How China Views It

SINO-AMERICAN TECHNOLOGY COMPETITION

Dan Blumenthal, Gregory Graff, and Christian Curriden

OCTOBER 2022

AMERICAN ENTERPRISE INSTITUTE

Contents

How China Views It

SINO-AMERICAN TECHNOLOGY COMPETITION

Dan Blumenthal

In the fall of 2021, in partnership with the Hertog Foundation, I led a research fellowship called "National Security & Sino-American Technology Competition." Fifteen emerging Asia strategists and technologists took part in a series of 18 evening seminars taught by top subject-matter experts on a wide range of topics, including artificial intelligence, cyberwarfare, semiconductors, biotechnology, and energy. I was fortunate to be able to draw on the expertise of my AEI colleagues—Mackenzie Eaglen, Sheena Chestnut Greitens, Kori Schake, and Derek Scissors—and leading researchers and practitioners, including Tarun Chhabra, senior director for technology and national security at the National Security Council; Lt. Gen. Jack Shanahan (ret.), former director of the Joint Artificial Intelligence Center; Michael Lauer, deputy director for extramural research at the National Institutes of Health; and James Mulvenon.

The fellows applied what they learned in the seminars to their own independent research project on US-China technology competition. The two reports that follow this foreword are from that exercise's top papers and were presented at a policy salon dinner hosted by AEI. Some of the policy community's top China and technology experts attended and took part in a lively and enriching discussion.

In the first report, Gregory Graff, a Department of Defense analyst, surveys US trade controls on dual-use technologies. Just a few years ago, this topic would have seemed overly technical and even unimportant. Now it is anything but. An analysis of US efforts to tighten export controls reveals much about China's technology strategy. Even as China seeks to achieve self-reliance and encourage indigenous innovation, it is still highly dependent on technology transfers from the US.

To make this case, Graff cites a Peking University study on the implications for China of potential decoupling from the United States. The article on the study disappeared from circulation right after it was published, almost certainly because of its brutal honesty about China's technological shortcomings. Graff writes:

> Peking University's Institute of International Strategic Studies concluded China would be at a greater disadvantage than the United States would from a mutual technology decoupling. . . . The article identifies that China lags in knowledge creation, financial investment, talent cultivation, some aspect of patents (though not total numbers), and overall dominance of international standards. Overall, its analysis views China as having made progress in some areas to catch up to the United States, but it says China continues to have obvious vulnerabilities and bottlenecks.

The article was clear-eyed about the US lead in most key measures of technological progress. Given its conclusions, it is little wonder that Chinese companies continue to seek technology from the US. But as Graff shows, US efforts to impede technology transfer are failing, with Chinese companies exploiting loopholes and other weaknesses in export controls.

Although both the US and China say they want decoupling, neither can bring itself to cut the relationship off—with the troubling result that Chinese military modernization is being driven, in part, by access

to American technology. This dynamic is likely to persist, since the People's Republic of China (PRC) will continue to seek technology from the United States.

The difficulty in even partial decoupling stems from the Sino-American technological relationship's roots in Deng Xiaoping's market-based economic reforms, which encouraged large-scale investment by multinationals in the Chinese economy. US technology policy was a pillar of the American grand strategy of engaging China. The US sought a strong partner against the Soviets during the Cold War and was mesmerized by Chinese success at economic development, hopeful that the introduction of markets into the Chinese economy would lead to political changes and strategic alignment. Undoing decades of this intensive commercial interaction and educational exchange is proving difficult.

One key takeaway from the Hertog fellowship is that the driving impetus behind US technology transfer to China was deliberate and purposeful. Much focus today is on US frustration with and concern about the growing challenge of China's technological development, especially since China's illicit programs of technology transfer are also so robust and effective. But it is worth remembering that the US decided to adjust its tech transfer policies only after decades of openness.

In any case, since Sino-American relations are highly competitive, with two strategic actors seeking to gain advantage, more scholarly and policy attention needs to be paid to *China's* profound frustration about its continued dependencies on the US and its fears of being cut off from "core technologies." Here is Xi Jinping on the topic:

> Advanced technology is the sharp weapon of the modern state. An important reason that Western countries were able to hold sway over the world in modern times was that they held the advanced technology. You cannot buy the truly core technologies.[1]

But despite such pronouncements and a determined strategy of self-reliance in core technology, the PRC is very much still buying those technologies from abroad. Take semiconductors: Nothing is more "core" than the integrated circuits that are the brains of all electronics, from personal computer CPUs to navigation systems for ballistic and cruise missiles. In 2021, microelectronics were China's top import, even above oil[2]—and this is not for lack of trying to meet demand indigenously.

According to the Congressional Research Service, in June 2014, when the Chinese government published *Guidelines to Promote National Integrated Circuit Industry Development*, the PRC's goal was to meet

> 70% of China's semiconductor demand with domestic production by 2025. In 2019, China revised the goal upward, setting an objective of expanding its domestic production of semiconductors (including from foreign firms in China) to meet 80% of domestic demand by 2030, as part of its *Made in China 2025* industrial strategy. . . . [But] IC Insights estimate that integrated circuits produced in China accounted for approximately 16% of China's total market.[3]

For the foreseeable future, China will import semiconductors designed in the US and manufactured, in one of the most complex industrial processes in existence, in Taiwan and South Korea. China's inputs into the process are further down the value chain. It is good at outsourced semiconductor assembly, packaging, and testing (OSAT), which is a lower value-added process. According to the Semiconductor Industry Association, China held 38 percent of the total OSAT market in 2020.[4] To be sure, it is improving in complex manufacturing (fiercely competing with Taiwan Semiconductor Manufacturing Company) and artificial intelligence chip design (competing with American players). Still, China is far behind, and it will be an importer for some time to come.

As Graff's report demonstrates, unless the US develops better export policies, harmonized with all major semiconductor players outside China, the US and its allies will continue to feed People's Liberation Army (PLA) modernization. As Graff notes, with the advent of China's Military-Civil Fusion program, which mobilized the civilian sector for military purposes, the sheer volume of Chinese companies working with the PLA is beyond the scope of the current

US policy of listing "entities" of national security concern for special scrutiny in export license applications. There are simply too many such entities in China.

As Graff comprehensively covers the shortcomings of the US system meant to stem the tide of the PLA's growth, Christian Curriden, a RAND Corporation defense analyst, provides a window into how the PLA views the role of new technologies in warfare. Curriden chronicles the PLA's absorption and adaptation of a host of information technologies into what PLA leaders hope is a novel form of warfare.

However, Curriden shows that this supposedly novel concept, called "systems warfare," has its roots in the American airpower theory tradition and the hopes of its advocates that strategic airpower could systemically paralyze an enemy, obviating the need for a protracted force-on-force clash. Ultimately, Curriden concludes that the PLA's aspirations for systems warfare will likely fall short, as did those of American airpower enthusiasts. Nevertheless, Curriden finds that the ambition is clear:

> The PLA has invested heavily in several new technologies that may prove just as decisive as military aviation, stealth, or precision-guided weapons. In particular, it hopes that the ability of artificial intelligence to gather and analyze large volumes of data may finally solve the long-standing problem of identifying and finding centers of gravity. Many of the PLA's artificial intelligence–related purchases have been of systems meant to disrupt command systems and data links.

According to Curriden, PLA thinking about how new technology can help it cut off the US military's head such that its body cannot function sound a lot like the

> assertions of [Billy] Mitchell, [Hugh] Trenchard, [Col. John] Warden, and others in arguing that enemies can be characterized as a system of interconnected nodes, that such a system is dependent on a relatively small number of centers of gravity whose disruption can paralyze the whole, and that this disruption can be achieved with long-range effects, without the need for a Clausewitzian clash of armies.

Curriden's report is of particular importance given how much PLA aspirations have driven China's overall technology. Even during the high tide of Sino-American engagement after the Cold War, the Chinese Communist Party's top leadership was increasingly appalled at how far ahead the US was technologically—and how that translated into military superiority. The PLA watched in fear as the US military dominated its opponents during the Iraq and Kosovo wars, with relatively little cost in blood or treasure. America had "won" the information revolution and leveraged its advantages into military power. The Gulf War was a window for Chinese leaders into a "frightening future where US high-technology weapons could be wielded against China's outdated forces."[5] Unchecked global power combined with a technological edge made the US a formidable foe.

These insights informed Xi's call to "catch up and surpass"[6] the US and win what he sees as the next revolution in technological affairs:

> A new technological and industrial revolution is brewing, a global revolution in military affairs is accelerating, and the pattern of international military competition is experiencing historic changes. The United States is the leader of the pack in this revolution in military affairs, and in many areas it holds the initiative, and it is also striving to gain new advantages in military technology.[7]

But Xi has also told his cadres that China has a chance to surpass the US in key aspects of what he sees as a new, fourth industrial revolution, driven by accelerations in computing power, artificial intelligence, and biotechnology.

As Xi argued in a 2018 speech, these technological changes could bring "earth-shaking changes" and an "important opportunity to promote leapfrog development," allowing China to bypass legacy systems and overtake competitors.[8] The question of whether we are indeed in a new technology revolution akin to the information revolutions is still open and debatable,

but Xi believes we are and that China can "win" to the PLA's benefit.

However, sober-minded US defense planners are less confident that these technological changes are actually changing the character of war. Another consistent theme of discussions during the Hertog fellowship was an appropriate techno-skepticism. For example, the US military is challenged by China because it has let all its capabilities to fight a peer competitor deteriorate. Possible technological lags are one element of this erosion.

The real problem is that the US does not have enough munitions, ships, bases, and intelligence, surveillance, and reconnaissance assets to stop the PLA from accomplishing its plans, and there is no technological fix for that. That requires adequate defense resourcing and diplomacy with allies to gain access to basing. These are decidedly low-tech endeavors.

Indeed, while technology competition is a key concern of policymakers in both countries, the ultimate geopolitical contest is unlikely to be decisively shaped by high-tech breakthroughs. Should the US decide to translate its still overwhelming economic wealth into diplomatic and military power in Asia, it is doubtful that China would succeed in its ambition of displacing the US as global leader.[9] To be sure, China will continue to challenge the US across a range of important industries and technologies, many of which can be translated into military power.

But ultimately, any US strategy aiming to maintain its leading position in the world order must pose many different kinds of problems for China, and at the military level, it must create many different kinds of targets Beijing must destroy to prevail in a war. That requires more resources, from steel to concrete to artificial intelligence chips, thoughtfully deployed.

Countering China's Military Modernization Through Technology Controls

EXISTING MEASURES AND OPPORTUNITIES TO ADVANCE FURTHER CONTROLS

Gregory Graff

Over the past two administrations, the US government has significantly increased its response to China's now well-known technology transfer efforts, having recognized the importance of maintaining a technological edge against a strategic competitor. The Trump administration's 2017 National Security Strategy began this effort, placing an emphasis on promoting and protecting the "National Security Innovation Base" and ensuring the US remains a science and technology leader.[10] President Joe Biden's recently released *Interim National Security Guidance* largely maintains continuity, directing that "America must reinvest in retaining our scientific and technological edge and once again lead." When discussing China, it notes, "We will confront unfair and illegal trade practices, cyber theft, and coercive economic practices that . . . undercut our advanced and emerging technologies, and seek to erode our strategic advantage and national competitiveness."[11] Both administrations were wrestling with a fundamental strategic challenge: how to preserve America's technology advantage and protect it from China's exploitation.

These strategies have been matched with action. Beginning in the Trump administration, the US government—through the Departments of Commerce and the Treasury—began to aggressively apply technology controls on China. Generally, if the US government seeks to restrict access to technology, it occurs under three separate but related policy regimes: (1) foreign investment, which is governed by the Committee on Foreign Investment in the United States (CFIUS) review process; (2) Department of Commerce export controls under the Export Administration Regulations (EAR) and the Department of State's International Traffic in Arms Regulations (ITAR); and (3) Treasury sanctions under the International Emergency Economic Powers Act (IEEPA).

This report explores the nuances of the technology controls applied across both administrations, how those controls have been applied, weaknesses in applied controls, and additional opportunities to restrict China's access to US technologies. Although one of the imperatives behind restricting China's access to advanced US technologies is to broadly ensure the technology leadership that advances US prosperity, this report focuses mainly on the effectiveness of controls at maintaining US military technology leadership and examines controls exclusively through that lens.

In addition, while CFIUS is discussed indirectly in later sections, most of this report focuses on export controls and financial sanctions. A major shift in CFIUS policy occurred with Congress passing the Foreign Investment Risk Review Modernization Act (FIRRMA) of 2018. And while CFIUS is an important tool, cases remain confidential, and broader policy

shifts in deciding those cases are difficult to discern based on publicly available information.

Conversely, there are significant publicly available data on the shifting policy approaches taken under the Trump administration—and continued under the Biden administration—emphasizing the use of controls on specific types or groups of Chinese entities through the export control and financial sanctions policy regimes. These have generally been effective at impeding, though often not outright eliminating, these entities' access to US technology. In many cases, there are clear shortcomings to the approach taken so far, in terms of matching scale to threat.

This report proceeds in three parts. The first section briefly examines China's strategic approach to technology competition, beyond the oft-discussed topics of technology transfer. It also examines recent Chinese writings from economic and strategic scholars, which likely reflect Beijing's concerns regarding its current dependence on US technology inputs.

The second section examines the entity-based controls applied in the Trump and Biden administrations using export controls and financial sanctions, including controls such as the Entity List and the Specially Designated Nationals (SDN) List. These controls specify, via lists, Chinese entities for which certain actions are prohibited, which provides some ability to target restrictions, but the controls have been applied too narrowly and lack scale.

The third section examines some incipient, broader technology controls that have not been applied or have only narrowly been applied—but which hold greater promise for preventing US technology from enabling the People's Liberation Army's (PLA) modernization. An exemplar case study of computer numerical controlled (CNC) machine tools is discussed—as well as counterarguments from US industry.

China's Science and Technology Strategy and Dependencies

Typically, analyses of China's science and technology strategy emphasize the many ways by which China is licitly and illicitly acquiring US science and technology. As there is little new ground to tread on that subject, this section focuses more on China's overall national strategy and how science and technology supports its pursuit of composite national power.

China's Strategy. Broadly, China is pursuing a whole-of-nation strategic effort to achieve political, economic, and social modernity by expanding China's composite national power to achieve "the great rejuvenation of the Chinese nation."[12] Chinese Communist Party (CCP) leaders describe China's fundamental national aspiration as "restor[ing]" China to a position of strength and prosperity on the world stage.[13] As the CCP constitution states:

> The basic line of the Communist Party of China . . . is to lead all the people of China together in a self-reliant and pioneering effort, making economic development the central task . . . so as to see China becomes a great modern socialist country.[14]

This aspiration matters because of the links Chinese leaders see between national development and military modernization. As expressed in the Department of Defense's (DOD) 2020 China military power report:

> China's military modernization objectives are commensurate with and part of China's broader national development aspirations and work in coordination with China's economic policies and systems. China's leaders directly link the pace and scale of the PLA's modernization with the country's overall development. China's economic, political, social, and military development efforts are mutually reinforcing and support its strategy of national rejuvenation.[15]

For China's strategists, military competition is a systems confrontation between two states and their respective defense strategies, systems, and degree of military-civil synergy. They believe that China's ability to win in its competition with the United States is directly based on its ability to marshal the full scope of its society and resources in support of military and development goals.[16]

China's science and technology strategy is a key pillar of China's national development and its military modernization. The most well-known exemplar of this is China's Made in China 2025 plan, which seeks to set higher targets for domestic manufacturing in strategic industries. Because of significant criticism, China began avoiding references to Made in China 2025, but seeking independence from foreign technology inputs remains a clear strategic imperative for China.[17]

A 2018 speech by President Xi Jinping emphasized this. He noted that for China, "key and core technologies" remain controlled by foreign countries. For China to "grow strong, prosperous, and rejuvenated," he instructed that it must "become the world's main center of science and the high ground of innovation."[18] This means that Xi is setting leadership in science and technology as an explicit foundational requirement for achieving the party's overall goal of rejuvenating China. For Xi and the CCP, the stakes cannot be higher.

Moreover, China's strategic science and technology goals do not exist in a vacuum. They are contextualized by China's broader perception that it is locked in a decades-long competition for power with the United States. Writings by Chinese strategists and economists, discussed later in this report, make clear the deep threat perception Beijing has regarding its dependence on US technology.

In the context of its broader view of this rivalry, Beijing will elevate the goal of eliminating these dependencies far above the business logic of whether it is efficient or cost-effective. Indeed, Beijing's logic rests on the strategic imperative of ensuring these dependencies are eliminated to provide China the latitude to achieve its grand objectives. A future in which China remains dependent on US technology inputs—in which it remains perpetually a fast follower—is fundamentally unacceptable to the CCP because it would mean that China had not achieved its goal of being a great, modern socialist country and a world leader in science and technology.

China's Dependencies. At present, Chinese sources reveal a deep concern over being cut off from access to Western technology. Chinese researchers and think tanks across the domains of strategic, economic, and military research have examined the effects of US technology controls and perceive them to be a critical threat to China's technology development. Despite some major successes in China's science and technology development, these researchers and think tanks still see significant exploitable dependence on the US for high technology and are concerned about the impact that losing access to US technology would have on China's ability to successfully catch up. Their recommendations, which because of their consistency across sources likely reflect a consensus view among Beijing's decision makers, are largely to accelerate China's own capacity for indigenous technology development while in some cases trying to squeeze as much utility as possible out of remaining links to the United States.

A 2021 article published in the *Journal of Inner Mongolia University of Finance and Economics*, by business school professors from Minnan Normal University, presents Chinese observations of the impact of US technology controls on China's integrated circuit industry, the reliance of that industry on US inputs, and the actions China is taking to counter them. The authors identify large structural dependencies in China's integrated circuit industry on US and other countries' exports to China across the Chinese microchip production chain, an "embarrassing situation" that they seek to resolve. Their writing reveals a deeply competitive mindset. They warn,

> In order to defend its economic interests, the United States will carry out precise strikes against relevant integrated circuit enterprises in [China], strictly control the supply of cutting-edge chip technology and products, and curb the development of [China]'s chip technology.[19]

As specific weaknesses, the authors identify high or complete dependence on the US for a variety of advanced chips—as well as materials and electronic design automation (EDA) software and tools. The authors even discuss the utility of mergers and acquisitions with US companies to obtain US technology, noting that "the United States has advanced

technology in the field of integrated circuits, and [our] country can carry out technical exchanges with it through mergers and acquisitions to shorten the time for technological catch-up." However, they note that the US has started using CFIUS reviews to prevent this and has "closed the door for Chinese integrated circuit companies to enter the US market . . . and to acquire core technologies by investing in US companies."[20]

In all, the article paints a stark portrait of US countermeasures to China's technology development, probably far greater than the on-the-ground reality. Nevertheless, the authors proceed with recommending countermeasures for Chinese companies. Many of their recommendations are well-known pillars of China's technology competition strategy: encourage enterprises to diversify their supply chains to reduce dependency on the United States, use government funding to increase domestic research and development of advanced chip designs, encourage international companies to establish research and development and production centers in China, and build a base of microchip talent.

The last recommendation they make, however, is far more undisguised and candid than the others. The authors argue that China should make "full use of interest groups to lobby the US government," leveraging US companies' interests in sales in China to influence US government decision-making. It references an example of an effort by the Semiconductor Industry Association (SIA), on behalf of Qualcomm and other companies, to lobby Commerce to lift the ban on Huawei's chip sales. The authors write,

> [Our] country should make full use of this point, strengthen interaction with US companies, actively push US companies to negotiate with the government, [and] apply for temporary licenses for product exports. . . . This will delay the effective time of the US technology blockade and buy time for the development of domestic integrated circuits.[21]

Another article published in 2022 by Peking University's Institute of International Strategic Studies concluded China would be at a greater disadvantage than the United States would from a mutual technology decoupling. This article made headlines in the West because of its candid conclusion and because it almost immediately disappeared—a likely indicator of its authoritativeness.[22] The article identifies that China lags in knowledge creation, financial investment, talent cultivation, some aspect of patents (though not total numbers), and overall dominance of international standards. Overall, its analysis views China as having made progress in some areas to catch up to the United States, but it says China continues to have obvious vulnerabilities and bottlenecks, while the United States is leading more comprehensively. China is "following" the United States in most fields, "running" in a few fields, and "leading" in very few fields.[23]

Interestingly, the authors note that a future challenge for China is that it has been so used to following and using the United States as a benchmark—adapting a Chinese proverb that says "crossing the river by feeling the stones" by describing it as "crossing the river by feeling the US"—that when China takes the lead in a field, it may lose that target and so lose momentum or direction for continued, original innovation. The article portrays the current US government approach to technology competition, noting that the United States seeks "precise decoupling" to strike a balance among national security, economic gains, and technology advantages and firmly decouple the "core technologies that China urgently needs but [in which it] cannot achieve self-sufficiency." In addition, the authors portray an effort to establish an "alliance of democracies for science and technology" to isolate China.

