for "Ensuring the Effective Protection of Technologies Critical to U.S. National Security Interests" and "Ensuring the Cybersecurity of the Nation," but those categories do not capture the full scope of government activities and policy objectives at issue.

CASE STUDIES

Huawei and ZTE. The Trump administration's early actions against Huawei and ZTE helped to correct what had been relatively lax attitudes toward Chinese technology threats at leading U.S. universities. During Trump's first two years in office, U.S. officials struggled to persuade American universities to impose heightened scrutiny on technology collaboration with China. This changed in 2019, when Huawei was indicted on multiple federal charges and ZTE remained under several high-profile investigations. In response to these developments, prominent universities—including the Massachusetts Institute of Technology (MIT), Stanford, and the University of California, Berkeley—froze new collaboration with both Chinese companies.[447] MIT went further, instituting a "new review process for 'elevated-risk' international proposals" involving China (as well as Russia and

Saudi Arabia). These university actions were responsible, well-tailored, and long overdue. They might not have happened without government pressure.

TikTok. In contrast, Trump's actions against TikTok were badly tainted by the appearance of improper motives and methods. Trump sought to ban the app during a hard-fought presidential election campaign in which he sought to frame Joe Biden as weak on China. There is reasonable speculation that Trump's ban was prompted in part by personal conversations with Facebook CEO Mark Zuckerberg, whose platform not only competes with TikTok but also served as a critical component of Trump's electioneering infrastructure.[448] Trump then ordered TikTok's owners to sell the company to an American firm based on the recommendation of CFIUS.[449] Rejecting the bids seen by outside observers as most viable, he instead chose Oracle, whose leaders were political supporters.[450]

These red flags might have been dismissible if Trump's TikTok actions were otherwise well-grounded in a legitimate policymaking process. But the executive orders lacked meaningful detail, and their implementation had to be repeatedly delayed. A federal court later found the ban to be legally questionable and prevented it from coming into effect, before Biden eventually reversed it.[451]

KEY OFFENSIVE POLICIES

If U.S. leaders want to look strong on China, they should support some of the many nonrestrictive policies highlighted throughout this report, each of which would help protect U.S. national security, economic prosperity, and values in the face of serious challenges from Beijing. Meanwhile, U.S. officials should focus on sharing factual, responsible assessments of Chinese technology threats with American businesses, universities, and the public. Many private stakeholders are clear-eyed about these threats and want detailed, actionable information from the government.

At the same time, Washington must be careful not to exaggerate China tech threats. The overheated rhetoric of the Trump administration did much to damage the U.S. government's credibility on this issue and inflame public opinion. To reverse these trends, the Biden administration must be prepared to listen as much as talk—to hear directly from private stakeholders about what they see as the costs and benefits of U.S.-China technological decoupling and governmental technology controls.

CONCLUSION

U.S.-China technological decoupling is extraordinarily complex, yet American strategy and policy debates are too often simplistic and vague. This report has sought to clarify how decoupling in a host of different technology areas could affect the gamut of American interests. Even so, reality is orders of magnitude more intricate and dynamic than what can be presented here. Washington must account for the decisions of dozens of other countries involved in the global tech trade, and it must make sound policy choices while the U.S. political system continues to deteriorate—to name just two enormous challenges that deserve far more analysis.

Complexity and uncertainty are key reasons to pursue a centrist strategy that can hedge against multiple futures. By imposing focused, carefully designed technology restrictions, U.S. decisionmakers can conserve their most critical resources: time to assess the situation, and control over the decoupling process. This report has offered a concrete picture of what centrist decoupling might look like and how implementation could work at the agency level. It has also demonstrated several points that further bolster the case for a centrist approach to decoupling.

Focused, carefully designed technology restrictions can help U.S. decisionmakers conserve their most critical resources: time to assess the situation, and control over the decoupling process.

First, the most strategically significant technologies (like 5G telecommunications equipment and semiconductors) are few in number and already subject to strong U.S. government controls. A handful of technology areas

may need tighter China-oriented restrictions—for example, drone swarms, the U.S. bulk power system, and technologies sold to Xinjiang. Yet certain China-focused controls seem counterproductive in a number of other high-profile areas, such as geolocation data, social media platforms, and consumer devices like smartphones. While future circumstances may justify increased decoupling, U.S. technology controls should not be greatly expanded at this time.

Second, official U.S. policy goals remain dangerously vague and open-ended across the board. Washington must publicly clarify its vision for the global tech trade and set more achievable ambitions for countering techno-authoritarianism, maintaining a military edge over China, and preventing Chinese espionage, sabotage, and influence operations. These are all important U.S. interests, but none would currently justify broad-based technology controls. Even so, U.S. rhetoric and policy actions continue to suggest the possibility of a costly and quixotic expansion of China-oriented controls. Clearer, narrower public messaging by U.S. leaders would help to focus agencies on those problems they can realistically address with restrictive tools and reduce the motivation of China and others to seize control of the decoupling process.

Third, "offensive" (self-improvement) policies have the greatest long-term potential for strengthening American technology leadership, competitiveness, and resilience. Granted, many offensive policies face substantial hurdles to implementation. The United States has so far lacked the political will to accelerate transformation of its military forces, create national cybersecurity and data privacy standards, or begin to repair the domestic information ecosystem—just as the centrists fear. But failure to enact these and other needed reforms would mean wasting the extra time that "defensive" measures can provide, placing U.S. security and prosperity at risk. Perhaps the rise of a formidable state rival such as China can finally persuade American leaders to take on fundamental challenges at home.

Not everyone will endorse a centrist strategy for technological decoupling or the specific policies recommended here. Some may doubt whether a comprehensive strategy is possible or even useful. But all should agree that the United States needs sharper public debates on this critical set of challenges. If nothing else, U.S. officials and analysts should confront the hardest questions head-on. What kind of technological future does America hope to create? And how can the tools of government policy help to bring about such a world? U.S. national strength and well-being will depend, in large part, on how American leaders answer these questions in the years to come. They must act carefully. But first, they must think clearly.

NOTES

FOREWORD

1 From the National Security Commission on Artificial Intelligence homepage at https://www.nscai.gov/.

EXECUTIVE SUMMARY

2 "Technological decoupling" is a contested and sometimes politically charged phrase. In its strongest form, it can mean a total technological divorce between the United States and China—a very grave prospect currently favored only by a few radical voices. In its weaker form, it can refer more generally to the kind of marginal reduction of technological interdependence seen for the last several years. This report uses the latter meaning. Although "decoupling" can carry conflicting and at times misleading meanings, no other single term has yet managed to displace it in common usage.

This report is about the decoupling of "technology." It does not focus on the range of other sectors (such as medical supplies, finance, entertainment, agriculture, and real estate) where U.S. analysts or officials have also proposed some partial decoupling from China. That said, "technology" is an elusive concept. While policymakers often speak of a distinct "tech sector" (which they sometimes equate with "Silicon Valley"), the truth is that every commercial sector employs, adapts, and develops technologies. Hence, loose talk of "technological decoupling" can often be confusing or misleading. Policymakers need more precise analysis of specific technology-related U.S. interests and objectives, as this report seeks to provide.

Within the broad category of technology, this report focuses mainly on digitally oriented technologies, whose major value stems from software, data, communications, and networks. Examples include machine learning systems, social media platforms, and large data caches. These raise particularly acute policy dilemmas, such as how to distinguish between dual-use applications and how to manage globalized supply chains and information flows. The report also addresses mixed digital-physical technologies, where hardware innovation is a crucial source of value; these include semiconductors, drones, and telecommunications equipment. However, highly physically oriented technologies—like nuclear reactors, advanced materials, and hypersonics—are not an explicit focus.

Finally, this report is concerned both with finished technology (end products and services) and with technology inputs. The latter includes elements of what is called "the supply chain," such as technology components, raw materials, data, know-how, and human capital that flow between the United States and China. It also includes financial support. U.S. and Chinese actors have each made significant investments in the other country's tech companies, and U.S. and Chinese tech companies receive significant revenue from sales to the other country's home markets. These financial flows can be as important as the supply chain itself, or even more so, and have become a major policy battleground.

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.

CHOOSING A STRATEGY

187 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.

188 For a more sophisticated taxonomy that is not tech-specific, see Ganesh Sitaraman, "Mapping the China Debate," Lawfare, May 26, 2020, https://www.lawfareblog.com/mapping-china-debate. For a robust synthesis of decades of expert debates on geo-technological competition and controls, see 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/.

189 Matt Pottinger, "Beijing's American Hustle," *Foreign Affairs*, September/October 2021, https://www.foreignaffairs.com/articles/asia/2021-08-23/beijings-american-hustle; Derek Scissors, "Partial Decoupling From China: A Brief Guide," American Enterprise Institute, July 2020, https://www.aei.org/wp-content/uploads/2020/07/Partial-decoupling-from-China.pdf; and Tom Cotton, "Beat China: Targeted Decoupling and the Economic Long War," February 2021, https://www.cotton.senate.gov/imo/media/doc/210216_1700_China%20Report_FINAL.pdf.

190 Farhad Manjoo, "Dealing With China Isn't Worth the Moral Cost," *New York Times*, October 9, 2019, https://www.nytimes.com/2019/10/09/opinion/china-houston-rockets.html; and "A Human Rights Approach to US-China Policy," Human Rights Watch, February 17, 2021, https://www.hrw.org/news/2021/02/17/human-rights-approach-us-china-policy.

191 Ryan Browne, "Top US General Says Google 'Is Indirectly Benefiting the Chinese Military,'" CNN, March 14, 2019, https://www.cnn.com/2019/03/14/politics/dunford-china-google/index.html.

192 A magisterial version of this argument can be found in Rush Doshi, *The Long Game* (New York: Oxford University Press, 2021). That said, Doshi's discussion of technology does not necessarily fit within restrictionist canon. He ultimately calls for a fairly targeted set of U.S. government tech controls combined with robust offensive investment and international coordination. Meanwhile, Hal Brands and Michael Beckley have provided a contrasting set of predictions, arguing that China is a "peaking power" whose growing boldness on the world stage stems from a sense of impending decline. Hal Brands and Michael Beckley, "China Is a Declining Power—and That's the Problem," *Foreign Policy*, September 24, 2021, https://foreignpolicy.com/2021/09/24/china-great-power-united-states/.

193 Hal Brands, "Containment Can Work Against China, Too," *Wall Street Journal*, December 3, 2021, https://www.wsj.com/articles/containment-can-work-against-china-too-11638547169. Elsewhere, Brands and Michael Beckley have argued that Washington should "check China's technological expansion" by "restrict[ing] the export of technologies made in the United States and other democracies on which Chinese technology still depends" (including "semiconductors"), yet they cautioned against a "full technological embargo." Michael Beckley and Hal Brands, "Competition With China Could Be Short and Sharp," *Foreign Affairs*, December 17, 2020, https://www.foreignaffairs.com/articles/united-states/2020-12-17/competition-china-could-be-short-and-sharp.

194 Kiran Stacey and James Politi, "Google Warns of US National Security Risks From Huawei Ban," *Financial Times*, June 6 2019, https://www.ft.com/content/3bbb6fec-88c5-11e9-a028-86cea8523dc2; and John Neuffer, "Report Shows Risks of Excessive Restrictions on Trade With China," Semiconductor Industry Association, March 9, 2020, https://www.semiconductors.org/report-shows-risks-of-excessive-restrictions-on-trade-with-china/.

195 "Internet Society Statement on U.S. Clean Network Program," press release, Internet Society, August 7, 2020, https://www.internetsociety.org/news/statements/2020/internet-society-statement-on-u-s-clean-network-program/; and "An Open, Interconnected and Interoperable Internet (Joint Letter)," World Wide Web Foundation, September 14, 2021, https://webfoundation.org/2021/09/an-open-interconnected-and-interoperable-internet-joint-letter/.

196 Bernie Sanders, "Washington's Dangerous New Consensus on China," *Foreign Affairs*, June 17, 2021, https://www.foreignaffairs.com/articles/china/2021-06-17/washingtons-dangerous-new-consensus-china.

