

CSBA

Center for Strategic and Budgetary Assessments

THE DECISIVE DECADE

UNITED STATES–CHINA COMPETITION IN
DEFENSE INNOVATION AND DEFENSE INDUSTRIAL
POLICY IN AND BEYOND THE 2020s



TAI MING CHEUNG
THOMAS G. MAHNKEN

THE DECISIVE DECADE

UNITED STATES–CHINA COMPETITION IN DEFENSE INNOVATION AND DEFENSE INDUSTRIAL POLICY IN AND BEYOND THE 2020s

TAI MING CHEUNG
THOMAS G. MAHNKEN

CSBA

Center for Strategic and Budgetary Assessments

2023

ABOUT THE CENTER FOR STRATEGIC AND BUDGETARY ASSESSMENTS (CSBA)

The Center for Strategic and Budgetary Assessments is an independent, nonpartisan policy research institute established to promote innovative thinking and debate about national security strategy and investment options. CSBA's analysis focuses on key questions related to existing and emerging threats to U.S. national security, and its goal is to enable policymakers to make informed decisions on matters of strategy, security policy, and resource allocation.

ABOUT THE AUTHORS

Tai Ming Cheung is director of the University of California-wide Institute on Global Conflict and Cooperation, and a professor in the School of Global Policy and Strategy at the University of California, San Diego. His areas of research focus include China's efforts to become a world-class science and technology power, defense innovation, and the relationship between geo-economics, innovation, and national security. His latest book is *Innovate to Dominate: The Rise of the Chinese Techno-Security State* (Cornell University Press, 2022). Dr. Cheung has a Ph.D. in War Studies from King's College, London.

Thomas G. Mahnken is President and Chief Executive Officer of the Center for Strategic and Budgetary Assessments. He is a Senior Research Professor at the Philip Merrill Center for Strategic Studies at The John Hopkins University's Paul H. Nitze School of Advanced International Studies (SAIS) and served for over 20 years as an officer in the U.S. Navy Reserve, including tours in Iraq and Kosovo. He currently serves as a member of the Congressionally-mandated 2022 National Defense Strategy Commission and as a member of the Army Science Board. His previous government career includes service as Deputy Assistant Secretary of Defense for Policy Planning from 2006-2009, where he helped craft the 2006 Quadrennial Defense Review and 2008 National Defense Strategy. He served as a member of the 2018 National Defense Strategy Commission and on the Board of Visitors of Marine Corps University. He served on the staff of the 2014 National Defense Panel, the 2010 Quadrennial Defense Review Independent Panel, and the Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction. He served in the Department of Defense's Office of Net Assessment and as a member of the Gulf War Air Power Survey. In 2009 he was awarded the Secretary of Defense Medal for Outstanding Public Service, and in 2016 the Department of the Navy Superior Civilian Service Medal.

ACKNOWLEDGMENTS

The authors would like to thank the participants in the CSBA workshop on “The U.S.-China Techno-Security Rivalry” for their insights. They would also like to thank Josh Chang for his assistance in preparing this manuscript and James Mersol for his editing and publication support. The analysis and findings presented here are solely the responsibility of the authors. CSBA receives funding from a broad and diverse group of contributors, including private foundations, government agencies, and corporations. A complete list of these organizations can be found on our website at www.csbaonline.org/about/contributors.

Cover Graphic: Cover design by James Mersol. F-22 photo taken by Staff Sgt. Vernon Young, United States Air Forces Central. J-20 photo courtesy of N509FZ (alias) under the Creative Commons BY-SA 4.0 license.

Contents

EXECUTIVE SUMMARY	i
CHAPTER 1: INTRODUCTION	1
CHAPTER 2: THE COMPETING TECHNO-SECURITY SYSTEMS	3
The Anti-Statist U.S. Techno-Security System	4
The Present State of the U.S. Techno-Security System	7
Collaboration with Global Partners Is Increasingly Necessary	9
The Chinese Techno-Security System.	11
CHAPTER 3: THE TRANSFORMATION OF THE CHINESE DEFENSE INDUSTRIAL BASE AND COMPARING THE U.S. AND CHINESE DEFENSE INDUSTRIES	15
The Political Clout of the Defense Industry.	18
Defense Financial Innovation in China	19
Weaknesses of the Chinese Defense Industrial Base	23
The Impact of the Ukraine War on the Chinese Defense Industry.	26
Prospects for Future China-Russia Defense Technological and Industrial Cooperation	27
Comparing the U.S. and Chinese Defense Industries	28
CHAPTER 4: ASSESSING THE U.S.-CHINA TECHNO-SECURITY RIVALRY	31
LIST OF ACRONYMS.	34