The authors predict that both China and the US are moving toward a common goal of "two-way decoupling," for which China's losses will be greater. Their recommendations for China are to "stabilize its advantageous areas" with academic exchanges, more investment in research and development, international cooperation, talent cultivation, "effective transformation of scientific and technological achievements," and "firm determination in independent innovation."[24]

Beyond economic and think tank researchers, the PLA has also wrestled with the challenge of

responding to US technology controls. Two authors at the Academy of Military Sciences, a premier PLA research institute, examine US actions, such as the Section 301 investigation and export controls, as evidence of a "technology blockade." One of the researchers is affiliated with the Academy of Military Sciences subordinate institute, the National Innovation Institute of Defense Technology. The existence of this institute indicates that the PLA is taking the challenge of technology competition seriously enough to dedicate resources and personnel to research it.[25]

The authors argue that US efforts will delay China's development of advanced information communications technologies and increase their costs—technologies they view as essential for China's political, economic, and military development. Interestingly, the Academy of Military Sciences authors ascribe the source of US efforts to contain China's technological development as stemming from US politicians' self-interests and desire to stoke conflict with China to distract from internal conflicts, which suggests that some flawed assessments of US strategy underlie PLA thinking. The authors also mirror the language used by the *Journal of Inner Mongolia University of Finance and Economics* in describing US actions as "precise attacks" on China's high-technology fields. Their recommendations are largely in line with other Chinese writings: strengthen top-level design and planning of China's science and technology, advance indigenous innovation and research and development, strengthen talent cultivation, and expand international cooperation.[26]

Entity-Based Controls

This section will examine entity-based controls applied in the Trump and Biden administrations, such as the Entity List and the SDN List. These lists specify Chinese entities for which certain actions are prohibited. Although entity-based controls provide some ability to target restrictions, they have been applied too narrowly and lack scale.

The Entity List. Over the past few years, the US government has added a significant number of Chinese entities to the Department of Commerce's Entity List. The Entity List was established by the EAR and includes foreign persons—including companies, research institutions, government organizations, specific individuals, and other types of legal persons—that are subject to specific license requirements for the export, reexport, or in-country transfer of specified items. Inclusion on the Entity List does not ban US companies from exporting to a listed entity outright—a common misunderstanding.

In the most stringent cases, inclusion on the list requires any US exporter to apply for a license to export any item to the listed company, regardless of whether the item would normally require a license under the EAR. However, Commerce imposes a license-application review policy for every entity on the Entity List, and for most entities, that policy is a "presumption of denial."[27] A presumption of denial for a company on the Entity List means, in effect, Commerce is giving potential US exporters notice that they must apply for a license to export anything to that company and that the exporters should presume their license will be denied unless they can make a strong case for why the transaction would not harm US national interests.[28]

Commerce's additions to the Entity List have included Chinese entities in multiple industries and have come with varied justifications. The industries represented have included supercomputers,[29] nuclear power generation,[30] internet security, cloud software and the Internet of Things,[31] high-technology surveillance,[32] communications,[33] microelectronics,[34] oil and gas,[35] quantum computing,[36] and biotechnology.[37] For many technologies, Commerce's justification is based on its role in enabling China's military modernization, but other justifications include human rights violations involving Uyghur Muslims in Xinjiang[38] and those technologies enabling the reclamation and militarization of South China Sea outposts.[39] Perhaps the most famous Chinese company on the Entity List, Huawei, was added because of its efforts to circumvent US sanctions on Iran,[40] not because of any asserted connections to China's military or security apparatus.

Commerce's use of the Entity List has engendered concerns in China of a US technology blockade impeding its development[41] and has led China's Ministry of Commerce to develop, in retaliation, its own "Unreliable Entity List" to punish Western companies.[42] The sum total of these effects has been more stringent licensing restrictions for US exports to these Chinese companies, which is likely affecting the companies' ability to access US technology.

The Military End User and Military Intelligence End User Lists. In the past two years, Commerce has also established two additional entity-based lists—the Military End User (MEU) and Military Intelligence End User (MIEU)—giving it additional flexibility to impose export controls on Chinese entities supporting China's military modernization. These lists supplement the Entity List, but each was established because of separate policy imperatives.

The MEU List grew as a necessity after Commerce changed its policy in 2020 on transfers of certain items for military end use. In 2007, Commerce published a rule imposing license requirements on exports, reexports, and transfers of certain items intended for military end use in China. Commerce's stated policy, at the time, was to approve exports for civil end use but generally deny exports that make a "direct and significant" contribution to Chinese military capabilities. As applied then, many Export Control Classification Numbers (ECCNs)—though not all—that would not have otherwise required a license to export to China would start to require one if the exporter knew its products were destined for military end use. Those licenses would be reviewed on a case-by-case basis to determine whether the export would make a "material contribution" to the PLA. The covered ECCNs included items not covered under national security controls, such as materials, software, tools for electronics design, computers, telecommunications equipment, sensors and lasers, navigation equipment, and aircraft parts.[43]

This authority was expanded in 2020 to include exports intended not only for military end use but also MEUs. On its face, this expansion seems to be counterintuitive: Items intended for military end use would presumably go to MEUs. Commerce released an FAQ for applying the MEU rule that revealed the regulatory logic behind this rule change.[44] Commerce defined MEUs as both the military and related organizations of a country and any other end users whose activities are intended to support military end use—that is, incorporating the product into a military item or using the product for supporting the operation, installation, maintenance, repair, overhaul, refurbishing, development, or production of military items.[45] This includes state-owned enterprises (SOEs) or other entities that develop, produce, use, or maintain military items.

Thus, items that would have been exempted from the military end use rule because they were exported to a nonmilitary SOE intended for civil end use would now require a license solely based on whether the end user is involved in military end uses. In other words, expanding the rule to include MEUs, as defined by Commerce, brought a greater number of transactions under the rule.

This is important because the MEU rule change also applies a license review policy of presumption of denial. However, according to Commerce's FAQ, that presumption can be overcome when license applications demonstrate "exclusive civil end use" or meet other criteria on a case-by-case basis.[46] Following Commerce's MEU rule change, it received numerous requests for advisory opinions on the applicability of the MEU rules in different cases to different end users. To ease the public's compliance burden, Commerce published a list of MEUs—what we know as the MEU List—which was explicitly non-exhaustive.[47]

A few months after releasing the MEU List, Commerce also released an MIEU rule. At first glance, this would appear largely duplicative, as an MIEU would, by definition, be an entity that conducts activities ultimately intended to support military end use—the definition of an MEU. Commerce's reasoning for establishing the MIEU rule was not duplicative, however; it was based on specific requirements set forth in the 2018 Export Control and Reform Act (ECRA).

ECRA stipulated that the president had to impose controls on the activities of US persons relating to several areas, including foreign military intelligence

services. The EAR already restricted activities for all areas except military intelligence services, so the MIEU restriction was necessary to cover that last part. The MIEU authority works by imposing license requirements for the export, reexport, and transfer of all items subject to the EAR when they are intended for military intelligence end uses and end users in China. This makes the MIEU broader than the MEU, since the MEU requires a license only for certain items in the EAR, rather than the entire EAR.[48] However, being listed on the MIEU carries fewer restrictions than being on the Entity List, which imposes a license requirement on both EAR and non-EAR goods.

As of right now, the MIEU is more of an export control novelty, as the only Chinese entity listed by Commerce on the MIEU List is the Joint Staff Department's Intelligence Bureau.[49] Admittedly, Commerce's list is non-exhaustive, but the failure to list the Strategic Support Force, which has military intelligence functions, suggests systematically evaluating and adding all applicable MIEUs is not a priority at this time.[50]

NS-CMIC Companies List. The origins of Treasury's Non-SDN Chinese Military-Industrial Complex (NS-CMIC) List begin in 2020, when the DOD began acting on a two-decades-old statutory requirement from the fiscal year (FY) 1999 National Defense Authorization Act (NDAA) Section 1237 to produce a list of Communist Chinese Military Companies (CCMCs). Section 1237 directed the secretary of defense to—not later than 90 days after the NDAA was signed—determine and publish a list of CCMCs operating in the United States, in consultation with the attorney general, director of central intelligence, and FBI. The NDAA defined a CCMC as any person "owned or controlled" by the PLA and "engaged in providing commercial services, manufacturing, producing, or exporting." The PLA is defined as the "land, naval, and air military services, the police, and the intelligence services of the Communist Government of the People's Republic of China, and any member of any such service or of such police."[51]

A key and unique provision of Section 1237 is that it authorizes the president to impose IEEPA restrictions on the commercial activity of any CCMC without having to declare a national emergency (which is statutorily required for exercising IEEPA authority).[52] IEEPA provides the president broad authority to regulate and block economic transactions subject to the jurisdiction of the United States and is commonly used to enforce financial sanctions. In recent history, the president's declaration of a national emergency to invoke the IEEPA has largely been a formality. The 1976 National Emergencies Act proscribes some congressional oversight and authorities to reverse presidential declarations of emergency, but these have never been exercised with respect to the IEEPA. As of 2020, there are 37 ongoing national emergencies, all but four of which invoked the IEEPA.[53]

From all available information, the DOD did not publicly respond to Section 1237, though a public response was not required. Later, Section 1237 was modified by Section 1222 of the FY2005 NDAA, which significantly expanded the definition of what entities could be classified as CCMCs, modifying the FY1999 definition to include

> any person that is owned, or controlled, *or affiliated with* the People's Liberation Army, *or a ministry of the government of the People's Republic of China, or that is owned or controlled by an entity affiliated with the defense industrial base of People's Republic of China.*[54] (Emphasis added.)

The 2005 definition could reasonably define *any* company in China, since in a Leninist state, any private enterprise is affiliated with the government, especially since at no point did the NDAA define what constitutes affiliation. Clearly, expanding the scope of the requirement did not result in the DOD publishing a public list for a long time, though given the potential impossibility of the task, it is difficult to fault them. The NDAA provision effectively was ignored by both DOD and Congress until September 2019, when Sens. Tom Cotton (R-AR) and Chuck Schumer (D-NY) and Reps. Michael Gallagher (R-WI) and Ruben Gallego (D-AZ) wrote a letter to then–Secretary of Defense Mark Esper asking him to release a list that complied with Section 1237.[55]

Beginning in June 2020, the department released an initial list of 20 qualifying CCMCs,[56] following up in August with another 11.[57] In November 2020, the Trump administration issued Executive Order (EO) 13959, which prohibited any US person from "any transaction in publicly traded securities, or any securities that are derivative of, or are designed to provide investment exposure to such securities" of any "Communist Chinese military company."[58] EO 13959 defines CCMCs as any person or entity the secretary of defense has already listed pursuant to Section 1237 and, in the future, any person or entity the secretary of defense in consultation with the secretary of the Treasury, or the secretary of the Treasury alone, determines meets the definition of Section 1237.

Two companies on the EO 13959 list have sued in the District Court for the District of Columbia, challenging their designation, and have been successful in obtaining preliminary injunctions against the US government.[59] Interestingly, despite Section 1237 permitting the president to exercise IEEPA authorities without declaring a national emergency, EO 13959 nevertheless declares a national emergency. When it comes to subsidiaries, Treasury's Office of Foreign Assets Control provided clarifying guidance that the provisions of EO 13959 would not apply to the subsidiaries of a CCMC unless OFAC lists that subsidiary itself.[60]

Section 1237 was updated in legislation under Section 1260H of the FY2021 NDAA, which made several changes. First, it shifted the name from "Communist Chinese military companies" to simply "Chinese military companies" (CMCs). It also directed the secretary of defense to submit a list of each identified company annually—a provision not specified in Section 1237—while permitting ongoing revisions as needed.

It also substantively narrowed the definition from the broad definition in the FY2005 NDAA. Under Section 1260H, a CMC is either

> an entity directly or indirectly owned, controlled, or beneficially owned by, or in an official or unofficial capacity acting as an agent of or on behalf of, the People's Liberation Army or any other organization subordinate to the Central Military Commission of the Chinese Communist Party [or identified as a] military-civil fusion contributor to the Chinese defense industrial base.[61]

That second category is significantly more broad. It includes entities receiving Chinese government assistance through science and technology efforts under China's military-industrial planning apparatus; entities affiliated with the Ministry of Industry and Information Technology; the State Administration for Science, Technology, and Industry for National Defense; entities residing in military-civil fusion (MCF) enterprise zones; and entities that have permits from the Chinese government to participate in the defense industrial base. The goal seems to be threading the needle between the FY1999 definition, which could miss much of China's defense industrial base, and the FY2005 definition, which would encompass essentially all of China's commercial enterprises.

Likely as a result of the updated statutory requirements and the priorities and approach of the Biden administration, the CCMC List began morphing into two separate lists. On June 3, 2021, the Biden administration issued EO 14032, which modifies and replaces the Trump administration's EO 13959, expanding restrictions in some areas while eliminating other prohibitions. Under EO 14032, Treasury created and published a new list of 59 NS-CMIC companies that would be covered under EO 14032. Unlike 13959's division of labor, where DOD designates a CCMC and OFAC implements investment restrictions, EO 14032 stipulates that only OFAC designates an NS-CMIC company.

On that same date, DOD released the names of CMCs required under Section 1260H of the FY2021 NDAA.[62] Following that, the DOD issued a federal ruling that the secretary of defense has removed the designation of CCMCs from entities previously listed as such under Section 1237, and as of the writing of this report, there are no CCMCs listed.[63] In fact, only 37 of the 47 CMCs on the 1260H CMC List are also designated under the NS-CMIC List. Because 1260H carries no IEEPA provisions, as 1237 did, that list

essentially functions only to name and shame. Only being listed as an OFAC-designated entity on the NS-CMIC List carries economic consequences.[64]

The initial development of the 1237 list and EO 13959 created numerous process errors that EO 14032 apparently seeks to remedy. One of the companies on DOD's original CCMC List, Xiaomi, was granted a preliminary injunction by the District Court for the District of Columbia enjoining any of EO 13959's restrictions from becoming effective. Of note, the court found that DOD failed to establish that Xiaomi is a CCMC. DOD defended its decision by pointing to Xiaomi's involvement in 5G internet networks and the receipt by Xiaomi's founder of an award by the Chinese government—an evidently threadbare justification.

In another example, Luokung Technology was listed, but Treasury delayed implementation of its restrictions because DOD had misspelled the company's name.[65] It was removed from the CCMC List when DOD removed all companies from that list, and it was never added to the NS-CMIC List.[66]

SDN List. Aside from the NS-CMIC List, another tool in Treasury's arsenal is the SDN List. As noted earlier, IEEPA provides the president broad authorities to investigate, regulate, and prohibit transactions and freeze assets. Although the NS-CMIC List falls under IEEPA, it does not take full advantage of IEEPA authorities. Only transactions in securities of the Chinese military-industrial complex companies are prohibited; assets are not frozen, and other, broader transactions with those companies are not blocked.

The NS-CMIC List's more limited employment of IEEPA authorities is a departure from how IEEPA has traditionally been used regarding counterterrorism, Iran, Russia, and other sanctions. Those sanctions employ the full scope of IEEPA authorities, freezing assets and prohibiting transactions, and sanctioned entities are included on the SDN List. Although both the Trump and Biden administrations have taken significant steps using other authorities to protect the US technological advantage, neither has employed the full scope of IEEPA authorities in the context of US-China technology competition.

Some Chinese companies and persons have been listed on the SDN List because they were listed under sanctions related to Ukraine and Russia, North Korea, Iran, illicit drugs and transnational crimes, and Syria. In fact, sanctions on Russia ultimately resulted in sanctions on the PLA's Equipment Development Department (EDD) and its director for purchasing Russian Su-35 combat aircraft and S-400 surface-to-air missile systems.[67] The EDD performs research, development, test, and evaluation functions and oversees procurement management for the PLA,[68] making the Russia-related sanctions on it the only time the SDN List was deliberately used to target some aspect of China's military technology acquisition and development apparatus.

None of these other sanction regimes are aimed at China specifically. Two sets of sanctions did, however, target China, but not for military or technology reasons. President Donald Trump signed EO 13936 in July 2020 to impose sanctions under IEEPA on Chinese entities that have been involved in undermining Hong Kong's autonomy, following Beijing's crackdown on protests there.[69] In addition, that same month, Treasury sanctioned several Chinese individuals and organizations in connection with human rights abuses in Xinjiang.[70] Both resulted in several Chinese individuals being listed on the SDN List, but these were relatively limited uses of IEEPA authorities and do not directly address Chinese military modernization.

Two other IEEPA declarations of national emergency exist that could be applied to China's technology acquisition entities but have not been so employed. In 2015, President Barack Obama issued EO 13694, declaring a national emergency for "cyber-enabled activities originating from, or directed by persons located, in whole or in substantial part, outside the United States."[71] This was later expanded under EO 13757 in 2016, in response to Russian interference in the US elections.[72] So far, however, sanctions under these EOs have only been applied to Russian and Iranian cyber actors, even though China has a well-known history of directing cyber activities against the United States.

In 2020, President Trump issued EO 13920 declaring a national emergency "with respect to the threat

to the United States bulk-power system." This EO prohibited any "acquisition, importation, transfer, or installation of any bulk-power system electric equipment" that is "designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary."[73] The EO never, however, defined who a foreign adversary was, leaving that authority to the secretary of energy. Ultimately, the EO was suspended by the Biden administration, which chose to pursue a slower but more methodical and wider-ranging effort to research and develop recommendations to build resilient, diverse supply chains under EO 14017.[74]

Shortcomings of Entity-Based Lists. All of these entity-based lists share similar shortcomings in preventing US technology from enabling China's military: an inability to address the scale of China's military modernization because of their whack-a-mole approach, a to-date policy approach that prioritizes fine-tuning rather than maximizing restrictions, and vulnerabilities to legal remedies from listed entities.

Whack-a-Mole Approach. Because entity-based lists can only address China's military modernization entity by entity, they represent a whack-a-mole approach that struggles to manage both the scale and inherent opacity of China's defense industrial base. The US sanctions regime against Iran and North Korea has notably also struggled with the challenge of Iranian companies repeatedly creating front companies to evade US government sanctions.[75]

Identifying and adding a Chinese entity to one of these lists requires an inherent expenditure of labor. For example, the Entity List uses a process in which companies of concern are identified and a committee composed of the Departments of Commerce, State, Defense, Energy, and (when appropriate) the Treasury adds an entity. Such a process is unlikely to mitigate this threat at scale.

China's MCF development strategy—and its 2017 National Intelligence Law and 2015 National Security Law—has been frequently discussed as a threat of diversion of goods and knowledge from China's civilian industry to its military. While MCF does not impose a legal obligation on companies to participate—China's authoritarian system can coerce cooperation without legal requirements—it does leverage incentives and muddy the lines between civilian and military sectors.[76]

Within MCF, the Advanced Defense Science, Technology, and Industrial System of Systems seeks to achieve "deep fusion" between the defense industrial base and the civilian industrial and manufacturing base.[77] Largely, this integration takes the form of encouraging greater private company participation in the sector, which has hitherto been dominated by large SOEs, such as China Aerospace Science and Technology Corporation (CASC). China's MCF development strategy opens the door for SOEs on the Entity List to leverage relationships with private companies entering the MCF ecosystem to procure needed equipment from the United States. China's defense SOEs can also establish front companies themselves, some of which end up on the Entity List, such as China National Nuclear Group Corporation's subsidiary Baotou Guanghua Chemical Industrial Corporation.[78]

A 2019 study by the China Aerospace Studies Institute suggests that 2 percent (3,000 out of 150,000) of China's private high-tech companies are involved in the defense supply chain and that they primarily provide parts or material supplies. Data it cites from the PLA's EDD indicate 2,300 civilian companies in China have an Equipment Manufacturing Unit Qualification Permit, the last of three permits required to take part in China's defense supply chain.[79]

In comparison, a review of Commerce's Entity List indicates that—judging by name alone—only around 270 private Chinese companies are listed. The NS-CMIC and MEU Lists are even smaller, with 68[80] and 56 companies[81] each. Even if all listed companies were MCF-related, which is not true for the Entity List but is for the others, these lists fall short of covering the scale of private industry supporting China's military modernization by an order of magnitude.

A Center for Security and Emerging Technology report, *Harnessed Lightning*, examined 273 known artificial intelligence equipment suppliers for the

PLA, and of those, only 22 were identified on the Entity List, the NS-CMIC List, or DOD's Section 1260H list.[82] Altogether, the number of companies on the Entity List, the NS-CMIC List, and the MEU List is dwarfed by the total number of companies estimated to be in China's defense industrial base. Using entity-based lists to adequately cover the full scope of China's MCF-involved private-sector companies would require a massive scale-up of current efforts and a concurrent increase in resources.