197 Daniel Flatley, "Bernie Sanders Proposes Forcing Chipmakers to Give U.S. Equity for Aid," *Bloomberg*, May 24, 2021, https://www.bloomberg.com/news/articles/2021-05-24/sanders-proposes-forcing-chipmakers-to-give-u-s-equity-for-aid?sref=QmOxnLFz.

198 "CAPAC Members and Attorney General Garland Discuss China Initiative, COVID-19 Hate Crimes Act, and Language Access," press release, Congressional Asian Pacific American Caucus, October 29, 2021, https://capac-chu.house.gov/press-release/capac-members-and-attorney-general-garland-discuss-china-initiative-covid-19-hate.

199 "Cooperation, Not Cold War, to Confront the Climate Crisis," open letter, Friends of the Earth, July 7, 2021, http://foe.org/wp-content/uploads/2021/07/Cooperation-Not-Cold-War-To-Confront-the-Climate-Crisis-129.pdf.

200 "Turnaround: New Multilateral Trade Rules for People-Centered Shared Prosperity and Sustainable Development," press release, Our World Is Not for Sale network, September 2021, https://ourworldisnotforsale.net/2021_WTO-Turnaround; and David Klion, "What Should the Left Do About China?," *The Nation*, January 11, 2022, https://www.thenation.com/article/world/china-left-foreign-policy/.

201 "Asymmetric Competition: A Strategy for China & Technology," China Strategy Group, Fall 2020, https://www.documentcloud.org/documents/20463382-final-memo-china-strategy-group-axios-1.

202 Stephanie Segal, "Degrees of Separation: A Targeted Approach to U.S.-China Decoupling – Final Report," Center for Strategic and International Studies, October 2021, https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/211021_Segal_DegreesSeparation_Final.pdf.

203 Richard Danzig and Lorand Laskai, "Symbiosis and Strive: Where Is the Sino-American Relationship Bound?," Johns Hopkins University Applied Physics Laboratory (JHU APL), 2020, https://www.jhuapl.edu/assessing-us-china-technology-connections/dist/00f3f3c246ab508f9fe11452bb18200c.pdf.

204 *Smart Competition: Adapting U.S. Strategy Toward China at 40 Years: A Hearing Before the House Foreign Affairs Committee*, 116th Cong. (2019) (testimony of Samm Sacks, May 8, 2019), https://www.congress.gov/116/meeting/house/109457/witnesses/HHRG-116-FA00-Wstate-SacksS-20190508.pdf.

205 Susan Shirk, "How to Shield Silicon Valley," *Bloomberg*, July 3, 2018, https://www.bloomberg.com/opinion/articles/2018-07-03/how-the-u-s-should-defend-its-high-tech-from-china?sref=QmOxnLFz.

206 Chris Coons, "Senator Coons Outlines Bipartisan Strategy for U.S.-China Relations at the Wilson Center," press release, October 18, 2019, https://www.coons.senate.gov/news/press-releases/senator-coons-outlines-bipartisan-strategy-for-us-china-relations-at-the-wilson-center.

207 Salman Ahmed et al., "Making U.S. Foreign Policy Work Better for the Middle Class," Carnegie Endowment for International Peace, September, 23, 2020, https://carnegieendowment.org/files/USFP_FinalReport_final1.pdf.

208 Dina Smeltz, Ivo Daalder, Karl Friedhoff, Craig Kafura, and Emily Sullivan, "A Foreign Policy for the Middle Class—What Americans Think," Chicago Council on Global Affairs, October 2021, https://www.thechicagocouncil.org/sites/default/files/2021-10/ccs2021_fpmc_0.pdf.

209 Andrew Imbrie, Ryan Fedasiuk, Catherine Aiken, Tarun Chhabra, and Husanjot Chahal, "Agile Alliances: How the United States and Its Allies Can Deliver a Democratic Way of AI," Center for Security and Emerging Technology, February 2020, https://cset.georgetown.edu/publication/agile-alliances/.

210 For more on the relationship between uncertainty and incrementalism, see Daniel W. Drezner, Ronald R. Krebs, and Randall Schweller, "The End of Grand Strategy," *Foreign Affairs*, May/June 2020, https://www.foreignaffairs.com/articles/world/2020-04-13/end-grand-strategy. Drezner, Krebs, and Schweller advocate decentralized, bottom-up decisionmaking, whereas this report proposes top-down strategic guidance.

211 Dan Strumpf, "U.S. Set Out to Hobble China's Huawei, and So It Has," *Wall Street Journal*, October 7, 2021, https://www.wsj.com/articles/u-s-set-out-to-hobble-chinas-huawei-and-so-it-has-11633617478.

212 Huawei's current placement on the Treasury Department's Non-SDN Chinese Military-Industrial Complex Companies List is an outgrowth of its earlier (now-lapsed) designation as a "Communist Chinese Military Company" by DOD. Huawei still remains on another, similar DOD list—the so-called Section 1260H List—but this does not yet have any clear legal consequences. "Biden Administration Revises and Expands Restrictions on U.S. Person Investment in Chinese Companies and Releases New

List of 'Chinese Military Companies' Under 2021 NDAA Section 1260H," Dorsey, June 10, 2021, https://www.dorsey.com/newsresources/publications/client-alerts/2021/06/new-list-of-chinese-military-companies.

213 "The Backlash to Huawei's Global 5G Expansion," Carnegie Endowment for International Peace, July 22, 2020, https://carnegieendowment.org/publications/interactive/huawei-timeline.

214 Stu Woo, "The U.S. Is Back in the 5G Game," *Wall Street Journal*, May 26, 2021, https://www.wsj.com/articles/us-5g-companies-11621870061.

215 Stu Woo and Drew Hinshaw, "U.S. Fight Against Chinese 5G Efforts Shifts From Threats to Incentives," *Wall Street Journal*, June 14, 2021, https://www.wsj.com/articles/u-s-fight-against-chinese-5g-efforts-shifts-from-threats-to-incentives-11623663252.

216 Ariel E. Levite and Lyu Jinghua, "Travails of an Interconnected World: From Pandemics to the Digital Economy," Lawfare, April 30, 2020, https://www.lawfareblog.com/travails-interconnected-world-pandemics-digital-economy.

217 "Court Imposes Maximum Fine on Sinovel Wind Group for Theft of Trade Secrets," press release, Justice Department, July 6, 2018, https://www.justice.gov/opa/pr/court-imposes-maximum-fine-sinovel-wind-group-theft-trade-secrets; and Diane Cardwell, "Solar Company Seeks Stiff U.S. Tariffs to Deter Chinese Spying," *New York Times*, September 1, 2014, https://www.nytimes.com/2014/09/02/business/trade-duties-urged-as-new-deterrent-against-cybertheft.html.

218 Jonathan Watts, "We Have 12 Years to Limit Climate Change Catastrophe, Warns UN," *Guardian*, October 8, 2018, https://www.theguardian.com/environment/2018/oct/08/global-warming-must-not-exceed-15c-warns-landmark-un-report.

219 Chris Buckley and Lisa Friedman, "Climate Change Is 'Not a Geostrategic Weapon,' Kerry Tells Chinese Leaders," September 1, 2021, https://www.nytimes.com/2021/09/02/world/asia/climate-china-us-kerry.html.

220 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.

221 Ellen Nakashima, "More Than 1,000 Visiting Researchers Affiliated With the Chinese Military Fled the United States This Summer, Justice Department Says," *Washington Post*, December 2, 2020, https://www.washingtonpost.com/national-security/more-than-1000-visiting-researchers-affiliated-with-the-chinese-military-fled-the-united-states-this-summer-justice-department-says/2020/12/02/9c564dee-34e1-11eb-b59c-adb7153d10c2_story.html.

222 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.

223 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/.

224 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/?sh=4f73456c3641.

225 For a side-by-side comparison of U.S. and Chinese government actions, see Yan Luo, Samm Sacks, Naomi Wilson, and Abigail Coplin, "Mapping U.S.–China Technology Decoupling," DigiChina, August 27, 2020, https://fsi-live.s3.us-west-1.amazonaws.com/s3fs-public/digichina-mapping-decoupling-final1.pdf.

226 B. Chen Zhu, Paul D. McKenzie, and Cheryl Zhu, "China's 'Unreliable Entity List' Creates New Countervailing Risks for Companies Navigating U.S. Sanctions and Long-Arm Enforcement," Morrison Foerster, October 7, 2020, https://www.mofo.com/resources/insights/201007-china-mofcom-unreliable-entity-list.html.

227 Jane Li, "The Return of Huawei CFO Meng Wanzhou Has Become a Nationalist Moment for China," Quartz, September 27, 2021, https://qz.com/2065090/the-return-of-huawei-cfo-becomes-a-nationalist-moment-for-china/.

228 "China Investigates Didi Over Cybersecurity Days After Its Huge IPO," Reuters, July 2, 2021, https://www.reuters.com/technology/china-cyberspace-administration-launches-security-investigation-into-didi-2021-07-02/.

229 Senator John Kennedy, "Kennedy, Sullivan Call on SEC to Enforce Transparency Laws for Chinese Companies Following Didi IPO Debacle," July 29, 2021, https://www.kennedy.senate.gov/public/2021/7/kennedy-sullivan-call-on-sec-to-enforce-transparency-laws-for-chinese-companies-following-didi-ipo-debacle.

230 "Trade War: How Reliant Are US Colleges on Chinese Students?," BBC, June 12, 2019, https://www.bbc.com/news/world-asia-48542913.

231 Mary Hui, "Japan's Global Rare Earths Quest Holds Lessons for the US and Europe," Quartz, December 28, 2021, https://qz.com/1998773/japans-rare-earths-strategy-has-lessons-for-us-europe/.

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

233 Samantha Subin, "Palantir CEO Says Companies Working With U.S. Adversaries Should Justify Their Position," CNBC, November 23 2021, https://www.cnbc.com/2021/11/23/palantir-ceo-companies-working-with-us-adversaries-should-justify-their-position-.html.

TRANSLATING STRATEGY INTO POLICY AND PROCESS

234 Although the analysis and recommendations in this section are grounded in the centrist strategy outlined earlier, the analytical structure and methodology used can be readily adopted by restrictionists or cooperationists to frame their own arguments.

MAINTAINING A MILITARY EDGE OVER CHINA

235 "China Military Power: Modernizing a Force to Fight and Win," Defense Intelligence Agency, 2019, https://www.dia.mil/Portals/110/Images/News/Military_Powers_Publications/China_Military_Power_FINAL_5MB_20190103.pdf.

236 *Department of Defense Budget Posture: A Hearing Before the Senate Armed Services Committee*, 115th Cong. (2017) (testimony of General Joseph F. Dunford, Jr., Chairman of the Joint Chiefs of Staff, June 13, 2017), https://www.armed-services.senate.gov/imo/media/doc/Dunford_06-13-17.pdf.

237 Michael Dahm, "Chinese Debates on the Military Utility of Artificial Intelligence," War on the Rocks, June 4, 2020, https://warontherocks.com/2020/06/chinese-debates-on-the-military-utility-of-artificial-intelligence/.

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

239 In a 2021 report to Congress, DOD stated, "The PRC Uses Imports, Foreign Investments, Commercial Joint Ventures, Mergers and Acquisitions, and Industrial and Technical Espionage to Help Achieve Its Military Modernization Goals." "Military and Security Developments Involving the People's Republic of China: 2021," Department of Defense, November 3, 2021, https://media.defense.gov/2021/Nov/03/2002885874/-1/-1/0/2021-CMPR-FINAL.PDF.

240 Robert D. Blackwill and Philip Zelikow, "The United States, China, and Taiwan: A Strategy to Prevent War," Council on Foreign Relations, Special report no. 90, February 2021, https://cdn.cfr.org/sites/default/files/report_pdf/csr90_1.pdf; Elbridge Colby and Walter Slocombe, "The State of (Deterrence by) Denial," War on the Rocks, March 22, 2021, https://warontherocks.com/2021/03/the-state-of-deterrence-by-denial/; and Tanner Greer, "Why I Fear for Taiwan," Scholar's Stage, September 11, 2020, https://scholars-stage.org/why-i-fear-for-taiwan/.