FIGURES

FIGURE 1: THE DIFFERING NATURES OF THE U.S. AND CHINESE TECHNO-SECURITY SYSTEMS	3
FIGURE 2: REVENUES AND PROFITS OF THE CHINESE DEFENSE INDUSTRY, 2009-2021	16
FIGURE 3: CHINESE DEFENSE INDUSTRY ORGANIZATION CHART, 2023	17
FIGURE 4: ASSET SECURITIZATION TRENDS IN THE CHINESE DEFENSE INDUSTRY, 2012-2020	21
FIGURE 5: THE STATE OF ASSET SECURITIZATION AMONG CHINA'S PRINCIPAL DEFENSE INDUSTRIAL CORPORATIONS IN 2020	22
FIGURE 6: FINANCIAL PERFORMANCE OF AVIC, 2009-2021	30

TABLES

TABLE 1: MEMBERS OF THE DEFENSE INDUSTRY FACTION IN THE CHINESE LEADERSHIP SYSTEM, 2023	19
TABLE 2: ASSET SECURITIZATION FUNDS RAISED BY CHINESE DEFENSE CORPORATIONS AS A RATIO OF THE OFFICIAL CHINESE DEFENSE BUDGET	20
TABLE 3: U.S. AND CHINESE DEFENSE PRIMES IN THE TOP 20 LIST OF GLOBAL DEFENSE CORPORATIONS.	29

Executive Summary

Long-term strategic competition between the United States (U.S.) and the People's Republic of China (PRC) will be increasingly defined by both countries' ability to mobilize and direct their respective techno-security systems over the next decade. Techno-security systems refer to the amalgamation of organizations comprising a nation's industrial economy and innovation base that produce key technologies for strategic, dual-use, and defense applications. The U.S. and Chinese techno-security systems differ significantly in terms of the state's role in guiding innovation, the relationships between private and public entities, and approaches to governance. The clash between these systems not only reflects the broader standoff between both states but also calls into question how each system will adapt both domestically and internationally to meet the demands of strategic inter-state competition.

The U.S. techno-security system can be characterized as anti-statist, with the federal government largely allowing private entities to direct and guide innovation but intervening in the economy when urgently needed. During the Cold War, the U.S. government relied on strong public-private partnerships and a decentralized network of federally-funded laboratories and service-specific research centers to generate new technologies. The U.S. government was also a prime sponsor of foundational scientific research throughout this period, accounting for a significant share of funding for this enterprise. Such an approach yielded important breakthroughs, such as the development of the U-2 and A-12/SR-71 reconnaissance aircraft by the Lockheed Skunk Works in partnership with the Air Force and Central Intelligence Agency, as well as the fielding of the *Atlas* intercontinental ballistic missile by Convair, working with the Air Force's Western Design Division.¹ The advantages of the U.S. approach diminished after the Cold War due to the growing gap between the public and private sectors and the federal government's status as a late adopter of new technology from the commercial sector. These issues have forced Washington to embrace a more internationalist and collaborative approach, opting for more partnerships with allies to develop key capabilities and technologies.

¹ Thomas G. Mahnken, *Technology and the American Way of War Since 1945* (New York: Columbia University Press, 2008), chapter 1.

The Chinese techno-security system, on the other hand, is largely state-driven and highly centralized, with the Chinese Communist Party (CCP) directing innovation and production through its control of state-owned enterprises (SOEs). The CCP aspires to create a techno-security system in which China can achieve wide-ranging self-sufficiency in its ability to develop and produce technology. Paradoxically, however, China's drive for technological independence is partly reliant upon the ability to acquire foreign capital and technology. This ambition has been historically curtailed throughout the PRC's history due to decoupling efforts by the Soviet Union, Europe, and now currently, the United States. The growing rift between the U.S. and China will intensify the techno-security competition between them as both states vie for dominance in a bipolar global technological order.

A key element of the Chinese techno-security system is the defense industry, which has grown tremendously since the end of the Cold War due to Beijing's interest in developing a formidable, world-class military that can compete with the United States. This growth is reflected in the substantial amount of investment in China's defense industry and the increase in its political clout within high-level party-state organizations. China's defense industry stands to benefit from the war in Ukraine by filling global arms exports gaps left by Russian defense manufacturers in the wake of Western sanctions against Moscow. There is also the potential for additional cooperation between the Chinese and Russian arms industry on strategic deterrence capabilities amidst both countries' mutual hostility toward the United States. A convergence of these two industries would present serious, credible challenges to the United States within the context of the Sino-U.S. techno-security competition.