Another obstacle to employing these lists at scale is their inability to target subsidiaries. For example, CASC and other SOEs like it are not listed in their entirety on Commerce's Entity List. Instead, Commerce will identify and list multiple of their subsidiaries—a trend also seen on the other lists, such as the NS-CMIC List. In Commerce's case, it does not just list a parent company without specifying which specific subsidiaries it also applies controls to, probably to provide specificity to exporters.

The shortcoming of this approach is that China's defense SOEs are gargantuan and labyrinthine organizations, and numerous gaps can be easily identified. For example, the Project 2049 Institute identified in 2009 that China Aerospace Science and Industry Corporation (CASIC) Fourth Academy was the likely systems integrator for China's anti-ship ballistic missile program—a key military capability for countering US military intervention in the region.[83] Yet it is not listed on the Entity List, which only includes CASIC Second Academy and several research institutes subordinate to the Third Academy.

In Treasury's case, a subsidiary of an NS-CMIC company is not automatically considered an NS-CMIC company. Treasury has to specifically add that entity to the NS-CMIC List. This provides investors a degree of clarity regarding what might or might not be a tradable security, but it belies that massive Chinese defense industrial companies have many subsidiaries. Since the NS-CMIC List was established, 22 entries have been added, with two removed after apparently being consolidated into other entries. This is far short of the scope of China's defense industry. *Harnessed Lightning* asserts that tens of thousands of Chinese companies are licensed to supply the PLA. Of the 273 known artificial intelligence equipment suppliers, roughly 12 percent are subsidiaries that have a parent company listed on the NS-CMIC List, but because EO 14032 specifies that ownership by an NS-CMIC parent company is not enough for a subsidiary to be automatically considered an NS-CMIC company, those subsidiaries are not automatically considered as on the NS-CMIC List.[84]

Another weakness of the entity-based approach is that any Chinese entity listed under a US sanctions regime could either set up a front company or leverage an existing Chinese company to procure prohibited items. Here again, *Harnessed Lightning* reveals a trend of Chinese suppliers making a business out of sourcing foreign data or components and reselling them to listed Chinese entities. As the report notes, many companies in China engage in this activity.[85] Trying to use entity-based controls to identify and list these broker companies will probably be an uphill battle, as new companies could take the place of sanctioned ones.

Fine-Tuning Approach. The US government's application of these lists has also taken a narrow approach in applying their full authorities. Often, the full scope of possible restrictions is not applied to an entity. For example, in using the Entity List, Commerce will often restrict the scope of its application of the policy of presumption of denial on licenses. These efforts create loopholes and inhibit the broader strategic challenge of countering China's military modernization.

Commerce's fine-tuning appears to represent a genuine effort to balance competing national priorities. For example, in December 2020, Commerce added over 70 companies and organizations—mostly Chinese entities—to the Entity List. Among these designations were four companies added because of their involvement in enabling human rights abuses in Xinjiang by providing genetic collection and analysis or high-technology surveillance equipment.[86] For these companies, Commerce chose to apply a case-by-case review for licenses for items necessary to detect, identify, and treat infectious disease but a presumption of denial for all other items. The infectious disease exemption was probably due to at least

one of these companies' involvement in COVID-19 test kit development.[87] Certainly, this had strategic merit given the ongoing pandemic.

In other cases, these efforts can create exploitable gaps. For example, Commerce designated the Semiconductor Manufacturing International Corporation (SMIC) and 10 of its subsidiaries as part of this tranche, based on its support of China's MCF strategy and "evidence of activities between SMIC and entities of concern in China's military-industrial complex." Despite the concerns stemming from SMIC's role in China's military modernization, Commerce chose to impose a license review policy of presumption of denial only for items "uniquely required" for production of cutting-edge semiconductors at 10 nanometers (nm) or below, "to prevent such key enabling technology from supporting China's military modernization efforts."[88] Commerce excluded items for higher nm—and thus less advanced—semiconductor manufacturing. At the time, SMIC was not producing semiconductors at the sub–14 nm size.[89] Commerce's approach apparently sought to balance the need to protect high-end chip manufacturing technologies and impede Chinese companies from developing and deploying leading-edge fabrication technologies, while still preserving the potential for US companies to export older fabrication technologies.

The fine-tuning of SMIC's Entity List–based controls appears to come with some risk of still enabling SMIC's advanced manufacturing. In 2021, when SMIC initiated construction on two new fabrication facilities, it had to equip both with US-made equipment from four US providers—all of which have applied for export licenses—though it is unclear whether those licenses were approved or denied. According to one trade publication, the facility was aimed at producing 28 nm and larger semiconductors;[90] however, another publication indicated it would focus on developing 14 nm and below chips, to include 7 nm chips.[91]

A related issue is the potential fungibility of equipment SMIC could procure from the United States that is not "uniquely required" for 10 nm or below but that could nevertheless be used for those chips. In fact, the advanced microchips SMIC aims to produce offer distinct military advantages, such as better communications, electronic warfare capabilities, and the ability to benefit from big data and machine learning.

A 2016 Defense Advanced Research Projects Agency analysis singled out 14 and 10 nm chips as applicable for cognitive electronic warfare.[92] Cognitive electronic warfare is the application of artificial intelligence technologies to electronic warfare to enable an electronic warfare system to quickly and autonomously perceive its electromagnetic environment—a capability the PLA Strategic Support Force is pursuing.[93]

Artificial intelligence and microchip industry publications already anticipate that the proliferation of artificial intelligence technologies on the "edge" of telecommunications networks—the end points, such as personal computers, phones, modems, and the devices that connect to them—will require semiconductors at the 14 nm and below feature size because of the requirements for small size and efficient power consumption.[94] It can be assumed that future warfare concepts, such as mosaic warfare, that emphasize the proliferation of artificial intelligence at the edge of warfighting networks, particularly among unmanned systems, will also necessitate that advanced microchips be integrated into those edge systems.

Thus, although SMIC was added to the Entity List because of its support to Chinese military modernization, the semiconductors it produces or will produce in the future to satisfy China's military requirements, particularly its requirements for semiconductors for advanced artificial intelligence–enabled and autonomous systems, could likely be produced using US exports sold to it after it was listed.

Indeed, Republican House Foreign Affairs Committee Chairman Rep. Michael McCaul (R-TX) released data from the Department of Commerce on SMIC license decisions from November 9, 2020, to April 20, 2021, which found that Commerce approved 188 of 206 (91.3 percent) licenses for SMIC, returning 17 without action (8.3 percent) and denying only one (0.5 percent). While 121 of the approved licenses were for EAR99 items—export goods the EAR deems nonsensitive and so carry no controls—67 approved licenses were for material processing items, electronic

items, information security items and services, and parts and equipment used to manufacture semiconductors, all controlled for a variety of reasons, including nuclear nonproliferation, anti-terrorism, and national security reasons. Altogether, these 67 approved licenses covered almost $6.8 million in value.[95] Chinese media reporting confirmed at least some of these licenses were for equipment supporting 14 nm processes, exempted from requiring a license under US policy for SMIC.[96]

The NS-CMIC List's emphasis on prohibiting investment, rather than employing the full scope of IEEPA's powers to prohibit all transactions, is another example. There are unrealized benefits to applying the full scope of IEEPA authorities by adding Chinese entities of concern to the SDN List to address China's technology acquisition efforts. These benefits go beyond just the NS-CMIC List's narrower prohibitions on securities trading, which do offer a means to prevent these entities from receiving US investment dollars via securities trading. When added to the SDN List, US persons, including US financial institutions, are generally prohibited from engaging in any transactions with the entity and are required to freeze any property or interests in property belonging to SDNs that are or come into US possession.

To be sure, many large SOEs supporting China's defense industrial base are unlikely to be vulnerable to or reliant on US bank accounts. However, as both Center for Security and Emerging Technology and Center for Advanced Defense Studies reports have identified, a significant number of universities and private enterprises also play a role in China's defense industrial base.[97] Indeed, the PLA's MCF development strategy emphasizes integrating the capabilities of these civilian sectors into supporting China's military technology development. For these private-sector and university entities, being denied access to US bank accounts or transactions from US persons could pose a significant consequence, impeding access to not just US technologies outright but also business relationships or other financial transfers.

Beyond protecting US technologies, a concerted effort to apply IEEPA sanctions to the private-sector entities supporting China's MCF development strategy could drive a wedge between technology companies, forcing them to choose between access to the US market or supporting MCF—an approach advocated by some analysts.[98] At a minimum, IEEPA sanctions on all companies on the MEU, NS-CMIC, and Entity Lists would seem a reasonable first step. After all, if a company is deemed enough of a national security threat to make it onto those lists in the first place, then the logic should also extend to denying it the full scope of US transactions under IEEPA.

Legal Countermeasures. Entity-based controls also present another challenge, as listed Chinese companies incur material damages, which gives them legal standing to file lawsuits. The discussion of the NS-CMIC List's predecessor, the CCMC List, already identified how Chinese entities successfully pursued cases against the US government, which were likely enabled by process shortcomings in the US government's implementation of the CCMC List.

Yet even a more robust process, such as Commerce's Entity List, has exposed the government to legal cases from Chinese companies. For example, in July 2020, Commerce added 11 Chinese companies to the Entity List because of their involvement in human rights violations against Uyghur Muslims in Xinjiang.[99] One of these companies, Changji Esquel Textile Company, filed a lawsuit a year later in a US district court, seeking relief from economic and reputational damages inflicted by the US government's Entity Listing. As a result of Esquel's lawsuit, the Department of Commerce's End-User Review Committee agreed to conditionally remove it from the Entity List if it met certain conditions.[100] As of October 2021, the company was still working to meet those conditions, while its efforts to seek a preliminary injunction were rejected by a US district judge.[101]

In July, Esquel lost an appeal of the rejection of its preliminary injunction, with the US Court of Appeals for the US District of Columbia ruling that Changji Esquel's claims were not likely to succeed.[102] Although the court ultimately rejected the legal basis of Changji Esquel's lawsuit, the incident nevertheless demonstrates how listed companies can slow or counteract the implementation of US national security

objectives implemented through list-based controls. Esquel argued that the ECRA's authority only allows for Entity Listing to control the release of items for use in proliferation of weapons of mass destruction or conventional weapons, acts of terrorism, other military programs threatening to the United States or its allies, and interference or disruption of critical infrastructure. Human rights violations are not enumerated as a reason to Entity List a company.[103]

ECRA itself states,

> The national security and foreign policy of the United States require that the export, re-export, and in-country transfer of items . . . be controlled for the following purposes . . . to carry out the foreign policy of the United States, including the protection of human rights and the promotion of democracy.[104]

However, when defining the use of the Entity List, ECRA stipulated only military technology–based reasons, not foreign policy or human rights concerns.[105] An authority such as IEEPA, on which the SDN List is based, may avoid similarly exposing the US government to legal arguments on the narrow interpretation of authorities because of the much broader language in IEEPA on what the president can declare constitutes an international emergency.

Even so, one shortcoming of using IEEPA is its own legal fragility stemming from a reliance on presidential declarations of international emergency, which could present opportunities for legal challenges that overturn the emergency itself or even challenge IEEPA's constitutional basis. IEEPA effectively enables the president to designate US persons or companies and block their access to financial resources and the broader US financial system. A US citizen designated under IEEPA is "unable to hold a job or pay rent without OFAC's permission," according to a study by the Brennan Center for Justice. Similarly, a US organization designated under IEEPA is "forced out of existence."[106]

This authority clearly carries significant concerns about constitutionality. Judicial review of the president's use of IEEPA has so far been limited. When the courts have recently reviewed agency decisions under IEEPA powers, it has been against procedural requirements specified under the Administrative Procedures Act (APA). Typically, the courts offer significant deference to the executive branch in its execution of national security powers. With IEEPA authorities, however, there has been one deviation from this trend: the Xiaomi case.

In the Xiaomi case, the court found that DOD failed to meet procedural requirements under the APA by making an "arbitrary and capricious" ruling, because it failed to articulate "substantial evidence" Xiaomi was a CCMC. With respect to the evidence that DOD provided, which focused on Xiaomi's investment in emerging technologies such as 5G and artificial intelligence, the court ruled that evidence alone "cannot be enough to support a conclusion that Xiaomi is a CCMC." The court asserted that supporting the standard of evidence DOD presented for Xiaomi would enable DOD to designate any Chinese company investing in technology with alternative military uses as a CCMC.[107]

While it is of course procedurally sound to require the executive branch to provide such substantial evidence for sanctioning a company supporting China's military modernization, and the Xiaomi case was a repudiation of an incredibly threadbare presentation of evidence on the part of the DOD, it still establishes a precedent for regulating the executive branch's use of sanctions through the APA "arbitrary and capricious" standard. Future legal challenges could overturn sanction designations for which the executive branch provided more evidence than it did in Xiaomi's but which a court nevertheless decides fails to meet the APA standard for substantial evidence. Ultimately, no court has yet established what constitutes substantial evidence for determining a risk of military diversion.

One means to mitigate the risk of legal challenges and provide more flexibility to the executive branch to respond to the diffuse and opaque nature of China's MCF ecosystem would be for Congress to act on its own authority by passing a law to empower the president to impose sanctions against Chinese companies that pose a threat without requiring the president to declare a national emergency. Congress has done so

already for human rights abusers, when it passed the Global Magnitsky Human Rights Accountability Act, which empowered the president to sanction foreign persons and companies involved in human rights abuse without requiring the president to declare a national emergency.[108] It is worth highlighting that Congress did this in 1999 through the CCMC List, though as discussed elsewhere, the language designating entities that could be added to that list was too open-ended to enable effective action, and the investment bans didn't take advantage of the full scope of IEEPA authorities.

Opportunities for Broader Controls

The MEU List, Entity List, NS-CMIC List, and SDN Lists have all, to greater and lesser extents, been brought to bear by the US government to restrict Chinese companies' access to US technology, capital, and financial resources. Across all, additional steps can be taken to employ the lists more effectively. Yet there are diminishing marginal returns for US competitive policy to further use these lists because of a fundamental shortcoming: They are all *lists*.

As has been noted, while China's defense SOEs are relatively few (excluding their many subsidiaries), the network of smaller private firms, universities, and research centers all participating, to various degrees, in China's MCF strategy is much larger. This ecosystem is too large and opaque to make list-based approaches effective alone. Broader approaches that move beyond identifying a bad actor in China have been applied, and expansion of their use should be considered to better insulate US technology from enabling China's military modernization. This next section examines some broader, non-list-based technology controls that have been applied and how their application could be expanded to cover gaps.

FDPR. One of the most well-known of these controls has been the Foreign Direct Product Rule (FDPR), which was first applied in the case of Huawei—the only time it has been applied to a Chinese company. At the time, Commerce had Huawei on its Entity List, curtailing its direct access to US suppliers. However, Huawei was still able to source items—particularly semiconductors—from semiconductor manufacturing fabrication plants outside the United States. These semiconductors were produced with US origin content or using US technology, software, or equipment.[109]

The FDPR existed before US controls on Huawei, specifically as the National Security Foreign Direct Product Rule (NS FDPR). In fact, it was first implemented in its original form in 1959 and set in its current form in 1996.[110] At its core, the NS FDPR applies to a specific set of transactions in which a second country, such as Taiwan, uses US-exported technology or software to produce a good and then seeks to export that foreign-produced "direct product" of US technology to a third country.

However, the application is far more complicated than that. First, the recipient country must be one that Commerce includes in its Group D:1, E:1, or E:2 lists. The D:1, E:1, and E:2 lists include a variety of countries for which the US has national security or terrorism concerns or an embargo. The D:1 specifically includes China. Second, the producing country must be from Commerce's Country Group B list, which broadly includes allies and partners of the US and other countries the US has not listed on D:1, E:1, or E:2 for national security, terrorism, or embargo reasons.[111] Third, the specific technology or software used by the producing country to produce the item for the recipient country must itself be controlled for national security reasons.[112]

National security controls apply to a wide range of semiconductor manufacturing equipment and technology—but not all. This limits the original FDPR's application to semiconductors produced for China in a third country using US equipment or technology. As an example: "Equipment for the manufacturing of semiconductor devices or materials" is classified by ECCN 3B001 and carries a national security control designation. In principle, this would mean products directly produced from this technology would be covered under the FDPR. However, 3B001 is highly specific in scope, not covering all possible semiconductor manufacturing equipment.

For example, extreme ultraviolet lithography tools, the most advanced photolithography tools available—which are required to produce the most advanced chips—are covered. Yet the second-most advanced photolithography tools, argon fluoride (ArF) immersion scanners—required for advanced chips, but not the most advanced chips—are only covered if they produce a pattern with a "minimum resolvable feature" size of 45 nm or less. As a Center for Security and Emerging Technology study found, however, advanced ArF immersion scanners only reach a minimum resolvable feature of 50 nm, thus avoiding national security controls.[113]

More broadly, national security controls such as 3B001 do not apply to a broad range of less advanced semiconductor manufacturing equipment and software, such as wafer manufacturing equipment, etching equipment, and EDA software.[114] The end result is that a foreign company that integrates some US semiconductor manufacturing technology and equipment into its processes may produce items that do not directly rely on the narrow set of national security–controlled technology or equipment, exempting those products from the FDPR. The FDPR also does not distinguish between transactions involving parties that are and are not on the Entity List.[115]

In light of these gaps, Commerce sought to expand the application of the FDPR—but only as it applied to Huawei. Under its rule change, the FDPR encompasses transactions in which a foreign entity that has knowledge an item it produces using US equipment, technology, or components will be exported, reexported, or transferred to Huawei or knows that Huawei will be the ultimate recipient of the item. This was called the "Entity List FDPR," though the only Entity List recipients covered are Huawei affiliates.

The Entity List FDPR covers transactions based on two criteria. First, the type of foreign-produced item must be a direct product of technology or software listed under 16 specific ECCNs.[116] In general, these ECCNs encompass a broad array of software and technology used in semiconductor manufacturing, high-performance computer design and manufacturing, and telecommunications equipment design and manufacturing. Importantly, these ECCNs are not limited to national security–controlled items, expanding the scope of items covered under the FDPR. These ECCNs would likely include ArF lithography equipment, EDA software, and other semiconductor manufacturing equipment and software not controlled for national security reasons.

Second, the foreign-produced item must be exported or used by an entity "with a footnote 1 designation in the license requirement column of the Entity List." The only entities that have such a footnote designation are Huawei-affiliated companies and organizations.[117] Essentially, the FDPR, as implemented, was designed with the specific intent of targeting Huawei's dependencies on foreign-produced semiconductors, which were produced in foundries using technologies covered under those ECCNs.

Although only narrowly applied currently, the FDPR has significant potential as a means of broadly targeting technology exports to China. For example, SIA notes that one more-expanded application of the FDPR would be to require a license for foreign-made items using US technology not controlled for national security reasons subject to the EAR.[118] This would have the same effect that the Entity List FDPR did, by expanding the scope of equipment and technology that triggers it—but increasing that effect beyond Huawei.

ECRA Emerging and Foundational Technologies List. The 2018 ECRA directs Commerce to establish a list of emerging and foundational technologies, which provides an opportunity to tighten controls on US technology from China's collection. As observed by the US-China Economic and Security Review Commission (USCC), there has been a "significant delay" in the Department of Commerce creating this list. In 2018, Commerce published an advance notice of proposed rulemaking to form such an emerging technologies list, listing 14 broad categories of technologies, such as artificial intelligence and biotechnology, and listing 45 more tangible example technologies, such as nanobiology and neural networks.[119] However, Commerce never followed up on this by finalizing an emerging technologies list. It made incremental steps to publish three new sets of ECCNs for items related

to chemical and biological weapons, human and animal pathogens and toxins, and associated equipment, which it designated as emerging technologies.[120]

One of the key challenges in implementing a list for emerging and foundational technologies is technology decomposition: defining a technology and its component elements. For example, Commerce's 2018 advance notice defined nanobiology as an example emerging technology in the biotechnology category. However, nanobiology as a field includes many different component technologies, including nanoscale assemblers, nanoscale medical sensors and devices, and enabling technologies, such as nanomaterials and nanomanufacturing.[121] Decomposing priority technology fields and then determining what component technologies need additional regulations takes effort and requires subject-matter expertise.