241 The research also found that "U.S. companies are inadvertently powering Chinese military advances in AI" due to "loopholes and shortfalls in the export control system." However, this problem is challenging to address and not cost-free, as discussed elsewhere. Ryan Fedasiuk, "We Spent a Year Investigating What the Chinese Army Is Buying. Here's What We Learned," *Politico*, November 10, 2021, https://www.politico.com/news/magazine/2021/11/10/chinese-army-ai-defense-contracts-520445.

242 "Final Report," National Security Commission on Artificial Intelligence, March 2021, https://www.nscai.gov/wp-content/uploads/2021/03/Full-Report-Digital-1.pdf.

243 "Military and Security Developments Involving the People's Republic of China: 2021," Department of Defense, November 3, 2021, https://media.defense.gov/2021/Nov/03/2002885874/-1/-1/0/2021-CMPR-FINAL.PDF.

244 Alex Stone and Peter W. Singer, "How China Is Planning for a Tech Decoupling," Defense One, October 12, 2021, https://www.defenseone.com/ideas/2021/10/how-china-planning-tech-decoupling/186029/.

245 Daniel H. Nexon, "Against Great Power Competition," *Foreign Affairs*, February 15, 2021, https://www.foreignaffairs.com/articles/united-states/2021-02-15/against-great-power-competition; and Cornell Overfield, "Biden's 'Strategic Competition' Is a Step Back," *Foreign Policy*, October 13, 2021, https://foreignpolicy.com/2021/10/13/biden-strategic-competition-national-defense-strategy/.

246 Gordon Long, "Fundamental Research Security," JASON, December 6, 2019, https://www.nsf.gov/news/special_reports/jasonsecurity/JSR-19-2IFundamentalResearchSecurity_12062019FINAL.pdf.

247 Ryan Browne, "Top US General Says Google 'Is Indirectly Benefiting the Chinese Military,'" CNN, March 14, 2019, https://www.cnn.com/2019/03/14/politics/dunford-china-google/index.html; and B. Chen Zhu, Brandon L. Van Grack, Timothy W. Blakely, and Charles L. Capito, "U.S. Court Blocks Trump-Era Designation of Xiaomi as a Chinese Military Company and Permits Continued Trading in Its Securities," Morrison Foerster, March 19, 2021, https://www.mofo.com/resources/insights/210319-us-court-blocks-trump-era-designation.html.

248 Fenella McGerty and Meia Nouwens, "China's New Five-Year Plan and 2021 Budget: What Do They Mean For Defence?," International Institute for Strategic Studies, March 8, 2021, https://www.iiss.org/blogs/analysis/2021/03/chinas-new-five-year-plan-and-2021-budget; and David Arthur and F. Matthew Woodward, "Long-Term Implications of the 2021 Future Years Defense Program," Congressional Budget Office, September 2020, https://www.cbo.gov/publication/56554.

249 This particular study was published in 2015, but in the intervening years, the key factors undergirding its conclusion have not reversed. Eric Heginbotham et al., "The U.S.-China Military Scorecard: Forces, Geography, and the Evolving Balance of Power, 1996-2017," RAND Corporation, 2015, https://www.rand.org/pubs/research_reports/RR392.html.

250 For example, the Lowy Institute's most recent Asia Power Index found that China is investing and gaining more in its international economic ties than in its defense capabilities and relationships. Hervé Lemahieu and Alyssa Leng, "Asia Power Index: Key Findings 2021," Lowy Institute, 2021, https://power.lowyinstitute.org/downloads/lowy-institute-2021-asia-power-index-key-findings-report.pdf.

251 This example is hypothetical.

252 Christian Brose, "The New Revolution in Military Affairs: War's Sci-Fi Future," *Foreign Affairs*, May/June 2019, https://www.foreignaffairs.com/articles/2019-04-16/new-revolution-military-affairs.

253 David Benowitz, "DJI Added to the US Entity List – What's the Impact?," DroneAnalyst, December 21, 2020, https://droneanalyst.com/2020/12/21/dji-added-to-the-us-entity-list-whats-the-impact.

254 B. Chen Zhu, Brandon L. Van Grack, Timothy W. Blakely, and Charles L. Capito, "U.S. Court Blocks Trump-Era Designation of Xiaomi as a Chinese Military Company and Permits Continued Trading in Its Securities," Morrison Foerster, March 19, 2021, https://www.mofo.com/resources/insights/210319-us-court-blocks-trump-era-designation.html.

255 "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.

256 "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.

257 Select Committee of the U.S. House of Representatives on U.S. National Security and Military/Commercial Concerns with the People's Republic of China, "U.S. Export Policy Toward the PRC, vol. III, ch. 9." May 25, 1999, https://www.govinfo.gov/content/pkg/GPO-CRPT-105hrpt851/pdf/GPO-CRPT-105hrpt851-3-5.pdf; and Ellen Nakashima and Gerry Shih, "China Builds Advanced Weapons Systems Using American Chip Technology," *Washington Post*, April 9, 2021, https://www.washingtonpost.com/national-security/china-hypersonic-missiles-american-technology/2021/04/07/37a6b9be-96fd-11eb-b28d-bfa7bb5cb2a5_story.html.

258 "Supercomputer Export Controls Strengthened," Arms Control Association, https://www.armscontrol.org/node/3147.

259 Ellen Nakashima and Gerry Shih, "China Builds Advanced Weapons Systems Using American Chip Technology," *Washington Post*, April 9, 2021, https://www.washingtonpost.com/national-security/china-hypersonic-missiles-american-technology/2021/04/07/37a6b9be-96fd-11eb-b28d-bfa7bb5cb2a5_story.html.

260 "Addition of Certain Persons to the Entity List; and Removal of Person From the Entity List Based on a Removal Request," Commerce Department, 80 Fed. Reg. 8,524 (February 18, 2015), https://www.federalregister.gov/documents/2015/02/18/2015-03321/addition-of-certain-persons-to-the-entity-list-and-removal-of-person-from-the-entity-list-based-on-a.

261 Ana Swanson, Paul Mozur, and Steve Lohr, "U.S. Blacklists More Chinese Tech Companies Over National Security Concerns," *New York Times*, June 21, 2019, https://www.nytimes.com/2019/06/21/us/politics/us-china-trade-blacklist.html; and Kate O'Keeffe and Asa Fitch, "U.S. Targets China's Supercomputing Push With New Export Restrictions," *Wall Street Journal*, June 21, 2019, https://www.wsj.com/articles/u-s-targets-chinas-supercomputing-push-with-new-export-restrictions-11561129547.

262 "Commerce Adds Seven Chinese Supercomputing Entities to Entity List for Their Support to China's Military Modernization, and Other Destabilizing Efforts," press release, Commerce Department, April 8, 2021, https://www.commerce.gov/news/press-releases/2021/04/commerce-adds-seven-chinese-supercomputing-entities-entity-list-their.

263 Jane Zhang and Che Pan, "China's Blacklisted Supercomputer Organisations: Who Are They and What Do They Do?," *South China Morning Post*, April 9, 2021 https://www.scmp.com/tech/tech-war/article/3128963/chinas-blacklisted-supercomputer-organisations-who-are-they-and-what; and Ana Swanson, Paul Mozur, and Steve Lohr, "U.S. Blacklists More Chinese Tech Companies Over National Security Concerns," *New York Times*, June 21, 2019, https://www.nytimes.com/2019/06/21/us/politics/us-china-trade-blacklist.html.

264 Jeff Gerth, "U.S. Raises Trade Issue With China," *New York Times*, July 2, 1997, https://www.nytimes.com/1997/07/02/world/us-raises-trade-issue-with-china.html; and Tom Mullaney, "The Origins of Chinese Supercomputing," *Foreign Affairs*, August 4, 2016, https://www.foreignaffairs.com/articles/china/2016-08-04/origins-chinese-supercomputing.

265 Mark Cancian and Adam Saxton, "What's in a Name? Billions in Cuts Depend on Defining 'Legacy,'" Breaking Defense, March 10, 2021, https://breakingdefense.com/2021/03/whats-in-a-name-billions-in-cuts-depend-on-defining-legacy/; Jack Detsch, "'No Decisions, No Changes': Pentagon Fails to Stick Asia Pivot," *Foreign Policy*, November 29, 2021, https://foreignpolicy.com/2021/11/29/pentagon-china-biden-asia-pivot/; and Joe Gould, "Tech Startups Still Face the Pentagon's 'Valley of Death,'" *Defense News*, January 30, 2020, https://www.defensenews.com/2020/01/30/tech-startups-still-face-the-pentagons-valley-of-death/.

266 Daniel Gonzales et al., "Unclassified and Secure: A Defense Industrial Base Cyber Protection Program for Unclassified Defense Networks," RAND Corporation, 2020, https://www.rand.org/pubs/research_reports/RR4227.html.

LIMITING CHINESE NATIONAL SECURITY ESPIONAGE

267 "The China Threat," Federal Bureau of Investigation, https://www.fbi.gov/investigate/counterintelligence/the-china-threat.

268 Christopher Wray, "The Threat Posed by the Chinese Government and the Chinese Communist Party to the Economic and National Security of the United States" (video lecture, Hudson Institute, Washington, DC, July 7, 2020), https://www.fbi.gov/news/speeches/the-threat-posed-by-the-chinese-government-and-the-chinese-communist-party-to-the-economic-and-national-security-of-the-united-states.

269 "Chinese National Who Conspired to Hack Into U.S. Defense Contractors' Systems Sentenced to 46 Months in Federal Prison," Justice Department, July 13, 2016, https://www.justice.gov/opa/pr/chinese-national-who-conspired-hack-us-defense-contractors-systems-sentenced-46-months.

270 "Russia, China and Iran Hackers Target Trump and Biden, Microsoft Says," BBC, September 11, 2020, https://www.bbc.com/news/world-us-canada-54110457.

271 Mark Mazzetti, Adam Goldman, Michael S. Schmidt and Matt Apuzzo, "Killing C.I.A. Informants, China Crippled U.S. Spying Operations," *New York Times*, May 20, 2017, https://www.nytimes.com/2017/05/20/world/asia/china-cia-spies-espionage.html.

272 Zach Dorfman, "China Used Stolen Data to Expose CIA Operatives in Africa and Europe," *Foreign Policy*, December 21, 2020, https://foreignpolicy.com/2020/12/21/china-stolen-us-data-exposed-cia-operatives-spy-networks/.

273 "China's Collection of Genomic and Other Healthcare Data From America: Risks to Privacy and U.S. Economic and National Security," National Counterintelligence and Security Center, February 2020, https://www.dni.gov/files/NCSC/documents/SafeguardingOurFuture/NCSC_China_Genomics_Fact_Sheet_2021revision20210203.pdf.

274 Zach Dorfman, "Tech Giants Are Giving China a Vital Edge in Espionage," *Foreign Policy*, December 23, 2020, https://foreignpolicy.com/2020/12/23/china-tech-giants-process-stolen-data-spy-agencies/.

275 Bojan Pancevski, "U.S. Officials Say Huawei Can Covertly Access Telecom Networks," *Wall Street Journal*, February 12, 2020, https://www.wsj.com/articles/u-s-officials-say-huawei-can-covertly-access-telecom-networks-11581452256; and Gordon Corera, "Eric Schmidt: Huawei Has Engaged in Unacceptable Practices," BBC, June 18, 2020, https://www.bbc.com/news/technology-53080113.

276 Christopher Wray, "The Threat Posed by the Chinese Government and the Chinese Communist Party to the Economic and National Security of the United States" (video lecture, Hudson Institute, Washington, DC, July 7, 2020), https://www.fbi.gov/news/speeches/the-threat-posed-by-the-chinese-government-and-the-chinese-communist-party-to-the-economic-and-national-security-of-the-united-states.

277 Stuart A. Thompson and Charlie Warzel, "Twelve Million Phones, One Dataset, Zero Privacy," *New York Times*, December 19, 2019, https://www.nytimes.com/interactive/2019/12/19/opinion/location-tracking-cell-phone.html; and Molly Olmstead, "A Prominent Priest Was Outed for Using Grindr. Experts Say It's a Warning Sign," Slate, July 21, 2021, https://slate.com/technology/2021/07/catholic-priest-grindr-data-privacy.html.