The techno-security competition will be decided by five crucial factors: 1) External threat perceptions and the threat environment; 2) the nature and configuration of the leadership and management coordination systems; 3) the governance regime that regulates the behavior of actors within the system; 4) the role of public-private relationships and the level of dual-use civil-military integration that has taken place; and 5) how the two systems balance between techno-nationalist self-reliance and engaging with foreign countries to forge global techno-security alliances. The United States possesses the lead in governance, public-private partnerships, civil-military integration, and techno-nationalism vs. global engagement. China leads in threat motivation, while both states are matched evenly in leadership and management coordination. Overall, the U.S. techno-security system is better organized and structured for long-term techno-security competition than China's.

CHAPTER 1

Introduction

The great power rivalry between the United States and China is at its most intense and adversarial in the techno-security domain, where national security, technological innovation, military power, industrial might, and economic development intersect. The 2022 US National Security Strategy points out that China is the only competitor to the U.S. with the intent and “economic, diplomatic, military, and technological power” to reshape the global order, and the “next 10 years will be the decisive decade” for this challenge to take place.²

Chinese leaders view the threat from the U.S. from an equally stark and alarmist perspective, although they are more circumspect in their public assessments. In his keynote speech at the 20th Chinese Communist Party Congress in October 2022, Chinese Communist Party General Secretary, State President, and Chairman of the Central Military Commission Xi Jinping said that China was “confronted with drastic changes in the international landscape, especially external attempts to blackmail, contain, blockade, and exert maximum pressure on China”, which was a clear if indirect allusion to the U.S.³ In closed-door forums, Xi has explicitly pointed out that “the United States is the biggest threat to China’s development and security.”⁴ China wants to ensure that the country’s development, of which the technological, security, and military bases are core, is “basically complete” by 2035, allowing it to begin to challenge the U.S. for global supremacy.

The outcome of this long-term techno-security struggle will hinge on how these two countries are organized, mobilized, and incentivized domestically as well as with external allies and like-minded states. The U.S. and Chinese techno-security systems are massive,

2 The White House, *U.S. 2022 National Security Strategy*, October 2022.

3 Xi Jinping, “Hold High the Great Banner of Socialism with Chinese Characteristics and Strive in Unity to Build a Modern Socialist Country in All Respects”, *Report to the 20th Chinese Communist Party National Congress*, 16 October 2022.

4 He, Bin, “Speech at Special Seminar for County-Level Leading Cadre to Study and Implement the 5th Plenum of 19th Central Committee” (在县级领导干部学习贯彻党的十九届五中全会专题研讨班上的发言), *Qilian News* (祁连新闻), 25 February 2021, <http://www.qiliannews.com/system/2021/02/25/013341147.shtml>.

sprawling collections of organizations that cover the most advanced components of their national innovation systems and industrial economies, especially the defense, dual-use, and strategic technology sectors. But these opposing techno-security systems are structured and managed very differently. The Chinese system is primarily state-led and top-down, while the U.S. system is more market-driven and bottom-up. Which of them will ultimately prevail will depend on how capable, robust, and adept they are in meeting the challenge of rapid and disruptive change.

This report offers a net assessment of the current U.S.-China competition in defense innovation and defense industrial policy and the prospects over the rest of this decade. There are three areas of focus:

1. The nature of the Chinese (statist) and U.S. (anti-statist) techno-security systems.
2. A detailed examination of the transformation of the Chinese defense industrial base in the 21st century along with comparing the U.S. and Chinese defense industrial bases. Topics of focus include assessing the Chinese defense industry's political clout and financial innovation that is bringing in significant amounts of market funds to support defense industrial production and development, critical weaknesses, the implications of the Ukraine War for the Chinese defense industry, and the prospects for future China-Russia defense technological and industrial cooperation.
3. An overall comparative net assessment of the U.S. and Chinese techno-security systems examining several key factors critical to how they perform.