The USCC report notes that Commerce can rely on advisory committees to come to a decision but has only minimally used such resources. In 2018, it repurposed the former Emerging Technology and Research Advisory Committee, renaming it the Emerging Technology Technical Advisory Committee, to "focus on the identification of emerging and foundation technologies." USCC reports that as of 2021, the committee had met twice—but without issuing any conclusions or taking follow-on actions.[122]

The consequences of not establishing the ECRA technologies list are significant. It hampers CFIUS's ability to screen foreign acquisition and investment in technologies that could be sensitive. Under FIRRMA, CFIUS was given authority to screen transactions that include investments in any US business by a foreign government if that investment could obtain the "use, development, acquisition, or release of critical technologies." FIRRMA defines critical technologies as any technology in five categories. The first four categories are based in existing regulations: the US Munitions List, the Commerce Control List, nuclear items specified in their own regulations, and agents and toxins specified in their own regulations. The fifth category is any emerging, foundational, or other critical technology controlled as part of Section 818 of FIRRMA, which directs the president to lead an interagency process to identify these technologies. This requirement is mirrored, intentionally, in ECRA.[123]

In other words, ECRA's list of emerging and foundational technologies constitutes one-fifth of CFIUS's review authorities but is so far undefined. Absent this list, a key FIRRMA expansion of CFIUS's review authority remains unexploited, enabling Chinese investment in and access to critical emerging technologies in the United States.

Further, ECRA and FIRRMA direct that once the president has generated this list, Commerce is required to specify the level of controls with respect to these identified technologies. In principle, this is a step forward, as many emerging technologies may not yet be covered under export controls. As a result, companies today may be exporting items to China that are not on Commerce's control list—and so carry no license requirements—but which may eventually be added when a final list is promulgated. Rather than relying on Commerce's efforts alone, there is clearly both a legal obligation and a policy obligation for a White House–led effort to define a list of critical technologies that should be leveraged to establish a national prioritization and unity of effort across the whole of government.

This is not without historic precedent. In the late 1980s, the US government, in response to concern about losing trade competitiveness to Japan and Europe, began wrestling with how to protect and promote critical technologies, leading it then—as it has now—to realize it had to first define "critical technology." Beginning in 1989 and occurring biennially through 1999, the US government provided a biennial National Critical Technologies Report (NCTR) to Congress through the National Critical Technologies Panel.

Based on legislation in the FY1990 NDAA, the panel of 13 government and private-sector experts would deliberate and produce a list of 30 "national critical technologies." For the first and second reports, the CIA provided assessments of foreign capabilities to inform the panel. These lists not only enumerated the technologies but also decomposed the technologies into subareas and specific technologies. For example,

one of the 28 technologies on the 1995 list was information and communication technology components, which included three subareas: high-density data storage, high-definition displays, and high-resolution scanning technologies, each having anywhere from one to seven component technologies.[124]

Efforts to revive this approach began in the last year of the Trump administration, when it released the *National Strategy for Critical and Emerging Technologies*, which enumerated 20 technology areas.[125] This was continued in the Biden administration, which released a C*ritical and Emerging Technologies List Update* that builds on the Trump administration's list by slightly narrowing the field of critical technologies.[126] The updated list also decomposes each technology into key subfields, focusing on core technologies rather than application areas or performance characteristics. For example, advanced computing, which is included in both lists, is decomposed in the updated list into supercomputing, edge computing, cloud computing, data storage, computing architectures, and data processing and analysis techniques.

In this way, the updated list mirrors the older NCTRs. One of the shortcomings of the NCTRs shared by the updated list is that neither mandates action by any federal agency. Indeed, the updated list says specifically that "this list should not be interpreted as a priority list for either policy development or funding."[127] The Biden administration has, in the updated list, a workable starting point for setting the baseline for not just the ECRA Emerging and Foundational Technologies list but also broader interagency priorities, including directing research funding and priorities from research grant–giving agencies. Either the administration or Congress should consider designating the updated list as the core list for FIRRMA and ECRA, tasking Commerce and the Treasury to work out any further details of its implementation as necessary—for example, providing further specificity of a technology or adding other technologies.

Wider Application of the Presumption-of-Denial Standard to National Security–Controlled Items. Items controlled for national security reasons encompass a significant portion of the EAR and include dual-use equipment and technologies. Generally, items that are exclusively military in nature, such as armaments and munitions, are controlled by other, stricter export control regimes. By regulation, an item controlled for national security reasons is one whose export would "make a significant contribution to the military potential of any other country . . . that would prove detrimental to the national security of the United States."[128]

In 2020, Commerce took an important first step to expanding the use of this control by revising its policies on approving or disapproving licenses for exports of national security–controlled items to China.[129] Previously, Commerce had "a general policy of approval" for export licenses to civil end uses and a presumption of denial for license applications that would make a "direct and significant contribution" to China's military capabilities.[130]

The new standard preserves a "general policy of approval" for license applications for "civil end users for civil end uses," which is slightly more specific than the previous civil end use policy of approval. It expands the presumption of denial to any item that would make "a material contribution to the 'development,' 'production,' maintenance, repair, or operation of weapons systems, subsystems, and assemblies."[131] Unfortunately, Commerce does not define "material contribution." Commerce regulations stipulate that factors to be considered in approving the license application of exporting a national security–controlled item to China include "the significance of the item for the weapon systems capabilities of the importing country" and the "involvement of any party to the transaction in military activities, including activities involving the 'development,' 'production,' maintenance, repair, or operation of weapons systems, subsystems, and assemblies."[132]

Bureau of Industry and Security (BIS) documents do not provide a precise picture of the number of license applications for national security–controlled items, but general trends can be observed. First, BIS has reported that it processed 37,985 export license applications in FY2020, a 10.8 percent increase from 34,207 in 2019. Its global FY2020 approval rate was

Table 1. US Approval and Denial Rate of Export License Applications to China

	2016	2017	2018	2019	2020
Denied	55	74	77	130	177
Returned Without Action	494	542	576	613	925
Approved	2,528	2,907	2,910	2,675	2,652
Denial Rate	2%	2%	2%	4%	5%
Approval Rate	82%	83%	82%	78%	71%

Source: Department of Commerce, Office of Technology Evaluation, "U.S. Trade with China," 2020, https://www.bis.doc.gov/index.php/documents/technology-evaluation/ote-data-portal/country-analysis/2735-2020-statistical-analysis-of-u-s-trade-with-china/file.

86 percent.[133] Its approval rate for China was somewhat lower: In 2020, BIS reviewed 3,754 license applications for China, approving 2,652, or 70.6 percent. In that same year, it denied 177 licenses, or a little under 5 percent. As shown in Table 1, BIS statistics indicate its approval rates for China-bound licenses have steadily decreased, while its denial rates have steadily increased.

While BIS does not provide a percentage breakdown on its approved licenses to China for national security–controlled items, it does provide a list of the top 10 approved ECCNs to China for 2020. Of the top 10 ECCNs, five are national security–controlled items, totaling 1,089 licenses—or about two-fifths of the approved licenses.[134] Commerce also provides a list of the top 10 license exports by value, which identifies an additional two national security–controlled ECCNs. All in, these seven identified ECCN categories include aero gas turbine technologies, machine tools, telecommunications technology, microelectronics, and lasers.[135] In principle, any of these ECCNs could make a material contribution to the PLA. Yet licenses for their export were approved, likely because it could not be established that the categories were significant enough, or by some other standard the license was judged to not materially contribute to the PLA.

Fundamentally, the material-contribution standard is open-ended and subject to interpretation, allowing for these license approvals to occur. An exporter could argue that a manufacturing tool does not meet a high enough standard of significance to a civilian SOE that might nevertheless support China's military-industrial complex, even indirectly. Arguably, no such standard could be written that would not be open to interpretation.

The fuzziness of the standard also contributes to a contradiction of policy. By definition, all national security–controlled items that US exporters apply for licenses to export to China should meet the standard of material contribution to China's military, because the definition of a national security–controlled item is one that could make a significant contribution to the military—and should therefore be denied to China. This is obviously not the case, raising the question of whether US policy is contradictory. If a national security–controlled item would *not* make a material contribution to China's military—as presumably would be the case for many licenses approved in 2020—then why is that item controlled? If the item should remain controlled for national security reasons, why can it be exported to China when the US government's stated policy is to not export items that provide a material contribution?

Another example of incongruence in the national security–controlled standard relates to cybersecurity exports. In late 2021, Commerce introduced a "long-awaited" set of export controls for "intrusion software" designed to avoid detection, defeat countermeasures, extract data, modify computer systems or user data, and inject unauthorized code. Although this software is controlled for national security reasons, it can receive a license exception for "legitimate" cybersecurity research and incident

response activities. While this license exception is flatly denied for Cuba, Iran, North Korea, and Syria, it is only denied to "government end users" in Group D countries—including China.[136]

In other words, an exporter can export intrusion software, as defined in Commerce's new controls, without a license to China as long as it is not going to a government end user. Yet members of China's intelligence services have been indicted for establishing front companies with legitimate-sounding names, such as Hainan Xiandun Technology Development Company, to hire hackers and linguists to conduct hacking on China's behalf, targeting the United States and almost a dozen other countries.[137]

Since the Chinese intelligence connection is obfuscated, this license exception would permit any US cybersecurity company to unknowingly export penetration-testing tools—a legitimate cybersecurity function—to China's intelligence front companies and private hackers. Because intelligence services set up these front companies to obfuscate their intelligence affiliation, it is unlikely an exporter would be able to detect the intelligence affiliation through their due diligence means.

The US government should consider reviewing licensing policies for national security–controlled items to close these clear loopholes. The potential contradictions in continued approval of national security–controlled items to China for civil end users for civil purposes demonstrates the need for a reconsideration of whether, if any, exceptions should be made for the export of national security–controlled items. They also point to a need to reconsider whether a national security–controlled item should remain a national security–controlled item.

Continuing with the current approach, in which the US government maintains a list of national security–controlled items defined as making a significant contribution to a country's military counter to the US national interest, but then in which the US government selectively approves licenses because some of these items can be considered to not make such a contribution, appears self-contradictory. Further, the license exceptions for exports of national security–controlled cybersecurity software to China, a country that the Office of the Director of National Intelligence assesses "presents a prolific and effective cyber-espionage threat [and] possesses substantial cyber-attack capabilities," pose clear vulnerabilities to US national interests.[138]

Machine Tools Case Study. Machine tools are a tangible example of how a lack of tighter controls on national security–controlled items enables their continued flow to China. These are national security–controlled items under ECCN 2B001 for machine tools and numerical control units. Recall that in 2020, this ECCN was fifth in total value of approved licenses. As noted earlier, these license approvals likely stem from judgments on individual licenses of these machine tools not providing a material contribution to the PLA.

Whatever the judgments behind individual export license approvals might have been, Chinese sources are clear in emphasizing the importance of machine tools—particularly advanced tools such as CNC machine tools—to China's defense industry.[139] They also identify an existing choke point where China relies on Germany, Japan, and the United States for a significant number of CNC machine tools.[140] One article notes that the self-sufficiency rate for China's CNC machine tool production is less than 10 percent.[141] Other articles state that China's advanced fighter aircraft, including the J-20 stealth fighter,[142] modular naval vessels, and aerospace special materials, all rely on foreign CNC machine tool technology. Indeed, one article claims that Chengdu Aircraft Industry Group purchases top-of-the-line Swiss CNC machine tools and speculates they would be the only ones with the precision necessary to produce the J-20.[143] It can be assumed US-made machine tools are also used to produce materials with the precision necessary for the production of advanced weapon systems.

Since the J-20 is a relatively mature aircraft already in production,[144] production lines have likely already been established and US-made machine tools employed in its production and broader supply chain have likely also already been purchased by Chinese manufacturers. Nevertheless, while the controls in

place today to prevent US-exported items—such as machine tools used to support the production of China's J-20s and future combat aircraft—are stronger than they were several years ago, gaps remain. Chengdu Aircraft Industry Group and its parent company, the Aviation Industry Corporation of China, are large, well-known SOEs, and they are listed on the Entity List and MEU List. Given Chengdu Aircraft Industry Group's role in the production of military aircraft, licenses to it would likely not require a significant burden of proof on the US government to deny, especially since it would be easy to argue that exports of machine tools to the manufacturer of the J-20 would materially contribute to the production of a military system.

That said, a company as large as Chengdu Aircraft Industry Group likely has multiple second- and third-tier parts and materials suppliers. These companies could easily claim to US exporters to be solely civilian aircraft manufacturers in order to receive exports of advanced machine tools, which they could use to manufacture the high-tolerance parts and materials needed to meet demand from Chengdu Aircraft Industry Group or other Chinese companies directly supplying the PLA. As a recent RAND study identified, China's defense industrial base is extremely large and nontransparent, "mak[ing] it extremely difficult to assess the relationships between and among firms inside and outside [it], including SOEs and other types of enterprises and organizations in dual-use sectors."[145]

This risk is likely to grow, as the Chinese government has taken steps to increase the participation of private firms in the defense industrial base by loosening many restrictions and barriers to entry.[146] In parallel, China has ramped down the public messaging behind MCF and will likely seek to increase the opacity surrounding connections between major defense SOEs and smaller, dual-use companies in that supply chain.[147] It is unclear if US end use monitoring could detect this, if these Chinese firms strove to keep the activity hidden.

Altogether, there is a significant gap in the openly available data on how large a problem this is. It is probable that national security–controlled items such as machine tools are being exported to China under licenses approved because there was no evidence the export would provide a material contribution to China's military. It is also clear that China is seeking to broaden the participation of its civilian dual-use manufacturing base, which remains significantly dependent on machine tools, in its defense industrial base. What remains uncertain is the degree to which US-exported manufacturing tools are being used by subcontractors in China's defense industrial base to supply major PLA weapons builders or diverted directly to CMCs.

This case study of machine tools is only one example of a national security–controlled ECCN that continues to flow to China despite the inherent national security implications. Similar threats exist among other national security–controlled items.

The Domestic Impact of Expanding Controls. As Sino-American competition has intensified and the United States has imposed more controls on technology trade with China, there have been negative reactions from industries that prize the market access they are poised to lose from these controls. This concern among industries is especially heightened by the emphasis on dual-use technologies.

In 2021, the US Chamber of Commerce provided a report examining the costs of decoupling, specifically across the aviation, semiconductor, chemical, and medical device industries. It found consistently lost revenues in the tens of billions of dollars, among other deleterious effects. The Chamber of Commerce's estimates usually used worst-case assumptions, such as all China sales revenue of US companies in a specific industry being reduced to zero or complete restrictions on imports from China and retaliatory tariffs from Beijing.

However, even more moderate assumptions are also costly, such as China substituting 50 percent of its replaceable US chip supply over three years, which would result in $36 billion in lost revenue and 40,000 lost jobs.[148] A 2020 Boston Consulting Group report, which produced the $36 billion figure, specifically examined a scenario in which existing Entity List–based restrictions on Chinese companies and other export controls were maintained. In

this scenario, only $8 billion of the $36 billion in lost revenue comes from Entity Listed Chinese companies under export bans replacing their US imports. Boston Consulting Group estimates that $19 billion of lost revenue in this scenario comes from Chinese companies proactively pursuing supplier diversification. Regarding companies on the Entity List, such as Huawei, Boston Consulting Group assessed that about 85–90 percent of their semiconductor demand is replaceable and not reliant on US companies.[149]

As these reports show, calls for tighter controls on China's access to US technology meet with two valid and interrelated arguments: These controls will impose revenue losses on US industry, and the Chinese companies could substitute US goods out of their supply chains. These arguments have merit, but there are counterarguments: The controls' impact may be overestimated, substitution may be harder for China, and substitution may occur independent of any US action.

Although US companies are certain to lose revenue from tighter controls, measuring the scale of that impact on US and Chinese companies can be difficult. For example, the 2020 Boston Consulting Group report assessed that Huawei could handily replace US components in its business segments. However, as of 2021, reduced access to US chips appears to have significantly affected Huawei's smartphone sales and 5G equipment sales and "crippled" its chip design efforts, according to the *Wall Street Journal*.[150] Moreover, the Boston Consulting Group report assumed that all exports to Huawei would be denied, when Commerce data released by the House Foreign Affairs Committee show that Huawei continues to have export licenses approved even after being on the Entity List.[151] To be sure, Huawei's future is uncertain, and its efforts to invest in domestic alternatives to foreign chips could pan out in the next few years.

Returning to the case of national security–controlled items, all licensed US exports to China (not just national security–controlled items) accounted for $478 million in revenue in 2019, or a paltry 0.4 percent of total exports to China.[152] In a macroscopic scale, the loss of these exports is unlikely to have major economic impacts on the United States.

Assessments like Boston Consulting Group's regarding the damage to US companies following US technology controls do not calculate only the revenue loss from prohibited exports but also assume follow-on, relatively seamless substitution by Chinese companies and factor in those costs. This is a legitimate consideration, but it also leads to the second counterargument that this substitution may be harder than anticipated and may nevertheless be happening independent of US action.

Analyses like Boston Consulting Group's assume that Chinese companies could achieve substitution of US imports relatively quickly—two to three years for devices such as smartphones, personal computers, and consumer electronics. As noted earlier, Huawei's experience suggests that this substitution may be harder to execute in practice. Chinese writings, discussed in an earlier section, paint a picture of much deeper, harder-to-rectify dependence on US technology inputs.

However, good data on Chinese companies' ability to substitute US technology are difficult to obtain. That makes these Chinese academic studies a unique "red" perspective, but it will be difficult to predict the controls' actual effect until they are applied. It is unlikely those studies would be showing consistent concern if there was not some merit to it. Overall, Chinese companies will likely face some challenges in substituting US imports, though this bears further research.

China's perceived strategic imperative to substitute out foreign technology inputs is at this point independent of US actions that might tighten or loosen export controls at the margins. As discussed in the first section of this report, Beijing views the United States as its strategic competitor and a fundamental threat to its goal of achieving national rejuvenation by becoming a science and technology world leader. China's motivation to substitute foreign technology is thus not dependent on its perception of the dependability of US firms. It will seek to eliminate dependencies on US technology regardless of how restrictive US export controls may be. Although market forces, such as Chinese firms' perceptions of US firms' reliability, are important, the broader calculus in China is

driven by the state's considerations, which will likely have a greater effect—via the state's control over the economy—in driving decisions by Chinese firms.

Conclusion

The United States and China are locked in strategic competition for composite national power, for which cutting-edge technology is a key enabler across economic and military domains. In response to China's growing technology levels and its whole-of-nation effort to absorb US technology, the US has pursued significant controls on China's commercial access to US technologies.

This report has examined China's strategic approach to technology competition, beyond the oft-discussed topics of technology transfer. It identified how China is pursuing a whole-of-nation strategic effort to achieve political, economic, and social modernity by expanding composite national power to achieve "the great rejuvenation of the Chinese nation."[153] China's strategists believe that the country's ability to win in its competition with the United States is directly based on its ability to marshal the full scope of its society and resources in support of military and development goals.

This report identified how Chinese sources reveal a deep concern over being cut off from access to Western technology. Despite some major successes in China's science and technology development, these Chinese sources still see significant exploitable dependence on the United States for high technology. In the context of China's broader view of its rivalry with the United States, Beijing will elevate the goal of eliminating its dependencies on US technology far above the business logic of whether it is efficient or cost-effective to do so.

In recent years, US technology-control efforts have emphasized entity-based controls, which specify, via lists, Chinese entities for which certain actions are prohibited. This provides some ability to protect US technology from exploitation. These controls rely on identifying a company or person supporting China's military modernization to establish the prohibitions on transactions or exports to that entity. The Department of Commerce has significantly expanded the number of Chinese entities on its Entity List while also establishing the MEU and MIEU lists. In addition, Treasury has established the NS-CMIC List and sparingly used the SDN List. These entity-based lists share similar shortcomings in their ability to prevent US technology from enabling China's military: an inability to address the scale of China's military modernization because of their whack-a-mole approach, a to-date policy approach that prioritizes fine-tuning rather than maximizing restrictions, and vulnerabilities to legal remedies from listed entities.

Beyond just the application of entity-based controls, this report has examined broader approaches that move beyond identifying a bad actor in China, and it has looked at how expansion of their use should be considered to better insulate US technology from enabling China's military modernization. The FDPR provides a tool to expand the scope of export controls on a company listed on the Entity List. Establishing the Emerging and Foundational Technologies List is also a crucial step to enabling CFIUS to fully employ its FIRRMA authorities while also enabling Commerce to regulate new and emerging technologies. Finally, the continued approval of licenses for the export of national security–controlled technologies to China indicates that there remains opportunity to either revise controls on those technologies or more aggressively deny the transfer of technologies with the inherent potential of making a significant contribution to China's military.

Finally, this report examined counterarguments from US industries against the costs of tightening China's access to US technology, as US companies are poised to lose market access and sales that generate the revenue needed to support the research and development of leading-edge technologies. Tightening controls on US technologies can also result in Chinese companies pursuing foreign substitutes, if they exist. However, the impact of technology controls applied so far may be overestimated, and concerns regarding the ability of Chinese firms to substitute US technology inputs appear to

contradict Chinese writings that are seriously concerned with a specific and hard-to-mitigate dependence on US technologies.

Ultimately, China's motivation to substitute foreign technology is not only dependent on its perception of the dependability of US firms in light of export controls. Because Beijing views the United States as a strategic competitor, it will seek to eliminate dependencies on US technology regardless of how restrictive US export controls may be.