278 Joseph Cox, "How the U.S. Military Buys Location Data From Ordinary Apps," *Motherboard*, November 16, 2020, https://www.vice.com/en/article/jgqm5x/us-military-location-data-xmode-locate-x; and Justin Sherman, "Data Brokers Are Advertising Data on U.S. Military Personnel," Lawfare, August 23, 2021, https://www.lawfareblog.com/data-brokers-are-advertising-data-us-military-personnel.

279 Edward Wong, "How China Uses LinkedIn to Recruit Spies Abroad," *New York Times*, October 14, 2021, https://www.nytimes.com/2019/08/27/world/asia/china-linkedin-spies.html.

280 Karen Weise and Paul Mozur, "LinkedIn to Shut Down Service in China, Citing 'Challenging' Environment," *New York Times*, October 14, 2021, https://www.nytimes.com/2021/10/14/technology/linkedin-china-microsoft.html.

281 Ben Kesling and Georgia Wells, "U.S. Military Bans TikTok Over Ties to China," January 3, 2020, *Wall Street Journal*, https://www.wsj.com/articles/u-s-military-bans-tiktok-over-ties-to-china-11578090613.

282 Jenna McLaughlin and Zach Dorfman, "'Shattered': Inside the Secret Battle to Save America's Undercover Spies in the Digital Age," Yahoo News, December 30, 2019, https://www.yahoo.com/entertainment/shattered-inside-the-secret-battle-to-save-americas-undercover-spies-in-the-digital-age-100029026.html.

283 More appropriate protections would include national data security and privacy standards, plus regulations, trainings, and counterintelligence programs specifically focused on the online activities of U.S. military members.

284 Martin Egnash, "Defense Travel System Data Breach Leaves Thousands Open to Identity Theft," *Stars and Stripes*, March 1, 2018, https://www.stripes.com/defense-travel-system-data-breach-leaves-thousands-open-to-identity-theft-1.514499.

285 "Provisions Pertaining to Certain Investments in the United States by Foreign Persons," Treasury Department, 85 Fed. Reg. 3,112 (January 17, 2020), https://www.federalregister.gov/documents/2020/01/17/2020-00188/provisions-pertaining-to-certain-investments-in-the-united-states-by-foreign-persons.

286 David J. Lynch, "Biotechnology: The US-China Dispute Over Genetic Data," *Financial Times*, July 31, 2017, https://www.ft.com/content/245a7c60-6880-11e7-9a66-93fb352ba1fe.

287 CFIUS also seems to be scrutinizing transactions involving much smaller pools of genetic data than its regulations would suggest. In October 2020, it reportedly prevented a Chinese entity from buying a San Diego fertility clinic. Eamon Javers, "U.S. Blocked Chinese Purchase of San Diego Fertility Clinic Over Medical Data Security Concerns," CNBC, October 16, 2020, https://www.cnbc.com/2020/10/16/trump-administration-blocked-chinese-purchase-of-us-fertility-clinic.html.

288 Echo Wang, "China's Kunlun Tech Agrees to U.S. Demand to Sell Grindr Gay Dating App," Reuters, May 13, 2019, https://www.reuters.com/article/us-grindr-m-a-beijingkunlun/chinas-kunlun-tech-agrees-to-u-s-demand-to-sell-grindr-gay-dating-app-idUSKCN1SJ28N.

289 Kamran Kara-Pabani and Justin Sherman, "How a Norwegian Government Report Shows the Limits of CFIUS Data Reviews," Lawfare, May 3, 2021, https://www.lawfareblog.com/how-norwegian-government-report-shows-limits-cfius-data-reviews.

290 "President Trump Orders Divestiture of StayNTouch, Inc. by Shiji Group of China," Covington, March 9, 2020, https://www.cov.com/en/news-and-insights/insights/2020/03/president-trump-orders-divestiture-of-stayntouch-inc-by-shiji-group-of-china.

291 Jena Tesse Fox, "Hotel Owner-Operator to Acquire PMS Company StayNTouch," Hotel Management, August 31, 2020, https://www.hotelmanagement.net/tech/mcr-to-acquire-pms-software-company-stayntouch.

292 Marriott International, Inc., "Form 10-K for the Fiscal Year Ended December 31, 2020," Securities and Exchange Commission, https://www.sec.gov/ix?doc=/Archives/edgar/data/0001048286/000162828021002433/mar-20201231.htm.

293 "Marriott Announces Starwood Guest Reservation Database Security Incident," press release, Marriott, November 20, 2018, https://marriott.gcs-web.com/news-releases/news-release-details/marriott-announces-starwood-guest-reservation-database-security.

294 Emphasis added. "Secretary Michael R. Pompeo at a Press Availability," State Department, July 8, 2020, https://2017-2021-translations.state.gov/2020/07/08/secretary-michael-r-pompeo-at-a-press-availability-8/index.html.

295 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; Maria Abi-Habib, "India Bans Nearly 60 Chinese Apps, Including TikTok and WeChat," *New York Times*, June 30, 2020, https://www.nytimes.com/2020/06/29/world/asia/tik-tok-banned-india-china.html; and Sameer Yasir and Hari Kumar, "India Bans 118 Chinese Apps as Indian Soldier Is Killed on Disputed Border," *New York Times*, September 2, 2020, https://www.nytimes.com/2020/09/02/world/asia/india-bans-china-apps.html.

296 Emphasis added. *Beijing's Long Arm: Threats to U.S. National Security: A Hearing Before the Senate Select Committee on Intelligence*, 117th Cong. (2021) (testimony of William R. Evanina, August 4, 2021), https://www.intelligence.senate.gov/sites/default/files/documents/os-bevanina-080421.pdf; and Dina Temple-Raston, "China's Microsoft Hack May Have Had a Bigger Purpose Than Just Spying," NPR, August 26, 2021, https://www.npr.org/2021/08/26/1013501080/chinas-microsoft-hack-may-have-had-a-bigger-purpose-than-just-spying.

297 Greg Roumeliotis and Echo Wang, "Exclusive China's Tencent in Talks With U.S. to Keep Gaming Investments -Sources," Reuters, May 5, 2021, https://www.reuters.com/technology/exclusive-chinas-tencent-talks-with-us-keep-gaming-investments-sources-2021-05-05/.

298 Jenny Leonard, Saleha Mohsin, and David McLaughlin, "Tencent's Gaming Stakes Draw U.S. National Security Scrutiny," *Bloomberg*, September 17, 2020, https://www.bloomberg.com/news/articles/2020-09-17/tencent-s-game-investments-draw-u-s-national-security-scrutiny.

299 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.

300 Joseph Marks, "The Cybersecurity 202: Our Expert Network Says It's Time for More Cybersecurity Regulations," *Washington Post*, June 11, 2021, https://www.washingtonpost.com/politics/2021/06/11/cybersecurity-202-our-expert-network-says-it-time-more-cybersecurity-regulations/; and Robert D. Williams, "To Enhance Data Security, Federal Privacy Legislation Is Just a Start," Brookings Institution, December 1, 2020, https://www.brookings.edu/techstream/to-enhance-data-security-federal-privacy-legislation-is-just-a-start/.

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

302 Emily O. Goldman and Michael Warner, "Why a Digital Pearl Harbor Makes Sense . . . and Is Possible," Carnegie Endowment for International Peace, October 16, 2017, https://carnegieendowment.org/2017/10/16/why-digital-pearl-harbor-makes-sense-.-.-.-and-is-possible-pub-73405.

303 Britain quickly abandoned this strategy due to its large costs. But that does not mean that China would never consider its own similar strategy in a future Sino-U.S. crisis. If Beijing implemented such a strategy, it might once again turn out to be a mistake. But an initial blow against the United States could nevertheless be powerful, justifying U.S. efforts to prevent and mitigate such a scenario. Nicholas Lambert, "Brits-Krieg: The Strategy of Economic Warfare," Carnegie Endowment for International Peace, October 16, 2017, https://carnegieendowment.org/2017/10/16/brits-krieg-strategy-of-economic-warfare-pub-73403.

304 "Annual Threat Assessment of the US Intelligence Community," Director of National Intelligence, April 9, 2021, https://www.dni.gov/files/ODNI/documents/assessments/ATA-2021-Unclassified-Report.pdf.

305 Peter Harrell, Elizabeth Rosenberg, and Edoardo Saravalle, "China's Use of Coercive Economic Measures," Center for a New American Security, June 2018, https://s3.us-east-1.amazonaws.com/files.cnas.org/documents/China_Use_FINAL-1.pdf; and Evan A. Feigenbaum, "Is Coercion the New Normal in China's Economic Statecraft?," Macro Polo, July 25, 2017, https://carnegieendowment.org/2017/07/25/is-coercion-new-normal-in-china-s-economic-statecraft-pub-72632.

306 For example, the Lowy Institute's most recent Asia Power Index identified "a short-term reprieve from an established pattern of relative US decline" compared to China. Hervé Lemahieu and Alyssa Leng, "Asia Power Index: Key Findings 2021," Lowy Institute, 2021, https://power.lowyinstitute.org/downloads/lowy-institute-2021-asia-power-index-key-findings-report.pdf. See also James Dobbins, Gabrielle Tarini, and Ali Wyne, "The Lost Generation in American Foreign Policy," RAND Corporation, 2020, https://www.rand.org/pubs/perspectives/PEA232-1.html.

307 The Biden administration's 100-day review of the U.S. supply chain makes this point elegantly. Though not focused on critical infrastructure per se, it outlines a range of domestic and international risks to U.S. resilience in key sectors, and wisely treats hostile subversion from China as just one of many challenges. "Building Resilient Supply Chains, Revitalizing American Manufacturing, and Fostering Broad-Based Growth," White House, June 2020, https://www.whitehouse.gov/wp-content/uploads/2021/06/100-day-supply-chain-review-report.pdf.

308 Ken Dilanian and Kelly O'Donnell, "Russian Criminal Group Suspected in Colonial Pipeline Ransomware Attack," NBC News, May 10, 2021, https://www.nbcnews.com/politics/national-security/russian-criminal-group-may-be-responsible-colonial-pipeline-ransomware-attack-n1266793.

309 Adi Robertson, "AT&T Recovers From Multi-state Outage After Nashville Bombing," The Verge, December 28, 2020, https://www.theverge.com/2020/12/28/22202822/att-outage-nashville-christmas-bombing.

310 "Hack Attack Causes 'Massive Damage' at Steel Works," BBC, December 22, 2014, https://www.bbc.com/news/technology-30575104.

311 Nick Thieme, "After Hurricane Maria, Puerto Rico's Internet Problems Go From Bad to Worse," PBS, October 23, 2018, https://www.pbs.org/wgbh/nova/article/puerto-rico-hurricane-maria-internet/.

312 William Yuen Ye, "With U.S. Restrictions on Huawei and ZTE, Where Will Rural America Turn?," Center for Strategic and International Studies, December 10, 2020, https://www.csis.org/blogs/new-perspectives-asia/us-restrictions-huawei-and-zte-where-will-rural-america-turn.

313 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/.

314 William Yuen Ye, "With U.S. Restrictions on Huawei and ZTE, Where Will Rural America Turn?," Center for Strategic and International Studies, December 10, 2020, https://www.csis.org/blogs/new-perspectives-asia/us-restrictions-huawei-and-zte-where-will-rural-america-turn.

315 Joint Chiefs of Staff, "Joint Publication 5-0: Joint Planning," December 1, 2020, https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp5_0.pdf.

316 "National Critical Functions Set," Cybersecurity and Infrastructure Security Agency (CISA), April 2019, https://www.cisa.gov/national-critical-functions-set.

317 "Systemic Cyber Risk Reduction Venture," CISA, https://www.cisa.gov/systemic-cyber-risk-reduction.