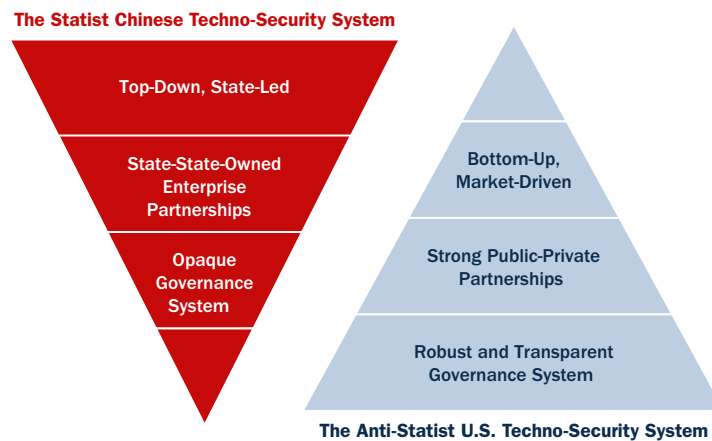
CHAPTER 2

The Competing Techno-Security Systems

The U.S. and Chinese techno-security systems are sprawling testaments to the industrial, technological, and military prowess of the nations they serve. The close bonds between the techno-security system and the state mean that how they are organized, managed, regulated, and operate also reflects the underlying political, social, and institutional ethos of the ruling regimes.

Consequently, it comes as no surprise that the U.S. and Chinese techno-security systems are set up and run in fundamentally different ways in their titanic fight for techno-security dominance. The U.S. techno-security system is anchored in a deeply held anti-statist ethos that emphasizes limited government and an expansive leading role for the private sector, even though the U.S. government has at times exerted a powerful influence in shaping the techno-security ecosystem.

FIGURE 1: THE DIFFERING NATURES OF THE U.S. AND CHINESE TECHNO-SECURITY SYSTEMS



Source: Authors

By contrast, although pro-market forces have played a vital role in the development of China's economy, its techno-security system is overwhelmingly statist, with the Communist party-state dominating ownership, control, and management. In reality, though, especially in the defense sphere, the balance between statist and anti-statist forces is blurred, and the key issue in this competition is how each country's techno-security system finds the most effective working relationship between the state and the market.

The Anti-Statist U.S. Techno-Security System

The U.S. techno-security system can trace its nature and fundamental characteristics to its origins in the Second World War and the early years of the Cold War. World War II witnessed an expansion of government support for scientific endeavors and created relationships among government agencies, universities, and industry. During the war, Franklin D. Roosevelt asked Vannevar Bush, Director of the Office of Scientific Research and Development (OSRD), for thoughts on how the successful application of science to wartime problems could be carried over into peacetime. In response, Bush proposed the establishment of the National Science Foundation to perpetuate the relationship between the scientific community and the government.⁵ The underlying philosophical belief that was widely shared by the U.S. scientific elite was that science and innovation would be far more successful and enduring under a democracy than in a totalitarian system. This belief arose because whereas top-down totalitarian regimes were "rigid, arbitrary, hierarchical, and regimented," the U.S. system was "essentially adapted for the purpose" of pursuing pioneering science and technology.⁶ Throughout the Cold War, the U.S. approach to scientific and technological development allowed the U.S. government to harness the creative energies of American society. Indeed, such an approach yielded a competitive advantage against the Soviet Union while avoiding too much centralization.

There were several core features of the Cold War U.S. techno-security state. The first was its pluralistic and decentralized nature.⁷ The military services each had their own research and development organizations, such as the Office of Naval Research, that competed far more than they cooperated with each other. Initial efforts to establish centralized, top-down coordination mechanisms met fierce resistance across the services and were largely unsuccessful.

5 G. Pascal Zachary, *Endless Frontier: Vannevar Bush, Engineer of the American Century* (Cambridge, M.A.: MIT Press, 1999).

6 Aaron L. Friedberg, *In the Shadow of the Garrison State: America's Anti-Statism and Its Cold War Grand Strategy* (Princeton, N.J.: Princeton University Press, 2000), pp. 304–305, and Vannevar Bush, *Modern Arms and Free Men: A Discussion of the Role of Science in Preserving Democracy* (New York: Simon and Schuster, 1949).

7 Friedberg, *In the Shadow of the Garrison State*, 306–07; Fred Block, "Innovation and the Invisible Hand of Government," in Fred Block and Matthew R. Keller, *State of Innovation: The U.S. Government's Role in Technology Development* (Boulder, C.O.: Paradigm Publishers, 2011), pp. 20–21.