Old Wine in New Bottles

PEOPLE'S LIBERATION ARMY SYSTEM DESTRUCTION WARFARE AND AMERICAN STRATEGIC-BOMBING THOUGHT

Christian Curriden

Since the military airplane first saw widespread use in World War I, its promises and possibilities have enamored technologically minded strategists. Why, they asked, should soldiers toil in the muck and blood of a draining war of attrition (as was so dramatically illustrated on the stalemated Western Front) when airborne bombers could simply bypass all that inefficient carnage to directly attack the cities, factories, governments, and people those soldiers were meant to protect?

These airpower enthusiasts had their differences, but generally they agreed on three fundamental principles: (1) The enemy was best seen as a system or network of distinct, interdependent nodes, which together functioned to support a war effort; (2) this system depended on a relatively small number of key nodes—which they termed "centers of gravity"—whose destruction or disruption could cause the whole system to become paralyzed and unable to continue resistance, even though much of its physical structure and fielded military forces remained intact; and (3) there was no effective way to defend these key nodes from aerial bombardment.

This report begins by briefly describing the ideas of these early airpower advocates. It then traces the evolution of these ideas, focusing on how new technologies and conflicts reshaped them. Next, it argues that these theories have been taken up by Chinese military thinkers, who in their advocacy of systems warfare have in many ways inherited the American airpower tradition. Finally, it discusses some of the criticisms of airpower theory and analyzes some of the ways in which new technologies and the US and Chinese militaries' unique characteristics may make those criticisms more or less valid.

The Airpower Prophets

As with most new technologies, powered flight was put to military use soon after its advent. By the end of World War I, all major Western military powers had flying corps and at least some experience with military aviation. For many, especially on the German and Russian general staffs, this experience reinforced the role of the airplane, alongside artillery or tanks, as an important tool for any land-based army trying to destroy another in the field.[154] Others, however, took a more expansive view.

One of the first pioneers was Italian Gen. Giulio Douhet. He argued that chaining air forces to naval or ground formations would be worse than a waste.[155] Instead, they should be allowed to operate independently, flying over both friendly and enemy troops to directly attack enemy cities. In thus bringing the battlefield directly to the civilians normally protected by the state's armies, he believed that an air force could cause so much suffering that the public would rise up and demand an end to the war, forcing the enemy to capitulate even if its army had not been defeated.[156]

Moreover, Douhet believed there was no effective defense to such an attack. Bombers could hide anywhere in the vast three-dimensional space over a country's territory. Even if enemy fighters could somehow locate these intruders, they likely would not be able to reliably launch, climb to meet the threat, and then have sufficient fuel to fend off enemy bombers before the bombers had dropped their payloads.[157]

Others offered a somewhat more nuanced view. Hugh Trenchard, the "Father of the [Royal Air Force]," argued that an enemy army in the field could be paralyzed if the factories and transportation it relied on for war matériel were destroyed.[158] In an analogy that would echo across decades and continents, Maj. Gen. J. F. C. Fuller claimed that the enemy could be seen as an integrated system, not unlike an organism. Like an organism, the whole system depended on a relatively small number of essential faculties. Destroying these would be like shooting an organism in the brain; though its limbs remained intact, they would be useless.[159] Others made similar analogies, comparing enemy war economies to watches whose operation could be disrupted by the destruction of a few key gears.[160] Brig. Gen. Billy Mitchell, one of the key luminaries of the future American Air Force, helped popularize these views in the United States.[161]

These theorists had their differences, but they generally agreed on several key points. Enemy nations could be viewed as large systems.[162] These systems depended on a relatively small number of identifiable nerve centers—or centers of gravity—the destruction of which would paralyze the whole.[163] Airpower allowed a state to bypass the armies and navies states had traditionally used to defend these centers of gravity—and destroy the centers directly.[164] Furthermore, these strategic bomber attacks would prove much less costly than a traditional military assault and be nearly impossible for the enemy nation to defend against.[165]

In World War II, these propositions were tested. The United States and Britain built large forces of highly advanced long-range bombers and convened councils of economists and other scholars to identify the German war economy's centers of gravity.[166] Massive raids were launched to destroy these carefully selected targets. The results were mixed. Heavy attrition showed that modern fighters and air defense systems could mount an effective defense against bomber attacks.[167] The German military was weakened by these raids' economic damage and the need to divert forces to defend against them, but it was not defeated until allied ground troops invaded Germany itself.[168] Despite these mixed results, many airpower advocates declared the war proof that their theories could work. The extent to which World War II validated these theories remains a hotly debated topic to this day.[169]

Since World War II, several explanations have been advanced for the failure of airpower alone to cause German capitulation. Douhet's ideas that terror bombing could force a change in policy via popular uprising have been generally discredited.[170] When subjected to bombardment, civilian populations have tended to become more apathetic than angry, and dictators have been found able to maintain power and continue to pursue aggressive policies despite great unpopularity.[171]

Attempts to paralyze the German economy faced a number of unforeseen obstacles as well. Perhaps the greatest was the difficulty of identifying critical centers of gravity without which the German war economy could not function.[172] War economies do not generally have clear breaking points, and they tend to be surprisingly resilient, able to adapt to compensate for damage inflicted from the air.[173] That said, the campaign presented many difficulties for the German high command, and some have argued that the use of airpower could have been more decisive had allied planners done a better job of choosing their targets—for example, by focusing more of their efforts on the German transportation system.[174]

A Prophecy Fulfilled?

Following World War II, debates regarding strategic airpower shifted their focus from which pinpricks could bring down an enemy system to nuclear deterrence and the finer technical problems of nuclear warfighting.[175] The Vietnam War was a major blow to airpower's prestige as a tool of national policy, and it wasn't until the 1980s that American airpower theorists began to return to the questions posed by Douhet and the other interwar airpower theorists.

In many ways, Col. John Warden (ret.) is the modern successor to Douhet, Mitchell, and Trenchard.[176] In his research and work helping plan the 1991 American air campaign against Iraq, he sought to resurrect many of the ideas that birthed the US Air Force as an independent institution with a unique and decisive mission separate from merely supporting ground troops or delivering nuclear weapons.

Like those early thinkers, he has argued that an enemy can be thought of as a system, that this system will depend on a relatively small number of critical centers of gravity, and that airpower can be used to reliably destroy these nodes, thus paralyzing the enemy system.[177] Like his predecessors, he has argued that this can be achieved and a war's political objectives attained without the need to destroy all or even most of an enemy's military in the field.[178]

He also agrees with the interwar airpower theorists on the crucial role of new technology in making this possible, though for him the technology was not the airplane itself so much as stealth aircraft and precision-guided munitions, which enabled a relatively small number of aircraft to penetrate most air defenses and strike a large number of targets simultaneously in a way that the lumbering air forces of World War II or the Vietnam War generally could not.[179] In particular, Warden emphasizes the need for attacks on as many centers of gravity as possible in parallel (i.e., simultaneously as opposed to in sequence) to prevent the enemy system from adapting to accommodate the damage.[180]

Warden also disagrees with his predecessors on some important points. First of all, he rejects Douhet's notion that bombing could defeat an enemy by causing its population to rise up against its government.[181] On the contrary, Warden argues that the ability of strategic bombing to paralyze and defeat an enemy while causing them minimal damage is an advantage. If the enemy government remains in place, this will give less reason for it to resent the victor, and if the enemy government is deposed, it will make rebuilding easier.[182] While he emphasizes the singular usefulness of air strikes to affect enemy centers of gravity, he recognizes that sometimes they are not the best tool for this. No need to use a bomb if a bribe will do the trick more efficiently.[183]

Furthermore, Warden has adopted a broader view of airpower than did his predecessors, including any guided flying object, regardless of which service launches it.[184] In some ways, this broader definition anticipated China's reliance on long-range conventionally armed ballistic missiles to achieve many of the strategic strike missions that the US would generally conduct by aircraft.

Perhaps Warden's most unique contribution is his suggestion of a novel method to identify centers of gravity in the enemy system. Based on the activities that any enemy must undertake to launch major military operations, Warden argues that any enemy system can be divided into five rings.[185] From the innermost and most crucial to the outermost and least crucial, these are the enemy's (1) leadership, (2) processes (institutions or mechanisms to transform energy or effort from one form into another, such as communications, food, manufacturing, and recruitment), (3) infrastructure, (4) population, and (5) fielded forces.[186]

The central rings (leadership and processes) have fewer and more important targets.[187] As long as a system's inner rings remain intact, an enemy can usually effectively reconstitute any damage done to its fielded forces.[188] If analyzing the enemy system along these lines does not reveal centers of gravity that can be effectively destroyed or disrupted, then one can take the analysis one step further, recursively dividing each of the five rings into its own set of five rings (e.g., the leadership, processes, infrastructure, population, and fielded forces of the overall societal leadership).[189] While Warden generally argues that a strategist should focus on the broader national system, should strikes on the enemy military become necessary, he believes that militaries and even individual military formations can also be broken down into five rings to identify centers of gravity.[190]

He goes on to suggest that the number of centers of gravity may be relatively small. While planning the Gulf War air offensive, he famously claimed that striking a list of 84 strategic targets, mostly communications centers in Iraq that allowed Saddam Hussein and other Iraqi leaders to stay in contact with their fielded forces and government, would bring the country to its knees.[191] More recently, he has suggested that even a large nation-state, such as the United States or China, could be subdued by the destruction of "considerably less than a thousand"

targets.[192] While this would seem a considerable target list, it pales in comparison to the number of targets that would need to be destroyed to significantly attrite the fielded forces of such a large country's military.[193]

As with their predecessors, Warden and other modern advocates of strategic airpower have been able to test their theories on the battlefield. The defeat of Saddam, it was believed, demonstrated the fragility of national war-making capacity and its vulnerability to strategic strike.[194] The 1999 US-led air war against Yugoslavia was, if anything, more decisive, because airpower appeared to achieve NATO's strategic aims without needing to involve ground forces directly in the conflict.[195] At last, it seemed, the promises of the interwar airpower theorists had been realized; strategic airpower, without any significant ground forces, seemed to have played a decisive role in winning a war without needing the expenditure of great sums of blood or treasure, or even the destruction of the enemy army.

The New Disciples

Across the Pacific, the Chinese People's Liberation Army (PLA) took notice. For decades, the PLA had a relatively ambivalent view toward new technology. While it engaged in periodic modernization campaigns, it generally held to the Maoist and guerilla-centric view that war is a predominantly human endeavor and that its primary objective is the destruction of the enemy army's "vital strength" on the battlefield.[196]

The American wars of the 1990s and early 2000s, however, displayed a better way to wage war. PLA analysts believed that American strategic strikes on the Iraqi government were so decisive that they rendered air attacks on Saddam's forces in Kuwait almost superfluous and that the Kosovo conflict drove this point home when Yugoslavia was defeated even though most of its army remained intact.[197] These American conflicts showed that in the future, wars would not be decided by human-centric battles between armies but by firepower-centric confrontations between advanced systems.[198]

Throughout the 2000s and early 2010s, the PLA digested these lessons, and by the early 2010s, it had developed a theory of "systems confrontation."[199] Like Warden and the interwar airpower theorists, this theory emphasized the need to see every nation and military as a system of nodes and connectors and war as a contest between rival systems.[200] It further postulates that these sprawling systems are dependent on a much smaller number of critical nodes and connections, the destruction or disruption of which can paralyze the whole even though most of the system remains intact.[201] The key to victory is to find and strike these critical nodes and connections.[202]

Following Warden's lead, PLA thinkers have argued that the fact that this can be achieved without greatly damaging fielded forces is a feature, not a bug; by paralyzing an enemy with minimal death and destruction, the Chinese Communist Party (CCP) can achieve its political goals while reducing the risks of escalation.[203] PLA thinkers have described this sort of conflict as "target-centric warfare," and they have claimed it is key in the prosecution of modern war.[204]

There are some differences between the PLA's theory of systems confrontation and the airpower theories of Douhet, Trenchard, Warden, and other American airpower enthusiasts. First, the PLA emphasizes jointness and integration in all military operations.[205] Airpower is only one of the many ways to attack nodes and connections in an enemy system, and PLA writings frequently extol the virtue of combining "hard" air and missile strikes with "soft" electromagnetic attacks and cyberattacks.[206] This is, however, a difference in emphasis more than kind—and one that has narrowed over time. And while Warden repeatedly extolled airpower's unique advantage in striking enemy centers of gravity, he also recognized that other tools could be used against them, but PLA writings often emphasize the particular importance of long-range strikes or direct disruption in a commander's tool kit for striking an enemy system.[207]

Perhaps a bigger difference is the PLA's greater emphasis on using this systems approach to paralyze and defeat an enemy's fielded forces rather than disabling the enemy nation-state as a whole. It's true that PLA writings describe an enemy's military

"operational system" as part of a larger national "war system," which includes economic, diplomatic, and political centers of gravity that could be targets of strategic attack.[208] That said, much of the PLA's discussion of systems confrontation revolves around characterizing the enemy military as a system, identifying its key nodes, and finding ways to destroy or disrupt it to paralyze the enemy's fielded forces.[209] In this emphasis, the PLA in some ways mirrors Warden's critics in its objectives, even if its methods are similar to those that American airpower activists would recommend.

Perhaps most significantly, the PLA has shown scant interest in Warden's five rings theory for identifying an enemy system's key targets. It is unsurprising that this should be an area of divergence; while American airpower advocates have long agreed on the existence of enemy systems' centers of gravity that can be destroyed with long-range bombardment, identifying these centers has always proven difficult and contentious.[210]

Instead of Warden's five rings or Trenchard's focus on economic targets, PLA theorists tend to emphasize the importance of information for operational systems to function, and they seek "information dominance," or the ability to amass real-time data on battlefield conditions and the enemy system while denying it to the adversary.[211] While forces and matériel must be moved and employed within an enemy system, its true lifeblood is information, whether intelligence, commands, statuses, or other data, and any part of the system that becomes cut off from this flow of information will be rendered inert, no matter how powerful its material capabilities.[212]

While publicly available sources do not generally go into detail about which targets to strike (perhaps because the PLA has classified these more specific discussions), they almost certainly include command centers, communications nodes, data links, data centers, and intelligence, surveillance, and reconnaissance platforms—any facilities or units that gather, analyze, or disseminate information through the operational system.[213]

Even this difference, however, is not as great as it might appear. While the PLA does not seem to have accepted Warden's five rings model for national war-making systems, the target lists generated by their information-centric model are probably similar to those that would be generated by a five rings analysis. Most would be within what Warden would consider the leadership and especially the processes rings, which he suggested is where one is likely to find the enemy's most important centers of gravity.[214]

Furthermore, both Warden's five rings and the PLA's quest for information dominance share a fundamental assumption: Target selection should be based on not only the value of the targets themselves but the ways in which striking them will affect the whole enemy system.[215] More broadly, all the theorists discussed here more or less agree that the enemy is best seen as a system or network of distinct, interdependent nodes, which together function to support a war effort, and that this system depends on a relatively small number of key nodes—or centers of gravity—whose destruction or disruption could paralyze the whole system, leaving it unable to continue resistance even though much of its physical structure and fielded military forces remain intact. In their emphasis on integrating hard and soft kill attacks, the Chinese (and to a lesser extent Warden) expand on the interwar airpower theorists' assertion that airpower is decisive in destroying these centers of gravity, but all are agreed that the centers are fundamentally vulnerable to long-range enemy attacks.

The Heretics

Chinese military doctrine drafters clearly read American military doctrine and make frequent references to it. It is surprising, therefore, that they do not often reference Warden or his five rings theory, given how much of their work mirrors his. This is not to say there is no discussion of Warden, but it is not as prominent as the discussion of other thinkers, such as Douhet or even Warden's near contemporary John Boyd.[216] Furthermore, there does not seem to be much critical discussion of Warden's many critics.[217]

While Warden and many other advocates of strategic airpower saw the wars in Iraq and Yugoslavia

during the 1990s as decisive proof that strategic airpower could be independently decisive, others have questioned these claims. Perhaps the most vocal of these skeptics has been Robert Pape, whose 1996 book *Bombing to Win: Air Power and Coercion in War* called into question the value of air strikes carried out independently of ground operations.[218] The skeptics argue that in Iraq, Warden's strategic campaign against regime and command and communications targets around Baghdad was largely ineffectual: Saddam was still able to effectively communicate with and send orders to his forces.[219] Airpower in this conflict was important, but the skeptics of strategic airpower contend that it was most useful when employed against the Iraqi forces in Kuwait, especially in punishing their attempt to withdraw from the country.[220] Other skeptics argue that despite a belief at the time that the Iraqi military was a formidable fighting force, it was in fact so weak relative to the American and allied powers that any strategy used against it was likely to be effective, and so it cannot be used as evidence for any particular approach.[221]

The 1999 Yugoslavia conflict presents a more difficult case for the skeptics because ground forces played such a limited role. Some have argued that the presence of American artillery-spotting radar on the ground in neighboring Albania was decisive and that without at least a small ground element, air forces are unable to effectively find their targets.[222] Others have argued that the threat of a NATO ground offensive, not the air campaign, was the decisive factor.[223] Some have also pointed to the international isolation of Serbian leaders at the time, European sanctions, and domestic Serbian politics as factors just as decisive as airpower.[224] Both sides have amassed evidence, and the debate continues.

More fundamentally, many have come to criticize some of the basic assumptions of Warden's (and the PLA's) work on systems paralysis. For many, while an enemy force or nation can indeed be viewed as a complex system, in practice such systems tend to be much more resilient than Warden or the PLA suggest. They believe that the number of centers of gravity could be much greater than either American or Chinese proponents of airpower recognize and that systems can adapt much more quickly than Warden or the PLA give them credit for.[225] Even seemingly highly centralized dictatorships can require a certain degree of decentralization, creating more centers of gravity than expected for those seeking a small number of critical nodes in their leadership or processes that connect the leadership to the government and military.[226]

While few contest the PLA's assertion that information is key to modern warfare and must be able to flow throughout a system, airpower skeptics take exception to the PLA's insistence that modern operational systems cannot function without high-bandwidth communications and data centers, arguing that many command functions can be accomplished with low-tech, low-bandwidth, intermittent communications.[227]

The same can be true of other essential system functions. In one example, the British in World War II adapted to German strikes on their radars by using a highly integrated system of human observers and fighter direction centers.[228] Some have suggested that with a concerted effort, units operating in range of enemy sensors and weapons could use a variety of low-tech methods to maintain communications links, including wired communications and even couriers.[229]

Even in the face of an American airborne onslaught focused explicitly on cutting communications links, Saddam and the Iraqi central command were able to receive information from their units in the field and send orders to their forces in Kuwait to retreat. While those retreating forces were devastated from the air, and American air superiority blinded Iraq to American redeployments in Saudi Arabia, the Iraqi strategic command system was still able to maintain enough functionality to absorb new information and act accordingly.[230] This particular criticism may apply more to the PLA's obsession with information links than Warden's broader set of potential targets, but broader national economies can also prove surprisingly resilient.[231]

A closely linked criticism is that American and European airpower enthusiasts (and, by extension, the PLA) do not sufficiently recognize the enemy's

ability to react and adapt, reducing it to a passive set of targets unable to respond to an air campaign.[232] Warden in particular argued that technology has enabled such widespread simultaneous attacks that traditional notions of action and reaction are outdated.[233] While the PLA tends to at least pay lip service to the need to take enemy reactions into account, it too insists that if a PLA firepower strike campaign is carried out with sufficient ferocity against an enemy's key targets, that enemy will be largely powerless to resist, at least for a time.[234]

Others, both in the US and China, have pointed out that there are active, creative ways enemies can make their systems more resilient in the face of long-range precision strikes.[235] Chinese writers have pointed out the ability of ground commanders to take advantage of urban and other complex terrain to avoid the precision firepower of their enemies.[236] The United States is already increasing the autonomy of lower-level commanders to operate independently if communications or logistical links with higher echelons are severed.[237] Efforts are also underway to improve the resiliency of long-range communications in the face of enemy disruption.[238] Many of these efforts involve units in the field using on-site computing power to determine what information needs to be shared and thus avoid the need for high-bandwidth, uninterrupted connections.[239]

Pape and his adherents are not skeptical of airpower per se, but unlike Warden, they feel that it is best used in close coordination with ground forces to destroy enemy fielded forces, especially when the enemy seeks to maneuver or reinforce them.[240] By savaging the enemy army in the field (an activity Warden considers to generally be a fool's errand), Pape argues that one can destroy an enemy's confidence in its ability to achieve its goals, thus leading it to give up the struggle.[241]

In some ways, on this issue, the PLA may actually side with Pape against Warden. While Chinese strategists clearly believe that an enemy force can be paralyzed with pinpoint strikes on a relatively small number of key targets, they are relatively agnostic on whether one uses such strikes to disable an enemy military or the broader enemy state, and much of their work seems to focus more on fielded forces than on broader national systems.[242]

Prophecy of Things to Come?