318 "2019 National Threat and Hazard Identification and Risk Assessment (THIRA): Overview and Methodology," Federal Emergency Management Agency, July 25, 2019, https://www.fema.gov/sites/default/files/2020-06/fema_national-thira-overview-methodology_2019_0.pdf; and "Homeland Security Planning Scenarios and Summary Descriptions," Brookings Institution, https://www.brookings.edu/wp-content/uploads/2016/06/20051026_3-1.pdf.

319 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.

320 "Large Power Transformers and the U.S. Electric Grid," Department of Energy, June 2021, https://www.energy.gov/sites/prod/files/Large%20Power%20Transformer%20Study%20-%20June%202012_0.pdf.

321 Black Sobczak and Peter Behr, "Security – China and America's 400-Ton Electric Albatross," E&E News, April 25, 2019, https://www.eenews.net/stories/1060216451/.

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

323 "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.

324 "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.

325 "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.

326 Brandon L. Van Grack, Charles L. Capito, and Joseph A. Benkert, "Biden Administration Carries Forward Trump Era Executive Order Scrutinizing Imports and Sales of Certain Communications Technology and Services," Morrison Foerster, April 1, 2021, https://www.mofo.com/resources/insights/210401-trump-executive-order.html.

327 As discussed earlier, Biden 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. The Commerce Department subsequently proposed to incorporate this guidance into the ICTS rule, and invited comment on whether Biden's criteria should also govern reviews of other kinds of software and hardware. 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; and "Securing the Information and Communications Technology and Services Supply Chain; Connected Software Applications," Commerce Department, 86 Fed. Reg. 67,379 (November 26, 2021), https://www.federalregister.gov/documents/2021/11/26/2021-25329/securing-the-information-and-communications-technology-and-services-supply-chain-connected-software.

328 Francesca M.S. Guerrero and Jennifer L. Parry, "Veritas, a U.S. Genetic Sequencing Company, Suspends U.S. Operations Due to Decreased Funding; CFIUS Thought to Be Leading Cause," Winston & Strawn, December 23, 2019, https://www.winston.com/en/global-trade-and-foreign-policy-insights/veritas-a-us-genetic-sequencing-company-suspends-us-operations-due-to-decreased-funding-cfius-thought-to-be-leading-cause.html.

329 Bill Gertz, "Lexmark, Lenovo Tech Funnels Data to China Intelligence Services," *Washington Times*, February 24, 2020, https://www.washingtontimes.com/news/2020/feb/24/lexmark-lenovo-tech-funnels-data-china-intelligenc/; Roslyn Layton, "Why Is U.S. Policy Tough on Huawei and TikTok but Not Lenovo?," *Forbes*, June 26, 2020, https://www.forbes.com/sites/roslynlayton/2020/06/26/why-is-us-policy-tough-on-huawei-and-tiktok-but-not-lenovo/?sh=3cdcb5cc7b6e; James Marks, "The Chinese Threat That's Hiding in Plain Sight," The Bulwark, September 12, 2019, https://thebulwark.com/the-chinese-threat-thats-hiding-in-plain-sight/; Roslyn Layton, "Stealing From the States: China's Power Play in IT Contracts," China Tech Threat, March 2020, https://chinatechthreat.com/wp-content/uploads/2020/02/CTT-Report-Stealing-From-States-Chinas-Power-Play-in-IT-Contracts.pdf; Ryan McMorrow and Kathrin Hille, "Lenovo's Sales Strong Despite Growing Threat of US Sanctions," *Financial Times*, August 13, 2020, https://www.ft.com/content/a5f5f290-04c9-4776-ae8d-ee881b13bb3a.

330 Robert K. Knake, "A Cyberattack on the U.S. Power Grid," Council on Foreign Relations, April 3, 2017, https://www.cfr.org/report/cyberattack-us-power-grid.

331 "Strategic Transformer Reserve," Department of Energy, March 2017, https://www.energy.gov/sites/prod/files/2017/04/f34/Strategic%20Transformer%20Reserve%20Report%20-%20FINAL.pdf.

332 Robert K. Knake, "A Cyberattack on the U.S. Power Grid," Council on Foreign Relations, April 3, 2017, https://www.cfr.org/report/cyberattack-us-power-grid; and "Strategic Transformer Reserve," Department of Energy, March 2017, https://www.energy.gov/sites/prod/files/2017/04/f34/Strategic%20Transformer%20Reserve%20Report%20-%20FINAL.pdf.

LIMITING CHINESE INFLUENCE OPERATIONS

333 Christopher Wray, "The Threat Posed by the Chinese Government and the Chinese Communist Party to the Economic and National Security of the United States" (video lecture, Hudson Institute, Washington, DC, July 7, 2020), https://www.fbi.gov/news/speeches/the-threat-posed-by-the-chinese-government-and-the-chinese-communist-party-to-the-economic-and-national-security-of-the-united-states.

334 Bethany Allen-Ebrahimian and Zach Dorfman, "Suspected Chinese Spy Targeted California Politicians," Axios, December 8, 2020, https://www.axios.com/china-spy-california-politicians-9d2dfb99-f839-4e00-8bd8-59dec0daf589.html; Bethany Allen-Ebrahimian and Zach Dorfman, "Republican Donor Cindy Yang Linked to Chinese Influence Machine," *Foreign Policy*, March 12, 2019, https://foreignpolicy.com/2019/03/12/962067-china-unitedfront-corruption-scandal/; and Bethany Allen-Ebrahimian, "China Built an Army of Influence Agents in the U.S.," Daily Beast, July 18, 2018, https://www.thedailybeast.com/how-china-built-an-army-of-influence-agents-in-the-us.

335 Joshua Kurlantzick, "How China Is Interfering in Taiwan's Election," Council on Foreign Relations, November 7, 2019, https://www.cfr.org/in-brief/how-china-interfering-taiwans-election; Amy Searight, "Countering China's Influence Operations: Lessons From Australia," Center for Strategic and International Studies, May 8, 2020, https://www.csis.org/analysis/countering-chinas-influence-operations-lessons-australia; and Alex Joske, Lin Li, Alexandra Pascoem and Nathan Attrill, "The Influence Environment: A Survey of Chinese-Language Media in Australia," Australian Strategic Policy Institute, December 2020, https://s3-ap-southeast-2.amazonaws.com/ad-aspi/2020-12/The%20influence%20environment.pdf?Mjytg1N_V2azySJlJoahgWzMOqxEpMYk.

336 "Annual Threat Assessment of the US Intelligence Community," Director of National Intelligence, April 9, 2021, https://www.dni.gov/files/ODNI/documents/assessments/ATA-2021-Unclassified-Report.pdf.

337 "Intelligence Community Assessment: Foreign Threats to the 2020 US Federal Elections," National Intelligence Council, March 10, 2021, https://www.dni.gov/files/ODNI/documents/assessments/ICA-declass-16MAR21.pdf.

338 Alex Joske, Lin Li, Alexandra Pascoem, and Nathan Attrill, "The Influence Environment: A Survey of Chinese-Language Media in Australia," Australian Strategic Policy Institute, December 2020, https://s3-ap-southeast-2.amazonaws.com/ad-aspi/2020-12/The%20influence%20environment.pdf?Mjytg1N_V2azySJlJoahgWzMOqxEpMYk.

339 Alex Hern, "Revealed: How TikTok Censors Videos That Do Not Please Beijing," *Guardian*, September 25, 2019, https://www.theguardian.com/technology/2019/sep/25/revealed-how-tiktok-censors-videos-that-do-not-please-beijing; Isobel Asher Hamilton, "A Senior TikTok Executive Admitted the Company Used to Censor Content Critical of China, 'Specifically With Regard to the Uighur Situation,'" Business Insider, November 5, 2020, https://www.businessinsider.com/tiktok-censor-china-critical-content-uighur-uighurs-2020-11.

340 Jon Bateman, Elonnai Hickock, Laura Courchesne, Isra Thange, and Jacob N. Shapiro, "Measuring the Effects of Influence Operations: Key Findings and Gaps From Empirical Research," Carnegie Endowment for International Peace, June 28, 2021, https://carnegieendowment.org/2021/06/28/measuring-effects-of-influence-operations-key-findings-and-gaps-from-empirical-research-pub-84824.

341 Major platform efforts include revisions to community standards, enforcement actions taken against proscribed activity, and adjustments to the functionality of platform products. For overviews of each of these three areas, see Jon Bateman, Natalie Thompson, and Victoria Smith, "How Social Media Platforms' Community Standards Address Influence Operations," Carnegie Endowment for International Peace, April 1, 2021, https://carnegieendowment.org/2021/04/01/how-social-media-platforms-community-standards-address-influence-operations-pub-84201; "Disinfodex," Berkman Klein Center at Harvard University and the Ethics and Governance of Artificial Intelligence Fund at The Miami Foundation, 2020, https://disinfodex.org/; and Kamya Yadav, "Platform Interventions: How Social Media Counters Influence Operations," Carnegie Endowment for International Peace, January 25, 2021, https://carnegieendowment.org/2021/01/25/platform-interventions-how-social-media-counters-influence-operations-pub-83698.

342 "One Year After Stop Hate for Profit: Platforms' Progress," Stop Hate for Profit, June 16, 2021, https://www.stophateforprofit.org/platforms-progress-year-later; and Jessica Guynn, "Facebook Winning War on COVID-19 Vaccine Lies, Hoaxes and Conspiracies. Twitter and TikTok? Not So Much, Report Says," *USA Today*, May 7, 2021, https://www.usatoday.com/story/tech/2021/05/07/facebook-twitter-tiktok-covid-vaccine-conspiracy-theories-lies-hoaxes/4994731001/.

343 Olivia Solon and Ken Dilanian, "China's Influence Operations Offer a Glimpse Into the Future of Information Warfare," NBC News, October 21, 2020, https://www.nbcnews.com/business/business-news/china-s-influence-operations-offer-glimpse-future-information-warfare-n1244065.

344 Betsy Woodruff Swan, "DHS Stands Up Domestic Terror Intelligence Team," *Politico*, May 11, 2021, https://www.politico.com/news/2021/05/11/dhs-domestic-terror-intelligence-487145.

345 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.

346 "Fact Sheet: Executive Order Protecting Americans' Sensitive Data From Foreign Adversaries," 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.

347 Marco Rubio, "Rubio Requests Biden Administration's Plan for TikTok, Protecting Americans' Data," press release, October 12, 2021, https://www.rubio.senate.gov/public/index.cfm/2021/10/rubio-requests-biden-administration-s-plan-for-tiktok-protecting-americans-data.

348 Greg Roumeliotis and Echo Wang, "China's Tencent in Talks With U.S. to Keep Gaming Investments -Sources," Reuters, May 5, 2021, https://www.reuters.com/technology/exclusive-chinas-tencent-talks-with-us-keep-gaming-investments-sources-2021-05-05/.

349 Vishnu Kannan, forthcoming paper, Carnegie Endowment for International Peace; and Kamya Yadav, "Countering Influence Operations: A Review of Policy Proposals Since 2016," Carnegie Endowment for International Peace, November 30, 2020, https://carnegieendowment.org/2020/11/30/countering-influence-operations-review-of-policy-proposals-since-2016-pub-83333.

350 Jon Bateman, Elonnai Hickock, Laura Courchesne, Isra Thange, and Jacob N. Shapiro, "Measuring the Effects of Influence Operations: Key Findings and Gaps From Empirical Research," Carnegie Endowment for International Peace, June 28, 2021, https://carnegieendowment.org/2021/06/28/measuring-effects-of-influence-operations-key-findings-and-gaps-from-empirical-research-pub-84824; and Jon Bateman, Elonnai Hickock, Jacob N. Shapiro, Laura Courchesne, and Julia Ilhardt, "Measuring the Efficacy of Influence Operations Countermeasures: Key Findings and Gaps From Empirical Research," Carnegie Endowment for International Peace, September 21, 2021, https://carnegieendowment.org/2021/09/21/measuring-efficacy-of-influence-operations-countermeasures-key-findings-and-gaps-from-empirical-research-pub-85389.

DENYING SUPPORT FOR CHINESE AND CHINA-ENABLED AUTHORITARIANISM AND REPRESSION

351 "Freedom on the Net 2021: China," Freedom House, 2021, https://freedomhouse.org/country/china/freedom-net/2021.