A second feature was the establishment of an expansive and robust system of large-scale federally-funded laboratories engaged in cutting-edge defense and dual-use-related big science endeavors such as nuclear weapons and space research.⁸ This included a nationwide system of nuclear weapons laboratories such as Los Alamos, Lawrence Livermore, and Sandia. Relatedly, the U.S. government established a broad array of university-affiliated research centers, such as the Johns Hopkins Applied Physics Laboratory, as well as federally-funded research and development centers, such as the RAND Corporation, to spur innovation.⁹

A third feature was the federal government's permanent shift in becoming the principal and long-term source of funding for foundational scientific research. The Department of Defense and military services became the biggest funders of basic research during the Cold War. At its peak in 1960, the DoD accounted for 36 percent of global research and development outlays, although this share has since declined to under 4 percent by the end of the 2010s.¹⁰

A fourth feature was the emergence of a strong public-private partnership between the government and private corporations in defense industrial production. Indeed, early in the Cold War, a close and mutually productive relationship between government customers and the defense industry yielded unprecedented capabilities rapidly. Key examples include the development of the U-2 and A-12/SR-71 reconnaissance aircraft by the Lockheed Skunk Works in partnership with the Air Force and Central Intelligence Agency, as well as the fielding of the *Atlas* intercontinental ballistic missile by Convair, working with the Air Force's Western Design Division.¹¹

Following its initial establishment, the U.S. techno-security system underwent subsequent rounds of adjustment to take into account major strategic, technological, and domestic changes. The first revamp occurred in the late 1950s in response to major Soviet technological and military industrial advancements, of which the most prominent was the 1957 launch of the Sputnik satellite coupled with concerns over what appeared to be growing bomber and missile gaps.¹² The fragmented and decentralized nature of the U.S. techno-security state was identified as the prime reason for the U.S. falling behind the Soviet Union in vital defense and strategic sectors, and this led to the formation of centralized civilian-led agencies reporting to the Secretary of Defense, which included the Advanced Research Projects Agency (ARPA), later the Defense Advanced Research Projects Agency, or DARPA. DARPA's

8 Block, "Innovation and the Invisible Hand of Government," p. 7.

9 Thomas G. Mahnken, *Forging the Tools of 21st Century Great Power Competition* (Washington, D.C.: Center for Strategic and Budgetary Assessments, 2020), pp. 21–24.

10 John F. Sargent Jr., Marcy E. Gallo, and Moshe Schwartz, *The Global Research and Development Landscape and Implications for the Department of Defense* (Washington, D.C.: Congressional Research Service, November 2018), <https://fas.org/sgp/crs/natsec/R45403.pdf>

11 Thomas G. Mahnken, *Technology and the American Way of War Since 1945* (New York: Columbia University Press, 2008), chapter 1.

12 See Friedberg, *In the Shadow of the Garrison State*.

mission was “to make pivotal investments in breakthrough technologies for national security.” The agency’s first three areas of research focused on space technology, ballistic missile defense, and solid propellants. Following the creation of NASA the following year, DARPA’s mission was refocused on formulating and executing research and development projects that would expand beyond the immediate and specific requirements of the services. It sought breakthrough technologies that would yield advantages on the battlefield.¹³

Around the same time, a group of talented young scientists and engineers known as the Fairchildren established a startup semiconductor enterprise that laid the seeds for the creation of Silicon Valley and several powerhouses of the late 20th century U.S. innovation system, such as Intel and AMD.¹⁴ These developments in the national S&T system, especially in the electronics and computing sectors, had profound consequences for the rise of the techno-security system.

Another important turning point for the U.S. techno-security system began in the mid-1970s and extended into the 1980s with the so-called Offset Strategy, which was subsequently re-dubbed the Second Offset Strategy. This was again in response to the external threat posed by growing Soviet quantitative superiority in conventional and strategic military capabilities.¹⁵ The U.S. could not compete on a like-for-like basis with the Soviet Union, so the DoD leadership decided instead to seek technological superiority in advanced capabilities such as precision strike, intelligence, surveillance, and reconnaissance, as well as radar-evading stealth capabilities.¹⁶ This eventually gave the U.S. a decisive technological edge by emphasizing U.S. strengths over Soviet weaknesses, most notably in the air defense arena, and helped to contribute to the collapse of the Soviet Union at the end of the 1980s.

With the U.S. techno-security system emerging triumphant at the end of the Cold War, it no longer faced any peer rivals and turned instead to dealing with threats from regional states, non-state actors, and technological challenges brought on by the shift from warfare in the industrial era to information-age warfare.¹⁷ The next major turning point for the U.S.