Despite efforts to improve resilience, there is reason to suspect that the United States' military (the "strong enemy" the PLA is thinking about how to defeat) may be especially susceptible to paralysis through target-centric warfare. China is much closer to most battlefields on which the PLA is likely to face the United States, and the need for American forces to travel long distances may make the US more vulnerable to long-range attacks on its limited number of bases, fleet of capital ships, and supply lanes.[243]

America's penchant for high-tech weapons platforms may make it more reliant on electronic communications than are other militaries.[244] Many also fear that the United States has become too dependent on large, fixed command facilities and air bases, which could create concentrated centers of gravity for the Chinese to strike.[245] The United States is aware of these problems and working to address them, but only time will tell if it will succeed.

From Douhet to Warden to the PLA, each generation of airpower advocates has generally felt that new technology has improved the US military's ability to paralyze an enemy system though firepower strikes. The PLA has invested heavily in several new technologies that may prove just as decisive as military aviation, stealth, and precision-guided weapons.[246] In particular, it hopes that the ability of artificial intelligence to gather and analyze large volumes of data may finally solve the long-standing problem of identifying and finding centers of gravity.[247] Many of the PLA's artificial intelligence–related purchases have been of systems meant to disrupt command systems and data links.[248]

Perhaps drone swarms, autonomous analysis of satellite images, the proliferation of battlefield robots, and other "intelligentized" technologies will finally make the battlefield perfectly legible and silence the airpower skeptics.[249] That said, if new technologies' long history of affecting warfare has

taught us anything, it is the difficulty of predicting their effects.

Conclusion: How China Will Fight

This report cannot take a decisive stand on the decades-old debate about the ability of pinpoint strikes on a relatively small number of targets to disable a nation or military while the majority of its forces remain intact but impotent. Even NATO's ability to defeat Yugoslavia in 1999 without ground combat has failed to render a final verdict on the issue. What historical evidence we have is from conflicts between the most advanced militaries in the world and relatively small, totally isolated adversaries. The great-power wars of the past happened without many of the key technologies that Warden and the PLA consider decisive in enabling systems confrontation. Until a full-scale conflict between technologically advanced militaries occurs, we are unlikely to know for certain whether Warden and the PLA are correct. Hopefully, such a conflict never occurs.

What this report can do is point out that the PLA seems to have firmly taken the side of airpower advocates over skeptics. They parrot the most stable assertions of Mitchell, Trenchard, Warden, and others in arguing that enemies can be characterized as a system of interconnected nodes, that such a system depends on a relatively small number of centers of gravity whose disruption can paralyze the whole, and that this disruption can be achieved with long-range effects, without the need for a Clausewitzian clash of armies.

Not only that, but they add to this body of work in important ways, offering new and innovative answers to the vexing problem of target selection with their theories of information dominance. They also hint at a possible synthesis of Pape's and Warden's seemingly antagonistic ideas, suggesting that pinpoint precision strikes can be used to so disable an enemy system that the enemy loses confidence in its ability to win the conflict, thus achieving Pape's ideal of denial. The Chinese have been incorporating American military doctrinal debates into their thinking on war. Perhaps it is time the US does the same to the Chinese. It might learn something.

Identifying these theoretical roots of China's systems confrontation doctrine also helps us understand how the Chinese military sees the world—and how it is likely to fight. We can be confident that, like the Allied Economic Objectives Unit of World War II or Warden's Air Force planners in the Gulf War, Chinese operational planners are scouring the American military for centers of gravity—key facilities or individuals without which the force cannot function. In particular, they will be looking for communications centers, computing centers, command centers, and logistical facilities. They are likely confident that destroying or disrupting a relatively small list of these targets will render the enemy unable to resist. The PLA may also be de-emphasizing strikes on most individual combat platforms, though they are less skeptical of the value of attacking opposing militaries than are their American counterparts, and in practice few militaries can resist the temptation to blow up the fielded fighters, tanks, and ships of their opponents.[250]

Knowing this, American planners can begin to prepare a response. Efforts are already underway to render the American command system's centers of gravity more numerous and protected. This knowledge may also help American planners understand the Chinese system's centers of gravity. The Chinese will consider the gathering, transmission, and analysis of information to be crucial, because, whether or not they are correct, they are convinced that information is the crucial factor in modern warfare. Even if they are wrong, disrupting their ability to gather information on our own operational systems and demonstrating our ability to interfere with the transmission of information in theirs could seriously shake their confidence. In doing so, we would ironically be treading the ground that the Chinese themselves have surveyed, seeking for operational denial through strategic strikes.

Notes

1. Chris Buckley and Paul Mozur, "What Keeps Xi Jinping Awake at Night," *New York Times*, May 11, 2018, https://www.nytimes.com/2018/05/11/world/asia/xi-jinping-china-national-security.html.

2. Wei Sheng, "China Spends More Importing Semiconductors Than Oil," Technode, April 29, 2021, https://technode.com/2021/04/29/china-spends-more-importing-semiconductors-than-oil.

3. Karen M. Sutter, *China's New Semiconductor Policies: Issues for Congress*, Congressional Research Service, April 20, 2021, https://www.everycrsreport.com/files/2021-04-20_R46767_2cd34407ee3ff126834038a7035fe41896fbe13b.pdf.

4. Semiconductor Industry Association, "Taking Stock of China's Semiconductor Industry," July 13, 2021, https://www.semiconductors.org.

5. Rush Doshi, *The Long Game: China's Grand Strategy to Displace American Order* (New York: Oxford University Press, 2021), 73.

6. Julian Baird Gewirtz, "China's Long March to Technological Supremacy," *Foreign Affairs*, August 27, 2019, https://www.foreignaffairs.com/articles/china/2019-08-27/chinas-long-march-technological-supremacy.

7. Buckley and Mozur, "What Keeps Xi Jinping Awake at Night."

8. Rush Doshi, "The United States, China, and the Contest for the Fourth Industrial Revolution," testimony before the Subcommittee on Security, Committee on Commerce, Science, and Transportation, US Senate, July 30, 2020, https://www.commerce.senate.gov/services/files/6880BBA6-2AF0-4A43-8D32-6774E069B53E. Doshi references Xi Jinping's speeches and writings. *Qiushi*, "Di Sici Gongyegeming shenmeyang? Xi Jinping Zheyang Miaohui Lantu," [What Is the Fourth Industrial Revolution? Xi Jinping Described the Blueprint Like This!], July 27, 2018; and *People's Daily*, "Xi Jinping Shunying Shidai Chaoliu, Shixian Gongtong Fazhan" [Xi Jinping: Follow the Trend of the Times and Achieve Common Development], July 26, 2018, http://cpc.people.com.cn/n1/2018/0726/c64094-30170246.html.

9. Contrary to conventional wisdom, the US may actually be pulling far ahead in actual national wealth, as the Federal Reserve counts it. National wealth is a better measure of a nation's assets and resources than is gross domestic product, which measures the value of annual transactions. Derek Scissors, "Is the US Economy Pulling Away from China's?," AEIdeas, October 22, 2019, https://www.aei.org/foreign-and-defense-policy/is-the-us-economy-pulling-away-from-chinas.

10. White House, *National Security Strategy of the United States of America*, December 2017, https://trumpwhitehouse.archives.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf.

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

12. Constitution of the Communist Party of China: Revised and Adopted at the 19th National Congress of the Communist Party of China on October 24, 2017, http://www.xinhuanet.com/english/download/Constitution_of_the_Communist_Party_of_China.pdf.

13. US Department of Defense, Office of the Secretary of Defense, *Military and Security Developments Involving the People's Republic of China*, 2020, https://media.defense.gov/2020/Sep/01/2002488689/-1/-1/1/2020-DOD-CHINA-MILITARY-POWER-REPORT-FINAL.PDF.

14. Constitution of the Communist Party of China.

15. US Department of Defense, Office of the Secretary of Defense, *Military and Security Developments Involving the People's Republic of China*.

16. Alex Stone and Peter Wood, *China's Military-Civil Fusion Strategy*, Air University, China Aerospace Studies Institute, June 15, 2020, https://www.airuniversity.af.edu/CASI/Display/Article/2217101/chinas-military-civil-fusion-strategy.

17. US Department of Defense, Office of the Secretary of Defense, *Military and Security Developments Involving the People's Republic of China*.

18. Ben Murphy et al., trans., "Xi Jinping: 'Strive to Become the World's Primary Center for Science and High Ground for Innovation,'" DigiChina, March 18, 2021, https://digichina.stanford.edu/work/xi-jinping-strive-to-become-the-worlds-primary-center-for-

science-and-high-ground-for-innovation.

19. Yang Biqin and Lai Yanting, "Zhōng měi màoyì mócā duì zhōngguó jíchéng diànlù jìn chūkǒu de yǐngxiǎng jí fāzhǎn duìcè" [The Influence of Sino-US Trade Friction on China's Integrated Circuit Import and Export and Development Countermeasures], *Journal of Inner Mongolia University of Finance and Economics* 19, no. 6: 99–105, https://www.cnki.com.cn/Article/CJFDTotal-NMCJ202106026.htm.

20. Yang and Lai, "Zhōng měi màoyì mócā duì zhōngguó jíchéng diànlù jìn chūkǒu de yǐngxiǎng jí fāzhǎn duìcè" [The Influence of Sino-US Trade Friction on China's Integrated Circuit Import and Export and Development Countermeasures].

21. Yang and Lai, "Zhōng měi màoyì mócā duì zhōngguó jíchéng diànlù jìn chūkǒu de yǐngxiǎng jí fāzhǎn duìcè" [The Influence of Sino-US Trade Friction on China's Integrated Circuit Import and Export and Development Countermeasures].

22. Josh Ye, "US-China Tech War: Top Chinese University Pulls Report That Concluded China Would Suffer More from Tech Decoupling with US," *South China Morning Post*, February 4, 2022, https://www.scmp.com/tech/tech-war/article/3165846/us-china-tech-war-top-chinese-university-pulls-report-concluded-china.

23. Peking University, Institute of International and Strategic Studies, "U.S.-China Strategic Competition in Technology: Analysis and Prospects," January 2022, https://uscnpm.org/2022/02/06/pku-iiss-2022-report-tech-competition.

24. Peking University, Institute of International and Strategic Studies, "U.S.-China Strategic Competition in Technology: Analysis and Prospects."

25. Lin Wangqun et al., "Túpò měi duì huá xìnxī yǔ tōngxìn jìshù fēngsuǒ de sīkǎo" [Reflections on Countermeasures to Break Through the Blockade of Information and Communication Technology], *National Defense Technology* 41, no. 3 (June 2020): 57–61, https://www.cnki.com.cn/Article/CJFDTotal-GFCK202003011.htm.

26. Lin et al., "Túpò měi duì huá xìnxī yǔ tōngxìn jìshù fēngsuǒ de sīkǎo" [Reflections on Countermeasures to Break Through the Blockade of Information and Communication Technology].

27. US Department of Commerce, Bureau of Industry and Security, "Entity List," https://www.bis.doc.gov/index.php/policy-guidance/lists-of-parties-of-concern/entity-list.

28. Mollie D. Sitkowski and Qiusi Y. Newcom, "Commerce Department Adds 33 Chinese Entities and Research Institutions to Entity List, Citing Military Ties and Human Rights Violations," Faegre Drinker Biddle & Reath, May 26, 2020, https://www.faegredrinker.com/en/insights/publications/2020/5/commerce-department-adds-another-33-chinese-entities-and-research-institutions-to-the-entity-list.

29. Daniel Andreeff, Lise S. Test, and Paul Amberg, "US Government Adds Five Chinese Entities Associated with Supercomputer Development to Entity List," Sanctions & Export Controls Update, June 27, 2019, https://sanctionsnews.bakermckenzie.com/us-government-adds-five-chinese-entities-associated-with-supercomputer-development-to-entity-list.

30. Elina Teplinsky, Anne Leidich, and Aaron R. Hutman, "Four China Nuclear Industry Companies Added to 'Entity List,'" Pillsbury Insights, August 15, 2019, https://www.pillsburylaw.com/en/news-and-insights/china-industry-entity-list.html.

31. US Department of Commerce, Bureau of Industry and Security, "Addition of Entities to the Entity List, Revision of Certain Entries on the Entity List," *Federal Register* 85, no. 109 (June 5, 2020): 34495, https://www.federalregister.gov/documents/2020/06/05/2020-10869/addition-of-entities-to-the-entity-list-revision-of-certain-entries-on-the-entity-list.

32. US Department of Commerce, "Commerce Department to Add Nine Chinese Entities Related to Human Rights Abuses in the Xinjiang Uighur Autonomous Region to the Entity List," press release, May 22, 2020, https://2017-2021.commerce.gov/news/press-releases/2020/05/commerce-department-add-nine-chinese-entities-related-human-rights.html.

33. US Department of Commerce, "Commerce Department Adds 24 Chinese Companies to the Entity List for Helping Build Military Islands in the South China Sea," press release, August 26, 2020, https://2017-2021.commerce.gov/news/press-releases/2020/08/commerce-department-adds-24-chinese-companies-entity-list-helping-build.html.

34. US Department of Commerce, "Commerce Adds China's SMIC to the Entity List, Restricting Access to Key Enabling U.S. Technology," press release, December 18, 2020, https://2017-2021.commerce.gov/news/press-releases/2020/12/commerce-adds-chinas-smic-entity-list-restricting-access-key-enabling.html.

35. US Department of Commerce, "Commerce Adds China National Offshore Oil Corporation to the Entity List and Skyrizon to the Military End-User List," press release, January 14, 2021, https://2017-2021.commerce.gov/news/press-releases/2021/01/commerce-adds-china-national-offshore-oil-corporation-entity-list-and.html.

36. US Department of Commerce, "Commerce Lists Entities Involved in the Support of PRC Military Quantum Computing Applications, Pakistani Nuclear and Missile Proliferation, and Russia's Military," press release, November 24, 2021, https://www.commerce.gov/news/press-releases/2021/11/commerce-lists-entities-involved-support-prc-military-quantum-computing.

37. US Department of Commerce, "Commerce Acts to Deter Misuse of Biotechnology, Other U.S. Technologies by the People's Republic of China to Support Surveillance and Military Modernization That Threaten National Security," press release, December 16, 2021, https://www.commerce.gov/news/press-releases/2021/12/commerce-acts-deter-misuse-biotechnology-other-us-technologies-peoples.

38. US Department of Commerce, "U.S. Department of Commerce Adds 28 Chinese Organizations to Its Entity List," press release, October 7, 2019, https://2017-2021.commerce.gov/news/press-releases/2019/10/us-department-commerce-adds-28-chinese-organizations-its-entity-list.html.

39. US Department of Commerce, Bureau of Industry and Security, "Addition of Entities to the Entity List," *Federal Register* 84, no. 98 (May 21, 2019): 22961, https://www.federalregister.gov/documents/2019/05/21/2019-10616/addition-of-entities-to-the-entity-list.

40. US Department of Commerce, Bureau of Industry and Security, "Addition of Entities to the Entity List."

41. Lin et al., "Túpò měi duì huá xìnxī yǔ tōngxìn jìshù fēngsuǒ de sīkǎo" [Reflections on Countermeasures to Break Through the Blockade of Information and Communication Technology], 57–61.

42. 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.

43. US Department of Commerce, Bureau of Industry and Security, "Revisions and Clarification of Export and Reexport Controls for the People's Republic of China (PRC); New Authorization Validated End-User; Revision of Import Certificate and PRC End-User Statement Requirements," *Federal Register* 72, no. 117 (June 19, 2007): 33646, https://www.federalregister.gov/documents/2007/06/19/E7-11588/revisions-and-clarification-of-export-and-reexport-controls-for-the-peoples-republic-of-china-prc.

44. US Department of Commerce, Bureau of Industry and Security, "Frequently Asked Questions: Expansion of Export, Reexport, and Transfer (In-Country) Controls for Military End Use or Military End Users in the People's Republic of China, Russia, or Venezuela. Final Rule. (85 FR 23459) (April 28, 2020)," https://web.archive.org/web/20200811145623/https://www.bis.doc.gov/index.php/documents/pdfs/2566-2020-meu-faq/file.

45. US Department of Commerce, Bureau of Industry and Security, "Restrictions on Certain 'Military End Use' or 'Military End User' in Belarus, Burma, Cambodia, the People's Republic of China, the Russian Federation, or Venezuela.," *Federal Register* 87, no. 45 (March 8, 2022): 13059, https://www.federalregister.gov/documents/2022/03/08/2022-04819/imposition-of-sanctions-against-belarus-under-the-export-administration-regulations-ear.

46. US Department of Commerce, Bureau of Industry and Security, "Frequently Asked Questions."

47. US Department of Commerce, Bureau of Industry and Security, "Addition of 'Military End User' (MEU) List to the Export Administration Regulations and Addition of Entities to the MEU List," *Federal Register* 85, no. 247 (December 23, 2020): 83793, https://www.federalregister.gov/documents/2020/12/23/2020-28052/addition-of-military-end-user-meu-list-to-the-export-administration-regulations-and-addition-of.

48. US Department of Commerce, Bureau of Industry and Security, "Expansion of Certain End-Use and End-User Controls and Controls on Specific Activities of U.S. Persons," *Federal Register* 86, no. 10 (January 15, 2021): 4865, https://www.federalregister.gov/documents/2021/01/15/2021-00977/expansion-of-certain-end-use-and-end-user-controls-and-controls-on-specific-activities-of-us-persons.

49. US Department of Commerce, Bureau of Industry and Security, "Expansion of Certain End-Use and End-User Controls and Controls on Specific Activities of U.S. Persons; Corrections; and Burma Sanctions," *Federal Register* 86, no. 67 (April 9, 2021): 18433, https://www.federalregister.gov/documents/2021/04/09/2021-07357/expansion-of-certain-end-use-and-end-user-controls-and-controls-on-specific-activities-of-us-persons.

50. See John Costello and Joe McReynolds, "China's Strategic Support Force: A Force for a New Era," in *Chairman Xi Remakes the PLA: Assessing Chinese Military Reforms,* ed. Phillip C. Saunders et al. (Washington, DC: National Defense University Press, 2019),

437–515.

51. Strom Thurmond National Defense Authorization Act for Fiscal Year 1999, Pub. L. No. 105-261 (October 17, 1998).

52. Strom Thurmond National Defense Authorization Act for Fiscal Year 1999, Pub. L. No. 105-261.

53. Christopher A. Casey et al., *The International Emergency Economic Powers Act: Origins, Evolution, and Use*, Congressional Research Service, July 14, 2020, https://sgp.fas.org/crs/natsec/R45618.pdf.

54. Ronald W. Reagan National Defense Authorization Act for Fiscal Year 2005, Pub. L. No. 108-375 (October 28, 2004).

55. Jordan Brunner, "Communist Chinese Military Companies and Section 1237: A Primer," Lawfare, March 22, 2021, https://www.lawfareblog.com/communist-chinese-military-companies-and-section-1237-primer.

56. US Department of Defense, "Qualifying Entities Prepared in Response to Section 1237 of the National Defense Authorization Act for Fiscal Year 1999 (Public Law 105-261)," August 28, 2020, https://media.defense.gov/2020/Aug/28/2002486689/-1/-1/1/LINK_1_1237_TRANCHE-23_QUALIFYING_ENTITIES.PDF.

57. US Department of Defense, "Qualifying Entities Prepared in Response to Section 1237 of the National Defense Authorization Act for Fiscal Year 1999 (Public Law 105-261)."

58. Executive Office of the President, "Executive Order 13959 of November 12, 2020: Addressing the Threat from Securities Investments That Finance Communist Chinese Military Companies," *Federal Register* 85, no. 222 (November 17, 2020): 73185, https://home.treasury.gov/system/files/126/13959.pdf.

59. Cari Stinebower, "Biden Amends EO 13959, Removes Several Previously Designated Chinese Military Companies, and Designates 59 Chinese Companies as Chinese Military-Industrial Complex Companies," Winston & Strawn, June 4, 2021, https://www.winston.com/en/global-trade-and-foreign-policy-insights/biden-amends-eo-13959-removes-eight-sanctioned-entities-and-designates-59-chinese-companies-as-chinese-military-industrial-complex-companies.html.

60. US Department of the Treasury, "Frequently Asked Questions: 857. Do the Prohibitions in Executive Order (E.O.) 13959, as Amended, Apply to Purchases or Sales of Publicly Traded Securities of Subsidiaries of Entities Listed on the Non-SDN Chinese Military-Industrial Complex Companies List (the 'NS-CMIC List')," June 3, 2021, https://home.treasury.gov/policy-issues/financial-sanctions/faqs/857.