352 John Hudson, "As Tensions With China Grow, Biden Administration Formalizes Genocide Declaration Against Beijing," *Washington Post*, March 30, 2021, https://www.washingtonpost.com/national-security/china-genocide-human-rights-report/2021/03/30/b2fa8312-9193-11eb-9af7-fd0822ae4398_story.html.

353 Alina Polyakova and Chris Meserole, "Exporting Digital Authoritarianism," Brookings Institution, August 2019, https://www.brookings.edu/wp-content/uploads/2019/08/FP_20190826_digital_authoritarianism_polyakova_meserole.pdf.

354 "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.

355 "Interim National Security Strategic Guidance," White House, March 2021, https://www.whitehouse.gov/wp-content/uploads/2021/03/NSC-1v2.pdf.

356 Matthew S. Erie and Thomas Streinz, "The Beijing Effect: China's 'Digital Silk Road' as Transnational Data Governance," *New York University Journal of International Law and Politics*, April 1, 2021, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3810256.

357 Matthew S. Erie and Thomas Streinz, "The Beijing Effect: China's 'Digital Silk Road' as Transnational Data Governance," *New York University Journal of International Law and Politics*, April 1, 2021, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3810256.

358 Steven Feldstein, "When It Comes to Digital Authoritarianism, China Is a Challenge—But Not the Only Challenge," War on the Rocks, February 12, 2021, https://warontherocks.com/2020/02/when-it-comes-to-digital-authoritarianism-china-is-a-challenge-but-not-the-only-challenge/.

359 "Three Former U.S. Intelligence Community and Military Personnel Agree to Pay More Than $1.68 Million to Resolve Criminal Charges Arising From Their Provision of Hacking-Related Services to a Foreign Government," press release, Justice Department, September 14, 2021, https://www.justice.gov/opa/pr/three-former-us-intelligence-community-and-military-personnel-agree-pay-more-168-million; Associated Press, "Germany Searches Premises of Spyware Maker FinFisher," October 14, 2020, https://apnews.com/article/germany-munich-spyware-software-7dd9b8d8cdd8021334b709165db949b6; "Commerce Adds NSO Group and Other Foreign Companies to Entity List for Malicious Cyber Activities," press release, Commerce Department, November 3, 2021, https://www.commerce.gov/news/press-releases/2021/11/commerce-adds-nso-group-and-other-foreign-companies-entity-list; Yonah Jeremy Bob, "Defense Min. Limits Countries Israeli Cyber Companies Can Sell to Post-NSO – report," *Jerusalem Post*, November 25, 2021, https://www.jpost.com/israel-news/defense-min-limits-countries-israeli-cyber-companies-can-sell-to-post-nso-report-687004; and Yonah Jeremy Bob, "Israeli Defense Ministry Tightens Cyber Exports Post-NSO Scandal," *Jerusalem Post*, December 6, 2021, https://www.jpost.com/breaking-news/defense-ministry-to-tighten-regulation-on-cyber-exports-687998.

360 Thomas Lum and Michael A. Weber, "Human Rights in China and U.S. Policy: Issues for the 117th Congress," Congressional Research Service, March 31, 2020, https://crsreports.congress.gov/product/pdf/R/R46750.

361 Amy K. Lehr, "The United States Blacklisted 28 Chinese Entities Over Repression of Muslim Minorities in Xinjiang. What Does This Mean for Human Rights?," Center for Strategic and International Studies, October 11, 2019, https://www.csis.org/analysis/united-states-blacklisted-28-chinese-entities-over-repression-muslim-minorities-xinjiang.

362 "Xinjiang Supply Chain Business Advisory," U.S. Government, July 13, 2021, https://www.state.gov/wp-content/uploads/2021/07/Xinjiang-Business-Advisory-13July2021-1.pdf.

363 Lily Kuo and Jeanne Whalen, "Biden Administration Bars Imports of Solar Panels Linked to Forced Labor in China's Xinjiang Region," *Washington Post*, June 24, 2021, https://www.washingtonpost.com/technology/2021/06/24/china-solar-forced-labor-imports-custom/; and Phred Dvorak and Matthew

Dalton, "Solar-Energy Supply Chain Depends on Region Where China Is Accused of Genocide," *Wall Street Journal*, April 11, 2021, https://www.wsj.com/articles/solar-energy-supply-chain-depends-on-region-where-china-is-accused-of-genocide-11618147228.

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

365 Will Knight, "MIT Cuts Ties With a Chinese AI Firm Amid Human Rights Concerns," *Wired*, April 21, 2020, https://www.wired.com/story/mit-cuts-ties-chinese-ai-firm-human-rights/.

366 Biden's new Indo-Pacific Strategy states that "our objective is not to change the PRC but to shape the strategic environment in which it operates." Trump's own China Strategy likewise stated that "United States policies are not premised on an attempt to change the PRC's domestic governance model." "Indo-Pacific Strategy of the United States," White House, February 2022, https://www.whitehouse.gov/wp-content/uploads/2022/02/U.S.-Indo-Pacific-Strategy.pdf; and "United States Strategic Approach to the People's Republic of China," White House, May 2020, https://trumpwhitehouse.archives.gov/wp-content/uploads/2020/05/U.S.-Strategic-Approach-to-The-Peoples-Republic-of-China-Report-5.24v1.pdf.

367 Robert O'Brien, "The Chinese Communist Party's Ideology and Global Ambitions," University of Southern California US-China Institute, June 24, 2020, https://china.usc.edu/robert-o%E2%80%99brien-chinese-communist-party%E2%80%99s-ideology-and-global-ambitions-june-24-2020.

368 Farhad Manjoo, "Dealing With China Isn't Worth the Moral Cost," *New York Times*, October 9, 2019, https://www.nytimes.com/2019/10/09/opinion/china-houston-rockets.html.

369 Anonymous, "The Longer Telegram: Toward a New American China Strategy," Atlantic Council, January 28, 2021, https://www.atlanticcouncil.org/content-series/atlantic-council-strategy-paper-series/the-longer-telegram/.

370 *The Broken Promises of China's WTO Accession: Reprioritizing Human Rights: A Hearing Before the Congressional-Executive Commission on China*, 115th Cong. (2017) (testimony of Sophie Richardson, March 1, 2017), https://www.cecc.gov/sites/chinacommission.house.gov/files/CECC%20Hearing%20-%20WTO%20-%20Sophie%20Richardson%20-1Mar17.pdf.

371 "A Human Rights Approach to US-China Policy," Human Rights Watch, February 17, 2021, https://www.hrw.org/news/2021/02/17/human-rights-approach-us-china-policy.

372 Kate O'Keeffe, Heather Somerville, and Yang Jie, "U.S. Companies Aid China's Bid for Chip Dominance Despite Security Concerns," *Wall Street Journal*, November 12, 2021, https://www.wsj.com/articles/u-s-firms-aid-chinas-bid-for-chip-dominance-despite-security-concerns-11636718400.

373 Zach Dorfman, "Tech Giants Are Giving China a Vital Edge in Espionage," *Foreign Policy*, December 23, 2020, https://foreignpolicy.com/2020/12/23/china-tech-giants-process-stolen-data-spy-agencies/; Katja Drinhausen and Vincent Brusee, "China's Social Credit System in 2021: From Fragmentation Towards Integration," MERICS, March 3, 2021, https://merics.org/en/report/chinas-social-credit-system-2021-fragmentation-towards-integration; Ryan Hass, "Assessing China's 'Common Prosperity' Campaign," Brookings Institution, September 9, 2021, https://www.brookings.edu/blog/order-from-chaos/2021/09/09/assessing-chinas-common-prosperity-campaign/; and Ann Listerud, "Chinese Communist Party Cells in Private Companies: Though Not Yet Universal, Increasingly Situated to Play Greater Roles in Corporate Governance," Sayari, April 7, 2021, https://sayari.com/resources/chinese-communist-party-cells-in-private-companies-though-not-yet-universal-increasingly-situated-to-play-greater-roles-in-corporate-governance/.

374 Thomas Carothers, "Does Democracy Promotion Have a Future?," in *Democracy and Development*, ed. Bernard Berendsen (Amsterdam: KIT Publishers, 2008), https://carnegieendowment.org/files/DemocracyDevm-Carothers-sec.pdf.

375 Clayton Thomas, Jeremy M. Sharp, Christopher M. Blanchard, and Christina L. Arabia, "Arms Sales in the Middle East: Trends and Analytical Perspectives for U.S. Policy," Congressional Research Service, November 23, 2020, https://sgp.fas.org/crs/mideast/R44984.pdf.

376 "Addition of Entities to the Entity List, Revision of Entry on the Entity List, and Removal of Entities From the Entity List," Commerce Department, 85 Fed. Reg. 83,416 (December 22, 2020), https://public-inspection.federalregister.gov/2020-28031.pdf.

377 Cate Cadell, "Drone Company DJI Obscured Ties to Chinese State Funding, Documents Show," *Washington Post*, February 1, 2022, https://www.washingtonpost.com/national-security/2022/02/01/china-funding-drones-dji-us-regulators/; Blake Schmidt and Ashlee Vance, "DJI Won the Drone Wars, and Now It's Paying the Price," *Bloomberg Businessweek*, March 26, 2020, https://www.bloomberg.com/news/features/2020-03-26/dji-s-drone-supremacy-comes-at-a-price; Matt Rivers, Max Foster, and James Griffiths, "Disturbing Video Shows Hundreds of Blindfolded Prisoners in Xinjiang," CNN, October 7, 2019, https://www.cnn.com/2019/10/06/asia/china-xinjiang-video-intl-hnk/index.html; and Liselotte Mas, "Drone Video Shows Blindfolded, Handcuffed Prisoners in China's Xinjiang Uyghur Region," France 24, September 25, 2019, https://observers.france24.com/en/20190925-drone-video-shows-mass-displacement-prisoners-china-xinjiang-uyghur-region.

378 John Venable and Lora Ries, "DJI Placed on the Entity List for Human Rights Abuses, but Concerns About Data Security Should Not Be Overlooked," Heritage Foundation, January 7, 2021, https://www.heritage.org/cybersecurity/commentary/dji-placed-the-entity-list-human-rights-abuses-concerns-about-data.

379 "Treasury Identifies Eight Chinese Tech Firms as Part of the Chinese Military-Industrial Complex," press release, Treasury Department, December 16, 2021, https://home.treasury.gov/news/press-releases/jy0538.

380 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.

381 Zak Doffman, "Is Microsoft AI Helping to Deliver China's 'Shameful' Xinjiang Surveillance State?," *Forbes*, March 15, 2019, https://www.forbes.com/sites/zakdoffman/2019/03/15/microsoft-denies-new-links-to-chinas-surveillance-state-but-its-complicated/; and Jacob Fromer, Cissy Zhoum, and Finbarr Bermingham, "US Farm Brand John Deere at Forefront of Surging Cotton Machinery Sales to Xinjiang, as Human Rights Sanctions Loom," *South China Morning Post*, August 8, 2020, https://www.scmp.com/economy/china-economy/article/3096510/us-farm-brand-john-deere-forefront-surging-cotton-machinery.

382 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; and Tamer A. Soliman, Andrew Olmem, Timothy J. Keeler, and Jason Hungerford, "US Investment Ban Targeting Companies Deemed Linked to Chinese Military Expanded to Chinese Surveillance Technology Sector," Mayer Brown, June 9, 2021, https://www.mayerbrown.com/en/perspectives-events/publications/2021/06/us-investment-ban-targeting-companies-deemed-linked-to-chinese-military-expanded-to-chinese-surveillance-technology-sector.

383 "Frequently Asked Questions: Chinese Military Company Sanctions" (question 900), Treasury Department, June 3, 2021, https://home.treasury.gov/policy-issues/financial-sanctions/faqs/topic/5671.

384 "Fact Sheet: Executive Order Addressing the Threat From Securities Investments That Finance Certain Companies of the People's Republic of China," White House, June 3, 2021, https://www.whitehouse.gov/briefing-room/statements-releases/2021/06/03/fact-sheet-executive-order-addressing-the-threat-from-securities-investments-that-finance-certain-companies-of-the-peoples-republic-of-china/.