61. William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, Pub. L. No. 116-283 (January 1, 2021).

62. US Department of Defense, "DOD Releases List of Chinese Military Companies in Accordance with Section 1260H of the National Defense Authorization Act for Fiscal Year 2021," press release, June 3, 2021, https://www.defense.gov/News/Releases/release/article/2645126/dod-releases-list-of-chinese-military-companies-in-accordance-with-section-1260.

63. US Department of Defense, Office of the Under Secretary of Defense (Acquisition and Sustainment), "Notice of the Removal of the Designation as Communist Chinese Military Companies Under the Strom Thurmond NDAA for FY99," *Federal Register* 86, no. 121 (June 28, 2021): 33994, https://www.federalregister.gov/documents/2021/06/28/2021-13755/notice-of-the-removal-of-the-designation-as-communist-chinese-military-companies-under-the-strom.

64. Nelson Dong et al., "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 & Whitney, June 10, 2021, https://www.dorsey.com/newsresources/publications/client-alerts/2021/06/new-list-of-chinese-military-companies.

65. Catherine Pan-Giordano et al., "U.S. Court Blocks Trump-Era Trading Ban on Xiaomi Stock," Dorsey & Whitney, March 26, 2021, https://www.dorsey.com/newsresources/publications/client-alerts/2021/03/us-court-blocks-trump-era-trading-ban.

66. Luokung Technology, "Luokung Announces Removal from Executive Order List, Favorable Conclusion of Department of Defense Designation Matter," Cision PR Newswire, June 15, 2021, https://www.prnewswire.com/news-releases/luokung-announces-removal-from-executive-order-list-favorable-conclusion-of-department-of-defense-designation-matter-301312082.html.

67. US Department of State, "CAATSA Section 231: 'Addition of 33 Entities and Individuals to the List of Specified Persons and Imposition of Sanctions on the Equipment Development Department,'" press release, September 20, 2018, https://2017-2021.state.gov/caatsa-section-231-addition-of-33-entities-and-individuals-to-the-list-of-specified-persons-and-imposition-of-sanctions-on-the-equipment-development-department/index.html.

68. State Council Information Office of the People's Republic of China, "China's National Defense in the New Era," Foreign Lan-

guages Press, July 24, 2019, https://www.andrewerickson.com/2019/07/full-text-of-defense-white-paper-chinas-national-defense-in-the-new-era-english-chinese-versions.

69. Executive Office of the President, "Executive Order 13936 of July 14, 2020: The President's Executive Order on Hong Kong Normalization," *Federal Register* 85, no. 138 (July 17, 2020): 43413, https://www.federalregister.gov/documents/2020/07/17/2020-15646/the-presidents-executive-order-on-hong-kong-normalization.

70. US Department of the Treasury, "Treasury Sanctions Chinese Entity and Officials Pursuant to Global Magnitsky Human Rights Accountability Act," press release, July 9, 2020, https://home.treasury.gov/news/press-releases/sm1055.

71. Executive Office of the President, "Executive Order 13694 of April 1, 2015: Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities," *Federal Register* 80, no. 63 (April 2, 2015): 18077, https://home.treasury.gov/system/files/126/cyber_eo.pdf.

72. Executive Office of the President, "Executive Order 13757 of December 28, 2016: Taking Additional Steps to Address the National Emergency with Respect to Significant Malicious Cyber-Enabled Activities," *Federal Register* 82, no. 1 (January 3, 2017): 1, https://home.treasury.gov/system/files/126/cyber2_eo.pdf.

73. Executive Office of the President, "Executive Order on Securing the United States Bulk-Power System," May 1, 2020, https://trumpwhitehouse.archives.gov/presidential-actions/executive-order-securing-united-states-bulk-power-system.

74. Executive Office of the President, "Executive Order 14017 of February 24, 2021: America's Supply Chains," *Federal Register* 86, no. 38 (March 1, 2021): 11849, https://www.federalregister.gov/documents/2021/03/01/2021-04280/americas-supply-chains.

75. Iran Times International, "Playing Whack-A-Mole, US Sanctions Another 10.," December 10, 2010, https://www.thefreelibrary.com/Playing+whack-a-mole%2C+US+sanctions+another+10.-a0245037276; and Scott Snyder, "How North Korea Evades UN Sanctions Through International 'Front' Companies," *Forbes*, March 3, 2017, https://www.forbes.com/sites/scottasnyder/2017/03/03/how-north-korea-evades-un-sanctions-through-international-front-companies.

76. 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.

77. Stone and Wood, *China's Military-Civil Fusion Strategy*, 61.

78. US Department of Commerce, Bureau of Industry and Security, "Supplement No. 4 to Part 744—Entity List," 2022, https://www.bis.doc.gov/index.php/documents/regulations-docs/2326-supplement-no-4-to-part-744-entity-list-4/file.

79. Stone and Wood, *China's Military-Civil Fusion Strategy*, 65.

80. US Department of the Treasury, "Consolidated Sanctions List (Non-SDN Lists)," June 2, 2022, https://home.treasury.gov/policy-issues/financial-sanctions/consolidated-sanctions-list-non-sdn-lists.

81. US Department of Commerce, Bureau of Industry and Security, "Supplement No. 7 to Part 744—'Military End-User' (MEU) List," February 24, 2022, https://www.bis.doc.gov/index.php/documents/regulations-docs/2714-supplement-no-7-to-part-744-military-end-user-meu-list/file.

82. Ryan Fedasiuk, Jennifer Melot, and Ben Murphy, *Harnessed Lightning: How the Chinese Military Is Adopting Artificial Intelligence*, Georgetown University, Center for Security and Emerging Technology, October 2021, 34, https://cset.georgetown.edu/publication/harnessed-lightning.

83. Mark Stokes, *China's Evolving Conventional Strategic Strike Capability: The Anti-Ship Ballistic Missile Challenge to U.S. Maritime Operations in the Western Pacific and Beyond*, Project 2049 Institute, September 14, 2009, 113, https://project2049.net/wp-content/uploads/2018/06/chinese_anti_ship_ballistic_missile_asbm.pdf.

84. Fedasiuk, Melot, and Murphy, *Harnessed Lightning*, 34.

85. Fedasiuk, Melot, and Murphy, *Harnessed Lightning*, 35.

86. US Department of Commerce, Bureau of Industry and Security, "Addition of Entities to the Entity List, Revision of Entry on the Entity List, and Removal of Entities from the Entity List," *Federal Register* 85, no. 246 (December 22, 2020): 83416, https://www.federalregister.gov/documents/2020/12/22/2020-28031/addition-of-entities-to-the-entity-list-revision-of-entry-on-the-entity-list-and-removal-of-entities.

87. *China Daily*, "Hefei-Developed Novel Coronavirus Test Kits Certified by EU," March 30, 2020, http://hefeihightech.chinadaily.

com.cn/2020-03/30/c_467677.htm.

88. US Department of Commerce, Bureau of Industry and Security, "Addition of Entities to the Entity List, Revision of Entry on the Entity List, and Removal of Entities from the Entity List."

89. Robert Castellano, "SMIC Is Closing the Gap with Industry Leaders Despite U.S. Sanctions," Seeking Alpha, August 11, 2021, https://seekingalpha.com/article/4448061-smic-closing-gap-with-industry-leaders-despite-us-sanctions.

90. Anton Shilov, "China's SMIC to Build a GigaFab for $8.87B: An Answer to the Shortages," AnandTech, September 6, 2021, https://www.anandtech.com/show/16931/china-smic-build-gigafab.

91. Ramish Zafar, "SMIC to Set Up $12 Billion Plant in Shanghai, China for Sub-14nm Chip Nodes," Where Consumers Come First Tech, https://wccftech.com/smic-to-set-up-12-billion-plant-in-shanghai-china-for-sub-14nm-chip-nodes.

92. Defense Advanced Research Projects Agency, "A DARPA Approach to Trusted Microelectronics," https://web.archive.org/web/20210308031008/https://www.darpa.mil/attachments/Background_FINAL3.pdf.

93. Network Information Military-Civil Integration, "Wáng shā fēi yuànshì: Réngōng zhìnéng yǔ diàncí pínpǔ zhàn" [Academic Wang Shafei: Artificial Intelligence and Electromagnetic Spectrum Warfare], February 22, 2018, https://web.archive.org/web/20190423014956/http://www.81it.com/2018/0222/8552.html.

94. See Swagath Venkataramani et al., "Efficient AI System Design with Cross-Layer Approximate Computing," *Proceedings of the IEEE* 108, no. 12 (2020): 2232–50, https://ieeexplore.ieee.org/document/9253640; and Synopsys, "What is an AI Accelerator?," https://www.synopsys.com/ai/what-is-an-ai-accelerator.html.

95. US Department of Commerce, Bureau of Industry and Security, "Export Control Licensing Decisions for SMIC (November 9, 2020–April 20, 2021)," https://gop-foreignaffairs.house.gov/wp-content/uploads/2021/10/SMIC-Licensing-Information.pdf; and Republican Foreign Affairs Committee, "McCaul Brings Transparency to Tech Transferred to Blacklisted Chinese Companies," press release, October 21, 2021, https://gop-foreignaffairs.house.gov/press-release/mccaul-brings-transparency-to-tech-transferred-to-blacklisted-chinese-companies.

96. *Global Times*, "SMIC Reportedly Gets US License to Purchase Chip-Making Equipment," March 2, 2021, https://www.globaltimes.cn/page/202103/1217089.shtml.

97. Fedasiuk, Melot, and Murphy, *Harnessed Lightning*, 22; and Marcel Angliviel de la Beaumelle, Benjamin Spevack, and Devin Thorne, *Open Arms: Evaluating Global Exposure to China's Defense-Industrial Base*, Center for Advanced Defense Studies, 2019, 21, https://static1.squarespace.com/static/566ef8b4d8af107232d5358a/t/5d95fb48a0bfc672d825e346/1570110297719/Open+Arms.pdf.

98. Elsa B. Kania and Lorand Laskai, "A Sharper Approach to China's Military-Civil Fusion Strategy Begins by Dispelling Myths," Defense One, February 4, 2021, https://www.defenseone.com/ideas/2021/02/sharper-approach-chinas-military-civil-fusion-strategy-begins-dispelling-myths/171854.

99. US Department of Commerce, "Commerce Department Adds Eleven Chinese Entities Implicated in Human Rights Abuses in Xinjiang to the Entity List," press release, July 20, 2020, https://2017-2021.commerce.gov/news/press-releases/2020/07/commerce-department-adds-eleven-chinese-entities-implicated-human.html.

100. Esquel Group, "Esquel Group Resumes Litigation Against U.S. Department of Commerce," August 28, 2021, https://www.esquel.com/news/esquel-group-resumes-litigation-against-us-department-commerce.

101. Jodi Xu Klein, "US Judge Rejects Esquel Group's Request to Remove Xinjiang Unit from 'Entity List,'" *South China Morning Post*, October 8, 2021, https://www.scmp.com/news/china/article/3151575/us-judge-rejects-esquel-groups-request-remove-xinjiang-unit-entity-list.

102. Jacob Kopnick, "DC Circuit Rejects Hong Kong Textile Co.'s 'Hail Mary' Injunction Bid Against Placement on Entity List," Trade Law Daily, July 20, 2022, https://tradelawdaily.com/news/2022/07/20/DC-Circuit-Rejects-Hong-Kong-Textile-Cos-Hail-Mary-Injunction-Bid-Against-Placement-on-Entity-List-2207190055.

103. United States District Court for the District of Columbia, "Complaint for Declaratory and Injunctive Relief," July 6, 2021, https://www.thefashionlaw.com/wp-content/uploads/2021/07/gov.uscourts.dcd_.233078.1.0.pdf.

104. Before 2018, the Entity List was not codified into law directly. Rather, it grew out of a 1996 National Security Council decision to develop a list of entities through what was called the "is informed" process. The Export Administration Regulations contain multiple

"is informed" provisions allowing the Department of Commerce to inform parties that, based on US national security or foreign policy interests, a license is required to export an item. Since February 1997, Commerce published the Entity List to identify businesses, organizations, and companies involved in proliferation activities, initially related to missile technology and weapons of mass destruction. See Kevin J. Wolf et al., "The Export Control Reform Act of 2018 and Possible New Controls on Emerging and Foundational Technologies," Akin Gump Strauss Hauer & Feld, September 12, 2018, https://www.akingump.com/en/news-insights/the-export-control-reform-act-of-2018-and-possible-new-controls.html; and US Department of Commerce, Bureau of Industry and Security, "BIS Annual Report—FY 1998," US Department of Commerce, Bureau of Industry and Security, April 28, 2014, https://www.bis.doc.gov/index.php/documents/policy-guidance/928-bis-annual-report-fy-1998.

105. US House of Representatives, Office of the Law Revision Counsel, "Chapter 58—Export Control Reform," https://uscode.house.gov/view.xhtml?path=/prelim@title50/chapter58&edition=prelim.

106. Andrew Boyle, *Checking the President's Sanctions Powers: A Proposal to Reform the International Emergency Economic Powers Act*, Brennan Center for Justice, June 10, 2021, 12, https://www.brennancenter.org/sites/default/files/2021-06/BCJ-128%20IEEPA%20report.pdf.

107. Bailey Williams, "*Xiaomi Corporation v. U.S. Department of Defense*: Defending the International Emergency Economic Powers Act," *Duke Journal of Constitutional Law & Public Policy* 17 (April 15, 2022): 353–55, https://scholarship.law.duke.edu/djclpp_sidebar/217.

108. Global Magnitsky Human Rights Accountability Act, 20 U.S.C. 2656 (2016).

109. Charles L. Capito 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.

110. Shiva Aminian et al., "US Government Clarifies, Reorganizes and Renames Descriptions of How Foreign-Produced Items Outside the United States Are Subject to US Export Controls as the US Contemplates New Restrictions on Russia," Akin Gump Strauss Hauer & Feld, February 9, 2022, https://www.jdsupra.com/legalnews/us-government-clarifies-reorganizes-and-3057179.

111. US Department of Commerce, Bureau of Industry and Security, "Country Group A," June 2, 2022, https://www.bis.doc.gov/index.php/documents/regulations-docs/2255-supplement-no-1-to-part-740-country-groups-1/file.

112. Department of Commerce, Bureau of Export Administration, "§ 740.6 Technology and Software Under Restriction (TSR)," *Federal Register* 61, no. 234 (December 4, 1996): 64275, https://www.govinfo.gov/content/pkg/FR-1996-12-04/pdf/96-30502.pdf; and Department of Commerce, Bureau of Industry and Security, "§ 740.6 [Amended]," *Federal Register* 80, no. 140 (July 22, 2015): 43318, https://www.govinfo.gov/content/pkg/FR-2015-07-22/pdf/2015-17981.pdf#page=5. See also Technology and Software Under Restriction (TSR), 15 C.F.R. § 740.6, https://www.law.cornell.edu/cfr/text/15/740.6.

113. Saif M. Khan, *U.S. Semiconductor Exports to China: Current Policies and Trends*, Georgetown University, Center for Security and Emerging Technology, October 2020, 27, https://cset.georgetown.edu/wp-content/uploads/U.S.-Semiconductor-Exports-to-China-Current-Policies-and-Trends.pdf.

114. Khan, *U.S. Semiconductor Exports to China*, 9.

115. Tamer A. Soliman et al., "The Long(er) Arm of US Export Controls: US Moves to Close 'Loophole' in Latest Bid to Hamper Huawei's Access to Supply of Chipsets," Mayer Brown, May 18, 2020, https://www.mayerbrown.com/en/perspectives-events/publications/2020/05/huaweis-supply-chain-faces-new-challenges-with-us-governments-proposed-rule-further-restricting-access-to-us-technology-and-software.

116. US Department of Commerce, "Part 734: Scope of the Export Administration Regulations," June 2, 2022, https://www.bis.doc.gov/index.php/documents/regulations-docs/2382-part-734-scope-of-the-export-administration-regulations-1/file.

117. US Department of Commerce, Bureau of Industry and Security, "Supplement No. 4 to Part 744—Entity List."

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

119. US Department of Commerce, Bureau of Industry and Security, "Review of Controls for Certain Emerging Technologies," *Fed-*

eral Register 83, no. 223 (November 19, 2018): 58201, https://www.federalregister.gov/documents/2018/11/19/2018-25221/review-of-controls-forcertain-emerging-technologies.

120. US Department of Commerce, Bureau of Industry and Security, "Implementation of the February 2020 Australia Group Intersessional Decisions: Addition of Certain Rigid-Walled, Single-Use Cultivation Chambers and Precursor Chemicals to the Commerce Control List," *Federal Register* 85, no. 117 (June 17, 2020): 36483, http://www.federalregister.gov/documents/2020/06/17/2020-11625/implementationof-the-february-2020-australia-group-intersessional-decisions-addition-of-certain.

121. Stephen J. Ridge, "A Regulatory Framework for Nanotechnology" (master's thesis, Naval Postgraduate School, March 2018), https://www.hsdl.org/?view&did=811314.

122. Emma Rafaelof, "Unfinished Business: Export Control and Foreign Investment Reforms," US-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.

123. US House of Representatives, Office of the Law Revision Counsel, "Chapter 58—Export Control Reform."

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

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

126. Executive Office of the President, National Science and Technology Council, Fast Track Action Subcommittee on Critical and Emerging Technologies, *Critical and Emerging Technologies List Update*, February 2022, https://www.whitehouse.gov/wp-content/uploads/2022/02/02-2022-Critical-and-Emerging-Technologies-List-Update.pdf.

127. Executive Office of the President, National Science and Technology Council, Fast Track Action Subcommittee on Critical and Emerging Technologies, *Critical and Emerging Technologies List Update*.

128. Department of Commerce, Bureau of Industry and Security, "§ 742.4 National Security," *Federal Register* 72, no. 117 (June 19, 2007): 33656, https://www.govinfo.gov/content/pkg/FR-2007-06-19/pdf/E7-11588.pdf#page=11. See also National Security, 15 C.F.R. § 742.4, March 8, 2022, https://www.law.cornell.edu/cfr/text/15/742.4.

129. US Department of Commerce, Bureau of Industry and Security, "Amendments to National Security License Review Policy Under the Export Administration Regulations," *Federal Register* 85, no. 210 (October 29, 2020): 68448–50, https://www.federalregister.gov/documents/2020/10/29/2020-23962/amendments-to-national-security-license-review-policy-under-the-export-administration-regulations.

130. National Security, 15 C.F.R. § 742.4.

131. US Department of Commerce, Bureau of Industry and Security, "Amendments to National Security License Review Policy Under the Export Administration Regulations."

132. National Security, 15 C.F.R. § 742.4.

133. US Department of Commerce, Bureau of Industry and Security, *Fiscal Year 2022 President's Budget Submission*, 2021, https://www.commerce.gov/sites/default/files/2021-06/fy2022_bis_congressional_budget_justification.pdf.

134. This number includes deemed exports.

135. US Department of Commerce, Office of Technology Evaluation, "U.S. Trade with China," 2020, https://www.bis.doc.gov/index.php/documents/technology-evaluation/ote-data-portal/country-analysis/2735-2020-statistical-analysis-of-u-s-trade-with-china/file.

136. Richard L. Matheny III et al., "Commerce to Impose Long-Anticipated Export Controls on Cybersecurity Items," Goodwin, November 8, 2021, https://www.goodwinlaw.com/publications/2021/11/11_08-commerce-to-impose-long-anticipated-export.

137. US Department of Justice, "Four Chinese Nationals Working with the Ministry of State Security Charged with Global Computer Intrusion Campaign Targeting Intellectual Property and Confidential Business Information, Including Infectious Disease Research," press release, July 19, 2021, https://www.justice.gov/opa/pr/four-chinese-nationals-working-ministry-state-security-charged-global-computer-intrusion.

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

139. Ace Arsenal, "Zhōngguó jīchuáng rúcǐ luòhòu, wèihé jūngōng fāzhǎn néng shíxiàn jǐngpēn shì fā zhǎn? Yōushì zài nǎlǐ?" [China's Machine Tools Are So Backward, Why Can the Development of the Military Industry Achieve a Blowout Development? Where Are the Advantages?], QQ, https://xw.qq.com/cmsid/20201228A0A8AQ00.

140. Eastday, "Zhōngguó zhòngduō jūnyòng jìshù wèihé yīlài rì měi shùkòng jīchuáng? Yuányīn pùguāng guórén xū jiābèi nǔlì" [Why Do Many Military Technologies in China Rely on Japanese and American CNC Machine Tools? The Reasons Exposed Chinese People Need to Redouble Their Efforts], April 8, 2016, http://listen.eastday.com/node2/node3/n403/u1ai587048_t92.html.

141. Xunpeng Technology, "Zhōngguó yīlài jìnkǒu de 20 zhǒng chǎnpǐn, bāokuò gāoduān shùkòng jīchuáng!" [China Relies on Imports for 20 Products, Including High-End CNC Machine Tools!], Wuxi Xunpeng CNC Equipment, October 8, 2020, https://web.archive.org/web/20210513153030/https://www.wxxpkj.com/news/zixun/289.html.

142. Wudu Yilian Industry Research Center, "Wǒguó zhòngxíng shùkòng jīchuáng fāzhǎn xùnsù, dàn gāodàng chǎnpǐn réng bèi guówài lǒngduàn!" [My Country's Heavy-Duty CNC Machine Tools Are Developing Rapidly, but High-End Products Are Still Monopolized by Foreign Countries!], Chenghua CNC Machine Tools Exhibition, September 2, 2021, http://www.cmtexpo.com/cz/news_view.asp?id=412.

143. Pratic, "Zhōngguó wǔdài jī lǐngxiān F22 de mìjué: Yǐnrù guówài cnc jīchuáng, dǎzào 'róuxìng shēngchǎnxiàn'" [The Secret of China's Fifth-Generation Machine Leading F22: Introducing Foreign CNC Machine Tools to Create a "Flexible Production Line"], April 30, 2021, https://www.pratic-cnc.com/xingyedongtai/273.html.

144. Reuben F. Johnson, "China's J-20 Fifth-Gen Fighter Moves into Series Production," Jane's 360, October 26, 2017, https://web.archive.org/web/20171029091958/http://www.janes.com:80/article/75232/china-s-j-20-fifth-gen-fighter-moves-into-series-production.

145. Cortney Weinbaum et al., *Assessing Systemic Strengths and Vulnerabilities of China's Defense Industrial Base with a Repeatable Methodology for Other Countries* (Santa Monica, CA: RAND Corporation, 2022), https://www.rand.org/pubs/research_reports/RRA930-1.html.

146. Angliviel de la Beaumelle, Spevack, and Thorne, *Open Arms*, 29.

147. Matt Ho, "Has China Gone into Stealth Mode with Its Military-Civil Fusion Plans?," *South China Morning Post*, June 5, 2020, https://www.scmp.com/news/china/military/article/3087785/has-china-gone-stealth-mode-its-military-civil-fusion-plans.

148. US Chamber of Commerce, China Center and Rhodium Group, *Understanding U.S.-China Decoupling: Macro Trends and Industry Impacts*, 2021, https://www.uschamber.com/assets/archived/images/024001_us_china_decoupling_report_fin.pdf.

149. Antonia Varas and Raj Varadarajan, *How Restrictions to Trade with China Could End US Leadership in Semiconductors*, Boston Consulting Group, 2020, https://media-publications.bcg.com/flash/2020-03-07-How-Restrictions-to-Trade-with-China-Could-End-US-Semiconductor-Leadership.pdf.

150. Dan Strumpf, "Huawei Pours Money into China's Chipmaking Ambitions," *Wall Street Journal*, January 10, 2022, https://www.wsj.com/articles/hungry-for-chips-huawei-invests-in-chinese-companies-that-make-them-11641819638.

151. Republican House Foreign Affairs Committee, "McCaul Brings Transparency to Tech Transferred to Blacklisted Chinese Companies," press release, October 21, 2021, https://gop-foreignaffairs.house.gov/press-release/mccaul-brings-transparency-to-tech-transferred-to-blacklisted-chinese-companies.

152. US Department of Commerce, Office of Technology Evaluation, "U.S. Trade with China."

153. Constitution of the Communist Party of China.

154. Peter R. Faber, "Paradigm Lost: Airpower Theory and Its Historical Struggles," in *Airpower Reborn: The Strategic Concepts of John Warden and John Boyd*, ed. John Andreas Olsen (Annapolis, MD: Naval Institute Press, 2015), 29–30.

155. David R. Mets, *The Air Campaign: John Warden and the Classical Airpower Theorists* (Maxwell Air Force Base, AL: Air University Press, 1998), 15, https://apps.dtic.mil/sti/pdfs/ADA358677.pdf.

156. Faber, "Paradigm Lost," 18.

157. Mets, *The Air Campaign*, 15.

158. David S. Fadok, *John Boyd and John Warden: Air Power's Quest for Strategic Paralysis* (Maxwell Air Force Base, AL: Air University Press, 1995), 5–11, https://media.defense.gov/2017/Dec/27/2001861508/-1/-1/0/T_0029_FADOK_BOYD_AND_WARDEN.PDF.

159. Fadok, *John Boyd and John Warden*, 6.

160. Faber, "Paradigm Lost," 20.
161. Mets, *The Air Campaign*, 79.
162. Fadok, *John Boyd and John Warden*, 5–7.
163. One of the key bones of contention among airpower theorists was how to identify these centers of gravity and the mechanisms by which their destruction would disable the system. See Fadok, *John Boyd and John Warden*, 7, 23–24; Faber, "Paradigm Lost," 29–30; and Mets, *The Air Campaign*, 75.
164. Fadok, *John Boyd and John Warden*, 7, 23–24; Faber, "Paradigm Lost," 29–30; and Mets, *The Air Campaign*, 75.
165. Mets, *The Air Campaign*, 18, 65.
166. Faber, "Paradigm Lost," 19.
167. Mets, *The Air Campaign*, 65; and David E. Johnson, *Fast Tanks and Heavy Bombers: Innovation in the U.S. Army, 1917–1945* (Ithaca, NY: Cornell University Press, 2003), 206–10.
168. Alan J. Levine, *The Strategic Bombing of Germany, 1940–1945* (Westport, CT: Praeger Publishers, 1992), 114–17, 199.
169. See, for example, John A. Warden III, "Smart Strategy, Smart Airpower," in *Airpower Reborn: The Strategic Concepts of John Warden and John Boyd*, ed. John Andreas Olsen (Annapolis, MD: Naval Institute Press, 2015), 117; and Heather Venable and Sebastian Lukasik, "'Bombing to Win' at 25," War on the Rocks, June 15, 2021, https://warontherocks.com/2021/06/bombing-to-win-at-25.
170. Robert A. Pape, "The Air Force Strikes Back: A Reply to Barry Watts and John Warden," *Security Studies* 7, no. 2 (1997): 193, https://www.tandfonline.com/doi/pdf/10.1080/09636419708429346?casa_token=8gqIKMX4pvIAAAAA:HnyscVZFaVxJgaxrMoSi0iGMf2vt_H9xPuIKfQG2zjzBLcqGAKXob9XtrVL8ZSIZqCKoldjxb6Rtkhk.
171. Pape, "The Air Force Strikes Back," 192; and Faber, "Paradigm Lost," 30.
172. Pape, "The Air Force Strikes Back," 192.
173. Faber, "Paradigm Lost," 31.
174. Venable and Lukasik, "'Bombing to Win' at 25."
175. Faber, "Paradigm Lost," 42–43.
176. Fadok, *John Boyd and John Warden*, 23.
177. Fadok, *John Boyd and John Warden*, 23–25; and Warden, "Smart Strategy, Smart Airpower," 105.
178. Fadok, *John Boyd and John Warden*, 26–27; and Warden, "Smart Strategy, Smart Airpower," 108.
179. Mets, *The Air Campaign*, 63; and Fadok, *John Boyd and John Warden*, 26.
180. Fadok, *John Boyd and John Warden*, 25–26.
181. Venable and Lukasik, "'Bombing to Win' at 25."
182. Mets, *The Air Campaign*, 73–74; and Warden, "Smart Strategy, Smart Airpower," 121–23.
183. Warden, "Smart Strategy, Smart Airpower," 112–13.
184. Warden, "Smart Strategy, Smart Airpower," 123–24. This would probably include most of the weapons systems operated by the People's Liberation Army Rocket Forces.
185. Warden, "Smart Strategy, Smart Airpower," 107–8.
186. Warden, "Smart Strategy, Smart Airpower," 106–9.
187. Warden, "Smart Strategy, Smart Airpower," 109–10.
188. Warden, "Smart Strategy, Smart Airpower," 108–9.
189. Fadok, *John Boyd and John Warden*, 24–25.
190. Warden, "Smart Strategy, Smart Airpower," 109.
191. Robert H. Gregory Jr., *Clean Bombs and Dirty Wars: Air Power in Kosovo and Libya* (Sterling, VA: Potomac Books, 2015), 6–7.
192. Warden, "Smart Strategy, Smart Airpower," 105–6.
193. For reference, a single American brigade combat team contains hundreds of combat vehicles. As of 2021, the American army fielded some 60 brigade combat teams. While it is unlikely that all of these would ever be employed in a single conflict, in the event of a major war, new brigade combat teams would likely be formed. While it is difficult to say with certainty, it is likely that seeking to defeat an enemy by simply destroying their armored vehicles in the field could require the destruction of many times the number of

targets that John Warden suggests would be needed to paralyze its national war-making capacity. See Congressional Research Service, "Defense Primer: Organization of U.S. Ground Forces," November 22, 2021, https://sgp.fas.org/crs/natsec/IF10571.pdf.

194. Fadok, *John Boyd and John Warden*, 25.

195. Gregory, *Clean Bombs and Dirty Wars*, 9.

196. Some Chinese sources minimize this distinction, arguing that while Mao Zedong called for the annihilation of enemy forces, he meant merely the elimination of their ability to resist, not necessarily their physical destruction. That said, it is a significant departure from traditional views of war in which each side would seek to destroy the other's fielded "vital strength." See Shou Xiaosong, *Zhanluexue* [*The Science of Military Strategy*] (Beijing, China: Military Science Press, 2013), 92, https://www.airuniversity.af.edu/Portals/10/CASI/documents/Translations/2021-02-08%20Chinese%20Military%20Thoughts-%20In%20their%20own%20words%20Science%20of%20Military%20Strategy%202013.pdf; and Jeffrey Engstrom, *Systems Confrontation and System Destruction Warfare: How the Chinese People's Liberation Army Seeks to Wage Modern Warfare* (Santa Monica, CA: RAND Corporation, 2018), 10, https://www.rand.org/pubs/research_reports/RR1708.html.

197. Engstrom, *Systems Confrontation and System Destruction Warfare*, 10.

198. Xue Yanxing, "Xinxihua Zhanzheng Yingyou Zhenyangde Luzhanguan" [What Sort of Ground Forces Are Necessary in Informationized Warfare], *People's Liberation Army Daily*, March 12, 2020, http://www.81.cn/jfjbmap/content/1/2020-03/12/07/20200312O7_pdf.pdf.

199. A series of exercises putting these theories into practice took place in the early 2010s. See Edmund J. Burke et al., "People's Liberation Army Operational Concepts," RAND Corporation, 2020, 6–7, 16–17, https://www.rand.org/pubs/research_reports/RRA394-1.html.

200. Engstrom, *Systems Confrontation and System Destruction Warfare*, 10–11; and Burke et al., "People's Liberation Army Operational Concepts," 6.

201. Engstrom, *Systems Confrontation and System Destruction Warfare*, 11; and Shou, *The Science of Military Strategy*, 92–93.

202. Engstrom, *Systems Confrontation and System Destruction Warfare*, 11; and Shou, *The Science of Military Strategy*, 92–93.

203. Burke et al., "People's Liberation Army Operational Concepts," 9–10.

204. Burke et al., "People's Liberation Army Operational Concepts," 20.

205. Burke et al., "People's Liberation Army Operational Concepts," 6; and Feng Donghao, "Guanzhu Waijun Zuozhan Lilun Fazhan Qushi" [Observations on the Trends in Foreign Military Thought], *People's Liberation Army Daily*, June 12, 2018, http://www.81.cn/jfjbmap/content/1/2018-06/12/07/2018061207_pdf.pdf.

206. Engstrom, *Systems Confrontation and System Destruction Warfare*, 11–13; and Warden, "Smart Strategy, Smart Airpower," 112–13, 122–24.

207. Warden, "Smart Strategy, Smart Airpower," 112–13, 122–24; and Burke et al., "People's Liberation Army Operational Concepts," 14.

208. Engstrom, *Systems Confrontation and System Destruction Warfare*, 55; and Shou, *The Science of Military Strategy*, 92–93.

209. Engstrom, *Systems Confrontation and System Destruction Warfare*, 23.

210. Pape, "The Air Force Strikes Back," 192; and Venable and Lukasik, "'Bombing to Win' at 25."

211. Engstrom, *Systems Confrontation and System Destruction Warfare*, 12.

212. Engstrom, *Systems Confrontation and System Destruction Warfare*, 16–17; and Burke et al., "People's Liberation Army Operational Concepts," 8, 12.

213. Engstrom, *Systems Confrontation and System Destruction Warfare*, 8, 16.

214. Warden, "Smart Strategy, Smart Airpower," 108–10.

215. Warden, "Smart Strategy, Smart Airpower," 105–6, 122–24; Burke et al., "People's Liberation Army Operational Concepts," 20–21; and Shou, *The Science of Military Strategy*, 93.

216. While John Boyd is often not mentioned by name, his favorite theoretical construct, the observe, orient, decide, and act loop, is frequently referenced both in Chinese and English. See Shou, *The Science of Military Strategy*, 39, 126; and Fu Zhengnan, "Touxi Meijun Renzhizhande 'Quanjiao Taolu'" [Analyzing the Moves of the American Military's "Martial Arts" in Cognition Warfare], *People's Liberation Army Daily*, December 2, 2021, http://www.81.cn/jfjbmap/content/1/2021-12/02/07/2021120207_pdf.pdf.

217. If there is a greater awareness of the People's Liberation Army's intellectual debt to Warden and of the arguments his critics have made against this theoretical foundation, it would not be contained in official People's Liberation Army doctrine or textbooks but hidden in the pages of academic publications. Scouring these publications to see if any such references exist and who is making them could be a fruitful avenue for future research, though proving a negative is always a difficult intellectual pursuit.

218. Robert A. Pape, *Bombing to Win: Air Power and Coercion in War* (Ithaca, NY: Cornell University Press, 1996), 1–54, 211–54. For a discussion of this debate, see Pape, "The Air Force Strikes Back," 213.

219. Mike Pietrucha, "The Five-Ring Circus: How Airpower Enthusiasts Forgot About Interdiction," War on the Rocks, September 29, 2015, https://warontherocks.com/2015/09/the-five-ring-circus-how-airpower-enthusiasts-forgot-about-interdiction; and Pape, "The Air Force Strikes Back," 191–214.

220. Mets, *The Air Campaign,* 78.

221. Mets, *The Air Campaign,* 78.

222. Gregory, *Clean Bombs and Dirty Wars*, 8.

223. Daniel R. Lake, "The Limits of Coercive Airpower: NATO's 'Victory' in Kosovo Revisited," *International Security* 34, no. 1 (Summer 2009): 83–84, https://direct.mit.edu/isec/article/34/1/83/11962/The-Limits-of-Coercive-Airpower-NATO-s-Victory-in. Daniel R. Lake himself does not believe that the threat was decisive, but he recognizes the controversy and the arguments made by those who believe it was a major factor.

224. Lake, "The Limits of Coercive Airpower," 86.

225. Pape, "The Air Force Strikes Back," 192.

226. Pietrucha, "The Five-Ring Circus."

227. Burke et al., "People's Liberation Army Operational Concepts," 20; and Pape, "The Air Force Strikes Back," 192.

228. Pape, "The Air Force Strikes Back," 203–4.

229. Scott Pence, "Fighting as Intended: The Case for Austere Communications," *Joint Force Quarterly* 102 (2021), 3–13, https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-102/jfq-102_4-13_Forum-Fighting_as_%20Intended.pdf.

230. While Allied air superiority prevented Iraq from observing the massing of forces to enter Iraq through the desert and cut off Iraqi forces in Kuwait, once those forces entered Iraq, Iraqi units in the field were able to communicate their presence to Baghdad. Baghdad was then able to order its units in the field to retreat, and it moved its best divisions to oppose this incursion. Retreating Iraqi forces were devastated, and the Iraqi Republican Guard divisions proved unable to stand up to American ground forces, but the expected systemic paralysis does not seem to have occurred. The enemy was neither entirely blind, deaf, nor dumb. Saddam Hussein's forces on the ground were simply too weak to resist. See Barry D. Watts, "Friction in the Gulf War," *Naval War College Review* 48, no. 4 (1995): 98–99, https://digital-commons.usnwc.edu/nwc-review/vol48/iss4/10.

231. Pape, "The Air Force Strikes Back," 192.

232. Faber, "Paradigm Lost," 28–29.

233. Fadok, *John Boyd and John Warden,* 29.

234. Shou, *The Science of Military Strategy*, 92–93.

235. Ye Huabin and Ai Zhengsong, "Xinxishidai Ruhe 'Jindi' Zuozhan" [How Can You "Approach the Enemy" in the Information Age], *People's Liberation Army Daily*, January 16, 2020, http://www.81.cn/jfjbmap/content/1/2020-01/16/07/2020011607_pdf.pdf.

236. Ye and Ai, "How Can You 'Approach the Enemy' in the Information Age."

237. Stephen Lanza and Daniel S. Roper, "Fires for Effect: 10 Questions About Army Long-Range Precision Fires in the Joint Fight," Association of the United States Army, August 2021, 8, https://www.ausa.org/sites/default/files/publications/SL-21-1-Fires-for-Effect-10-Questions-about-Army-Long-Range-Precision-Fires-in-the-Joint-Fight.pdf; and Bryan Clark et al., *The Invisible Battlefield: A Technology Strategy for US Electromagnetic Spectrum Superiority,* Hudson Institute, March 2021, 9, https://rvjinstitute.org/wp-content/uploads/2021/04/invisible_battlefield_report.pdf.

238. US Department of Defense, *Command, Control, and Communications Modernization Strategy*, September 2020, 6, https://dodcio.defense.gov/Portals/0/Documents/DoD-C3-Strategy.pdf.

239. David Deptula, "A New Battle Command Architecture for Air Force–Led All Domain Operations," Dubai International Air Chiefs

Conference, November 2021, https://www.diacc.ae/articlespdf/Article_02_David_Deptula.pdf.

240. Pietrucha, "The Five-Ring Circus"; and Pape, "The Air Force Strikes Back," 192.

241. Faber, "Paradigm Lost," 24. For the source of many of these arguments, see Pape, *Bombing to Win*. See also Venable and Lukasik, "'Bombing to Win' at 25."

242. Many of the targets they recommend, including intelligence, surveillance, and reconnaissance systems; logistical nodes; and command-and-control systems seem to be more focused on disabling operational systems rather than war systems. See Engstrom, *Systems Confrontation and System Destruction Warfare*, 17, 55; and Shou, *The Science of Military Strategy*, 92–93.

243. Martin D. Mitchell, "The South China Sea: A Geopolitical Analysis," *Journal of Geography and Geology* 8, no. 3 (2016): 19–21, http://www.geographicalinsights.com/uploads/1/0/9/2/109251369/south_china_sea_jog_copy.pdf.

244. Ye and Ai, "How Can You 'Approach the Enemy' in the Information Age."

245. The US has sought to address this vulnerability by experimenting with using a large number of dispersal fields on small islands in the Pacific. See Valerie Insinna, "A US Air Force War Game Shows What the Service Needs to Hold Off—or Win Against—China in 2030," *Defense News*, April 12, 2021, https://www.defensenews.com/training-sim/2021/04/12/a-us-air-force-war-game-shows-what-the-service-needs-to-hold-off-or-win-against-china-in-2030.

246. While many believe that technology has already achieved this goal, especially in the 1999 conflict between NATO and Yugoslavia, controversy over this point persists.

247. Forrest E. Morgan et al., *Military Applications of Artificial Intelligence: Ethical Concerns in an Uncertain World* (Santa Monica, CA: RAND, 2020), 66–69, https://www.rand.org/pubs/research_reports/RR3139-1.html.

248. Fedasiuk, Melot, and Murphy, *Harnessed Lightning,* 38–39.

249. Morgan et al., *Military Applications of Artificial Intelligence*, 61–69.

250. In 1991 the United States launched a concerted air campaign against both strategic and tactical targets.

About the Authors

Dan Blumenthal is a senior fellow at the American Enterprise Institute, where he focuses on East Asian security issues and Sino-American relations. He has served in and advised the US government on China issues for more than a decade.

Christian Curriden is a defense analyst at the RAND Corporation, where he focuses on Chinese and Korean issues, especially Chinese military interventions and proxy wars, People's Liberation Army (PLA) research and development, and the PLA's artificial intelligence applications. He has also conducted both primary and secondary source research in Korean on Northeast Asian diplomacy and lived in South Korea for two years as a missionary for the Church of Jesus Christ of Latter-day Saints.

Gregory Graff is an analyst for the Department of Defense focusing on China's military and strategy. He has previously worked as a China policy adviser in the Office of the Deputy Assistant Secretary of Defense for China, where he focused on technology competition, and as an East Asia counterintelligence analyst. He was a fellow with the Hertog Foundation's inaugural National Security & Sino-American Technology Competition Fellowship.

Opinions, conclusions, and recommendations expressed or implied in this report are solely those of the author and do not necessarily represent the views of the Department of Defense or any other agency of the federal government.