385 "Treasury Sanctions Perpetrators of Serious Human Rights Abuse on International Human Rights Day," press release, Treasury Department, December 10, 2021, https://home.treasury.gov/news/press-releases/jy0526.

386 UIGHUR Act of 2019, S. 178, 116th Cong. (2019), https://www.congress.gov/bill/116th-congress/senate-bill/178/text; and Matt Spetalnick, Patricia Zengerle, David Brunnstrom, "U.S. Uighur Bill's Threat to Surveillance Economy Puts China on Offensive," Reuters, December 5, 2019, https://www.reuters.com/article/us-usa-china-xinjiang/u-s-uighur-bills-threat-to-surveillance-economy-puts-china-on-offensive-idUSKBN1Y92TV.

387 Uyghur Human Rights Policy Act of 2020, Public Law No. 116-145.

388 "Joint Statement on the Export Controls and Human Rights Initiative," White House, December 10, 2021, https://www.whitehouse.gov/briefing-room/statements-releases/2021/12/10/joint-statement-on-the-export-controls-and-human-rights-initiative/.

389 "White House Announces Launch of the International Grand Challenges on Democracy-Affirming Technologies for the Summit for Democracy," White House, December 8, 2021, https://www.whitehouse.gov/ostp/news-updates/2021/12/08/white-house-announces-launch-of-the-international-grand-challenges-on-democracy-affirming-technologies-for-the-summit-for-democracy/.

390 These are just a few of the possibilities. See Winnona DeSombre et al., "Countering Cyber Proliferation: Zeroing in on Access-as-a-Service," Atlantic Council, March 1, 2021, https://www.atlanticcouncil.org/in-depth-research-reports/report/countering-cyber-proliferation-zeroing-in-on-access-as-a-service/#policy recommendations.

391 Commerce Department, "Commerce Adds NSO Group and Other Foreign Companies to Entity List for Malicious Cyber Activities," November 3, 2021, https://www.commerce.gov/news/press-releases/2021/11/commerce-adds-nso-group-and-other-foreign-companies-entity-list; Yonah Jeremy Bob, "Defense Min. Limits Countries Israeli Cyber Companies Can Sell to Post-NSO – Report," *Jerusalem Post*, November 25, 2021, https://www.jpost.com/israel-news/defense-min-limits-countries-israeli-cyber-companies-can-sell-to-post-nso-report-687004; and Yonah Jeremy Bob, "Israeli Defense Ministry Tightens Cyber Exports Post-NSO Scandal," *Jerusalem Post*, December 6, 2021, https://www.jpost.com/breaking-news/defense-ministry-to-tighten-regulation-on-cyber-exports-687998.

392 "Join the Effort to Create A Bill of Rights for an Automated Society," White House, November 10, 2021, https://www.whitehouse.gov/ostp/news-updates/2021/11/10/join-the-effort-to-create-a-bill-of-rights-for-an-automated-society/.

COUNTERING UNFAIR CHINESE ECONOMIC PRACTICES AND INTELLECTUAL PROPERTY THEFT

393 Two fairly exhaustive lists of U.S. grievances compiled by the Trump administration include "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; and "How China's Economic Aggression Threatens the Technologies and Intellectual Property of the United States and the World," White House, June 18, 2018, https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/06/FINAL-China-Technology-Report-6.18.18-PDF.pdf.

394 "2021 China Business Climate Survey Report," AmCham China, March 2021, https://www.amchamchina.org/climate-survey/2021-business-climate-survey/.

395 "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; "U.S. Accuses China of Violating Bilateral Anti-hacking Deal," Reuters, November 9, 2018, https://www.reuters.com/article/usa-china-cyber-idUKL2N1XK06K; Ton Zuijdwijk, "Understanding the Intellectual Property Disputes between China and the United States," Centre for International Governance Innovation, May 15, 2019, https://www.cigionline.org/articles/understanding-intellectual-property-disputes-between-china-and-united-states/; and Stephen Ezell, "False Promises II: The Continuing Gap Between China's WTO Commitments and Its Practices," Information Technology & Innovation Foundation, July 26, 2021, https://itif.org/publications/2021/07/26/false-promises-ii-continuing-gap-between-chinas-wto-commitments-and-its.

396 "Statement by the President Regarding Trade With China," White House, June 15, 2018, https://trumpwhitehouse.archives.gov/briefings-statements/statement-president-regarding-trade-china/.

397 Jeanne Whalen, "Biden's Commerce Secretary Pick Pledges a Tough Line on China but Doesn't Detail How She'd Deal With Huawei," *Washington Post*, January 26, 2021, https://www.washingtonpost.com/technology/2021/01/26/gina-raimondo-confirmation-china/.

398 "Statement From President Donald J. Trump on Additional Proposed Section 301 Remedies," White House, April 5, 2018, https://trumpwhitehouse.archives.gov/briefings-statements/statement-president-donald-j-trump-additional-proposed-section-301-remedies/; and Ana Swanson, "W.T.O. Says American Tariffs on China Broke Global Trade Rules," *New York Times*, September 15, 2020, https://www.nytimes.com/2020/09/15/business/economy/wto-trade-china-trump.html.

399 Jeffrey J. Schott and Euijin Jung, "In US-China Trade Disputes, the WTO Usually Sides With the United States," PIIE, March 12, 2019, https://www.piie.com/blogs/trade-and-investment-policy-watch/us-china-trade-disputes-wto-usually-sides-united-states.

400 Nina M. Hart and Brandon J. Murrill, "The World Trade Organization's (WTO's) Appellate Body: Key Disputes and Controversies," Congressional Research Service, July 22, 2021, https://crsreports.congress.gov/product/pdf/R/R46852; Gary Clyde Hufbauer, "WTO Judicial Appointments: Bad Omen for the Trading System," PIIE, June 13, 2011, https://www.piie.com/blogs/realtime-economic-issues-watch/wto-judicial-appointments-bad-omen-trading-system; Manfred Elsig, Mark Pollack, and Gregory Shaffer, "The U.S. Is Causing a Major Controversy in the World Trade Organization. Here's What's Happening," *Washington Post*, June 6, 2016, https://www.washingtonpost.com/news/monkey-cage/wp/2016/06/06/the-u-s-is-trying-to-block-the-reappointment-of-a-wto-judge-here-are-3-things-to-know/; Steve Charnovitz, "The Obama Administration's Attack on Appellate Body Independence Shows the Need for Reforms," International Economic Law and Policy Blog, September 22, 2016, https://worldtradelaw.typepad.com/ielpblog/2016/09/the-obama-administrations-attack-on-appellate-body-independence-shows-the-need-for-reforms-.html.

401 Brandon J. Murrill, "The WTO's Appellate Body Loses Its Quorum: Is This the Beginning of the End for the 'Rules-Based Trading System'?," Congressional Research Service, December 19, 2019, https://crsreports.congress.gov/product/pdf/LSB/LSB10385; and Marianne Schneider-Petsinger, "Reforming the World Trade Organization," Chatham House, September 11, 2020, https://www.chathamhouse.org/2020/09/reforming-world-trade-organization/04-dispute-settlement-crisis.

402 Bryce Baschuk, "Biden Picks Up Where Trump Left Off in Hard-Line Stances at WTO," *Bloomberg*, February 22, 2021, https://www.bloomberg.com/news/articles/2021-02-22/biden-picks-up-where-trump-left-off-in-hard-line-stances-at-wto.

403 WTO, "Principles of the Trading System," https://www.wto.org/english/thewto_e/whatis_e/tif_e/fact2_e.htm. "WTO" here is used as shorthand for various international agreements, starting chronologically with the 1947 General Agreement on Tariffs and Trade, that the WTO now oversees. The WTO regime is complemented by other international bodies that have also adopted nondiscrimination as a core economic principle. See "Guidelines for Recipient Country Investment Policies Relating to National Security," Organisation for Economic Co-operation and Development, 2009, https://www.oecd.org/investment/investment-policy/43384486.pdf.

404 Bryce Baschuk, "Biden Picks Up Where Trump Left Off in Hard-Line Stances at WTO," *Bloomberg*, February 22, 2021, https://www.bloomberg.com/news/articles/2021-02-22/biden-picks-up-where-trump-left-off-in-hard-line-stances-at-wto.

405 A WTO panel reviewed this history at length in a landmark 2019 decision regarding Russia's claim of a "national security exception" vis-à-vis Ukraine. "Russia – Measures Concerning Traffic in Transit: Report of the Panel" (Appendix), WTO, April 5, 2019, https://docs.wto.org/dol2fe/Pages/SS/directdoc.aspx?filename=q:/WT/DS/512R.pdf.

406 Peter Van den Bossche and Sarah Akpofure, "The Use and Abuse of the National Security Exception Under Article XXI(b)(iii) of the GATT 1994," World Trade Institute, Working Paper no. 345, September 15, 2020, https://www.wti.org/research/publications/1299/the-use-and-abuse-of-the-national-security-exception-under-article-xxibiii-of-the-gatt-1994/.

407 "2021 Trade Policy Agenda and 2020 Annual Report of the President of the United States on the Trade Agreements Program," USTR, March 2021, https://ustr.gov/sites/default/files/files/reports/2021/2021%20Trade%20Agenda/Online%20PDF%202021%20Trade%20Policy%20Agenda%20and%202020%20Annual%20Report.pdf.

408 "A Conversation With Ambassador Katherine Tai, U.S. Trade Representative," Center for Strategic and International Studies, October 4, 2021, https://www.csis.org/analysis/conversation-ambassador-katherine-tai-us-trade-representative.

409 "Ambassador Katherine Tai's Remarks as Prepared for Delivery on the World Trade Organization," USTR, October 14, 2021, https://ustr.gov/about-us/policy-offices/press-office/speeches-and-remarks/2021/october/ambassador-katherine-tais-remarks-prepared-delivery-world-trade-organization.

410 "U.S.-EU Trade and Technology Council Inaugural Joint Statement," press release, USTR, September 29, 2021, https://ustr.gov/about-us/policy-offices/press-office/press-releases/2021/september/us-eu-trade-and-technology-council-inaugural-joint-statement.

411 "A Conversation With Ambassador Katherine Tai, U.S. Trade Representative," Center for Strategic and International Studies, October 4, 2021, https://www.csis.org/analysis/conversation-ambassador-katherine-tai-us-trade-representative.

COMPETING AND LEADING IN STRATEGIC INDUSTRIES

412 Remco Zwetsloot et al., "China Is Fast Outpacing U.S. STEM PhD Growth," Center for Security and Emerging Technology, August 2021, https://cset.georgetown.edu/publication/china-is-fast-outpacing-u-s-stem-phd-growth/; "The Human Capital Report 2016," World Economic Forum, 2016, https://www3.weforum.org/docs/HCR2016_Main_Report.pdf; and "Gross Domestic Spending on R&D," Organisation for Economic Co-operation and Development, 2021, https://data.oecd.org/rd/gross-domestic-spending-on-r-d.htm.

413 Robert Greene and Paul Triolo, "Will China Control the Global Internet Via Its Digital Silk Road?," SupChina, May 8, 2020, https://carnegieendowment.org/2020/05/08/will-china-control-global-internet-via-its-digital-silk-road-pub-81857.

414 For a review of this history, see 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.

415 Mark Scott and Emily Birnbaum, "How Washington and Big Tech Won the Global Tax Fight," *Politico*, June 30, 2021, https://www.politico.eu/article/washington-big-tech-tax-talks-oecd/.

416 James Andrew Lewis, "Mapping the National Security Industrial Base: Policy Shaping Issues," CSIS, May 19, 2021, https://www.csis.org/analysis/mapping-national-security-industrial-base-policy-shaping-issues.

417 The blue-ribbon Cyberspace Solarium Commission expressed a version of this concern: "Chinese national companies like Huawei are part of an integrated strategy to use predatory pricing to dominate and eventually monopolize key information and communications technology supply chains. The goal is to drive non-Chinese alternatives out of business, leaving the Chinese Communist Party and its business allies with a stranglehold on the global supply chain." "Final Report," Cyberspace Solarium Commission, March 2020, https://www.solarium.gov/report.

418 John S. McCain National Defense Authorization Act for Fiscal Year 2019, Public Law No. 115-232, § 1702(c)(1).

419 Commerce Department, "Review of Controls for Certain Emerging Technologies," 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.

420 Peter Lichtenbaum, Victor Ban, and Lisa Ann Johnson, "Defining 'Emerging Technologies': Industry Weighs in on Potential New Export Controls," China Business Review, April 17, 2019, https://www.chinabusinessreview.com/defining-emerging-technologies-industry-weighs-in-on-potential-new-export-controls/; Paul H. DeLaney, "Business Roundtable Comments on the Advance Notice of Proposed Rulemaking (ANPRM) Regarding the Review of Controls for Certain Emerging Technologies," January 12, 2019, https://www.businessroundtable.org/business-roundtable-comments-on-the-advance-notice-of-proposed-rulemaking-anprm-regarding-the-review-of-controls-for-certain-emerging-technologies; and Linda Dempsey, "Comments of the National Association of Manufacturers on the Review of Controls for Certain Emerging Technologies (Docket BIS 2018-0024)," National Association of Manufacturers, January 9, 2019, http://documents.nam.org/iea/NAM%20Comments%20on%20Emerging%20Technology%20for%20BIS%20(final).pdf.

421 Council on Governmental Relations et al., "RIN 0694-AH80, Identification and Review of Controls for Certain Foundational Technologies ANPRM," November 2020, https://www.cogr.edu/sites/default/files/AAU_COGR_ACE_APLU_AAMC_ANPRM%20Foundational%20Technologies.pdf.

422 Steven W. Popper and Caroline Wagner, "Identifying Critical Technologies in the United States: A Review of the Federal Effort," *Journal of Forecasting* 22, no. 2–3 (2003), https://www.researchgate.net/publication/5141648_Identifying_critical_technologies_in_the_United_States_A_review_of_the_federal_effort; and Mary Ellen Mogee, *Technology Policy and Critical Technologies: A Summary of Recent Reports* (Washington DC: National Academies Press, 1991), https://www.nap.edu/read/20840/chapter/5.

423 "National Critical Technologies Report—Appendix A: National Critical Technologies List," White House, March 1995, https://clintonwhitehouse3.archives.gov/WH/EOP/OSTP/CTIformatted/AppA/appa.html.

424 "National Strategy for Critical and Emerging Technologies," White House, October 2020, https://trumpwhitehouse.archives.gov/wp-content/uploads/2020/10/National-Strategy-for-CET.pdf.

425 "Critical and Emerging Technologies List Update," National Science and Technology Council, February 2022, https://www.whitehouse.gov/wp-content/uploads/2022/02/02-2022-Critical-and-Emerging-Technologies-List-Update.pdf.

426 Emphasis in original.

427 "Asymmetric Competition: A Strategy for China & Technology," China Strategy Group, Fall 2020, https://www.documentcloud.org/documents/20463382-final-memo-china-strategy-group-axios-1; and Jeffrey Ding and Allan Dafoe, "The Logic of Strategic Assets: From Oil to AI," *Security Studies* 30, no. 2 (2021), https://doi.org/10.1080/09636412.2021.1915583.

428 The United States does not have a single company that competes on a one-for-one basis with Huawei or ZTE in 5G telecommunications equipment markets. However, U.S. partners Finland (Nokia) and Sweden (Ericcson) do compete in aspects of these markets, and the United States has an interest in preventing Chinese dominance. Moreover, U.S. companies support various aspects of the 5G supply chain, and could do so more fully and effectively if the open, software-based 5G standard known as O-RAN continues to develop as a viable alternative to the closed, hardware-based systems sold by Huawei and ZTE.

429 Justin Hodiak and Scott W. Harold, "Can China Become the World Leader in Semiconductors?," *The Diplomat*, September 25, 2020, https://thediplomat.com/2020/09/can-china-become-the-world-leader-in-semiconductors/; Christopher A. Thomas, "Lagging But Motivated: The State of China's Semiconductor Industry," *Brookings TechStream* (blog), Brookings Institution, January 7, 2021, https://www.brookings.edu/techstream/lagging-but-motivated-the-state-of-chinas-semiconductor-industry/; Arjun Kharpal, "China Is Ramping Up Its Own Chip Industry Amid a Brewing Tech War," CNBC, June 4 2019, https://www.cnbc.com/2019/06/04/china-ramps-up-own-semiconductor-industry-amid-the-trade-war.html; and Jordan Schneider, "China's Chip Industry: Running Faster But Still Falling Behind," Rhodium Group, April 22, 2021, https://rhg.com/research/china-chips/.

430 Alexandra Alper, Toby Sterling, and Stephen Nellis, "Trump Administration Pressed Dutch Hard to Cancel China Chip-equipment Sale: Sources," Reuters, January 6, 2020, https://www.reuters.com/article/us-asml-holding-usa-china-insight/trump-administration-pressed-dutch-hard-to-cancel-china-chip-equipment-sale-sources-idUSKBN1Z50HN; and Justin Hodiak and Scott W. Harold, "Can China Become the World Leader in Semiconductors?," *The Diplomat*, September 25, 2020, https://thediplomat.com/2020/09/can-china-become-the-world-leader-in-semiconductors/.

431 Karen Freifeld, "Huawei Gets U.S. Approvals to Buy Auto Chips, Sparking Blow Back," Reuters, August 25, 2021, https://www.reuters.com/business/autos-transportation/exclusive-us-approves-licenses-huawei-buy-auto-chips-sources-2021-08-25/.

432 For an explanation of this issue, 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.

433 Ellen Nakashima and Jeanne Whalen, "Key Security Agencies Split Over Whether to Blacklist Former Huawei Smartphone Unit," *Washington Post*, September 19, 2021, https://www.washingtonpost.com/national-security/huawei-honor-security-export/2021/09/19/6d49d27c-17ef-11ec-b976-f4a43b740aeb_story.html.

434 Michael McCaul et al., letter to Gina Raimondo, August 6, 2021, https://gop-foreignaffairs.house.gov/wp-content/uploads/2021/08/8-6-21-CTF-Letter-to-Sec-Raimondo-RE-Honor-Device-Co-1.pdf.

435 Christine Fox, "An Entwined AI Future: Resistance Is Futile," 2020, JHU APL, https://www.jhuapl.edu/assessing-us-china-technology-connections/dist/071c25aa35e135f3c20c2f53f182de11.pdf.

436 Regarding China's potential advantages in certain AI sub-fields, one recent study noted that "a disproportionate share of China's highly cited and top-venue [AI] publications include publications on general-purpose computer vision research, as well as applications of AI to surveillance and industry." Ashwin Acharya and Brian Dunn, "Comparing U.S. and Chinese Contributions to High-Impact AI Research," Center for Security and Emerging Technology, January 2022, https://cset.georgetown.edu/publication/comparing-u-s-and-chinese-contributions-to-high-impact-ai-research/.

437 Rand Waltzman et al., "Maintaining the Competitive Advantage in Artificial Intelligence and Machine Learning," RAND Corporation, 2020, https://www.rand.org/pubs/research_reports/RRA200-1.html.

438 Sam Shead, "Why the Buzz Around DeepMind Is Dissipating as It Transitions From Games to Science," CNBC, June 5, 2020, https://www.cnbc.com/2020/06/05/google-deepmind-alphago-buzz-dissipates.html.

439 A much more detailed and comprehensive set of proposals, related primarily but not exclusively to AI, can be found in the report of the National Security Commission on Artificial Intelligence. "Final Report," National Security Commission on Artificial Intelligence, March 2021, https://www.nscai.gov/wp-content/uploads/2021/03/Full-Report-Digital-1.pdf.

440 Robert D. Atkinson, "The Case for a National Industrial Strategy to Counter China's Technological Rise," Information Technology & Innovation Foundation, April 13, 2020, https://itif.org/publications/2020/04/13/case-national-industrial-strategy-counter-chinas-technological-rise.

441 Robert D. Atkinson, "The Case for a National Industrial Strategy to Counter China's Technological Rise," Information Technology & Innovation Foundation, April 13, 2020, https://itif.org/publications/2020/04/13/case-national-industrial-strategy-counter-chinas-technological-rise.

OBTAINING GENERAL LEVERAGE OVER CHINA

442 Michael S. Schmidt and Maggie Haberman, "Bolton Was Concerned That Trump Did Favors for Autocratic Leaders, Book Says," *New York Times*, June 17, 2020, https://www.nytimes.com/2020/01/27/us/politics/john-bolton-trump-book-barr.html; and "Trump Says Huawei Could Be Part of Trade Deal," BBC, May 24, 2019, https://www.bbc.com/news/business-48392021.

443 John D. McKinnon, "Trump Says 'There Has Been No Folding' Over Possible ZTE Deal," *Wall Street Journal*, May 16, 2018, https://www.wsj.com/articles/trump-says-there-has-been-no-folding-over-possible-zte-deal-1526494867.

444 Sarah Zheng, "US-China Relations: Meng Wanzhou's Return Clears One Roadblock to a Reset," *South China Morning Post*, September 27, 2021, https://www.scmp.com/news/china/diplomacy/article/3150302/us-china-relations-meng-wanzhous-return-clears-one-roadblock.

445 Sha Hua and Timothy Puko, "U.S.-China Surprise Cooperation on Climate Change Driven by Biden and Xi's Need for Deal," *Wall Street Journal*, November 12, 2021, https://www.wsj.com/articles/biden-and-xi-pressed-for-u-s-china-climate-statement-11636718318.

SHAPING U.S. DOMESTIC NARRATIVES

446 "High-Risk Series: Dedicated Leadership Needed to Address Limited Progress in Most High-Risk Areas," Government Accountability Office, March 2, 2021, https://files.gao.gov/reports/GAO-21-119SP/index.html.

447 Yajana Sharma, "Top US Research Universities Freeze Ties With Huawei," University World News, February 11, 2019, https://www.universityworldnews.com/post.php?story=20190211124159161.

448 Georgia Wells, Jeff Horwitz, and Aruna Viswanatha, "Facebook CEO Mark Zuckerberg Stoked Washington's Fears About TikTok," *Wall Street Journal*, August 23, 2020, https://www.wsj.com/articles/facebook-ceo-mark-zuckerberg-stoked-washingtons-fears-about-tiktok-11598223133.

449 "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," press release, Treasury Department, August 14, 2020, https://home.treasury.gov/news/press-releases/sm1094.

450 Georgia Wells, Aaron Tilley, and John D. McKinnon, "How Dark Horse Oracle Became TikTok's Leading Suitor," *Wall Street Journal*, September 14, 2020, https://www.wsj.com/articles/oracle-tiktok-deal-trump-politics-microsoft-11600129980.

451 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.

CARNEGIE ENDOWMENT FOR INTERNATIONAL PEACE

The Carnegie Endowment for International Peace is a unique global network of policy research centers in Russia, China, Europe, the Middle East, India, and the United States. Our mission, dating back more than a century, is to advance peace through analysis and development of fresh policy ideas and direct engagement and collaboration with decision-makers in government, business, and civil society. Working together, our centers bring the inestimable benefit of multiple national viewpoints to bilateral, regional, and global issues.

TECHNOLOGY AND INTERNATIONAL AFFAIRS PROGRAM

The Carnegie Technology and International Affairs Program (TIA) helps governments and industries reduce large-scale international risks of new technologies and related services. Recognizing that commercial actors control many of the most germane technologies, TIA identifies best practices and incentives that can motivate industry stakeholders to pursue growth by enhancing rather than undermining international relations.

TIA's work informs and is informed by direct dialogues among thought-leaders, senior officials, and executives in key countries. We share the data, insights, and policy recommendations that result in reports, commentaries, and web tools. Carnegie's regional centers and networks in the United States, China, Europe, India, and Russia provide a widely respected international platform for promoting our policy proposals.

CarnegieEndowment.org