13 Thomas G. Mahnken, *Forging the Tools of 21st Century Great Power Competition* (Washington, D.C.: Center for Strategic and Budgetary Assessments, 2020), p. 22.

14 Block, “Innovation and the Invisible Hand of Government,” pp. 8–9.

15 Robert Martinage, *Toward a New Offset Strategy: Exploiting U.S. Long-Term Advantages to Restore U.S. Global Power Projection Capability* (Washington, D.C.: Center for Strategic and Budgetary Assessments, 2014), <https://csbaonline.org/uploads/documents/Offset-Strategy-Web.pdf>.

16 This asymmetric strategy was known as the competitive strategies concept and was developed by Andrew W. Marshall, the legendary head of the Office of Net Assessment in the Pentagon. See A.W. Marshall, *Long-Term Competition with the Soviets: A Framework for Strategic Analysis* (Washington, D.C.: RAND Corp., 1972), <https://www.rand.org/pubs/reports/R862.html>. See also Thomas G. Mahnken, “Arms Competitions, Arms Control, and Strategies of Peacetime Competition from Fisher to Reagan” in Hal Brands, editor, *The New Makers of Modern Strategy: From the Ancient World to the Digital Age* (Princeton: Princeton University Press, 2023).

17 Thomas G. Mahnken, *Technology and the American Way of War Since 1945* (New York: Columbia University Press, 2008), chapter 5.

techno-security state has been coping with the intensifying great power rivalry with China, which has steadily grown since the early 2010s.

The Present State of the U.S. Techno-Security System

In the post-Cold War era, and especially in the 21st century, the traditional strengths of the U.S. techno-security system have not aged well. Three aspects, in particular, are worth considering. First, mutually rewarding partnerships between the public and private sectors have historically been an important driver of U.S. performance. The public-private relationship has, however, become strained in the 21st century. All too often, the views of those in the defense industry have been greeted with suspicion, and an adversarial narrative between government and industry has grown more prominent in recent years.¹⁸ This development threatens to turn this pillar of strength into a source of weakness. Whereas Beijing aspires to military-civil fusion, the U.S. government often holds the defense industry at arm's length. Whereas there has been much talk in recent years about the need to embrace innovation, such talk has often not been matched by action. The fact that complaints that the Defense Innovation Unit, which was founded to speed new technology to the field, took shortcuts in hiring and contracting were sufficient to derail the candidacy of the unit's director to serve as Under Secretary of Defense for Acquisition and Sustainment illustrate the government's schizophrenia on the topic.¹⁹

Two trends, in particular, have contributed to the erosion of public-private partnerships in the United States that are a worrying source of vulnerability in its rivalry with China. First, the defense acquisition system has become increasingly rigid and risk-averse. It gives corporations few incentives to take the sort of risks that are central to the process of innovation. The system also discourages firms from quickly fixing problems with known or promising solutions. The system is so expansive and complex as to defy reform. Moreover, the Defense Department is increasingly isolated from large portions of the most innovative and thriving commercial sectors of the economy. It should not be surprising that, according to former Under Secretary of Defense for Research and Engineering Mike Griffin, it takes the Defense Department 16 years to deliver an idea to operational capability, whereas it is claimed that China can sometimes do it in less than seven years, although a select analysis of Chinese programs shows that this is not the case and the actual acquisition cycles ranged between

18 Rhys McCormick, "Defense Acquisition in the Biden Administration", Center for Strategic and International Studies, February 2021, <https://www.csis.org/analysis/defense-acquisition-biden-administration>; and "Joe Biden is Filling Top Pentagon Positions with Defense Contractors", The Intercept, May 28, 2021, <https://theintercept.com/2021/05/28/biden-pentagon-defense-contractors/>

19 "DIU's Mike Brown Pushed 'Unethical' Contracting and Hiring, Former CFO Alleges", *FedScoop*, April 29, 2021, <https://fedscoop.com/mike-brown-diu-ig-investiation-unethical-contracting-former-cfo-says/>

11–18 years.²⁰ In any case, one of the critical dimensions of the techno-security competition between the U.S. and China is the pace of technological development and effectiveness of the acquisition process, and the U.S. is increasingly turning into the tortoise rather than the hare in the race.

Second, the U.S. techno-security system is struggling to have its voice heard in guiding innovation, as its once-dominant position as the biggest source of investment in research and development has eroded. The U.S. Department of Defense at the beginning of the 2020s accounted for a mere 3.6 percent of global research and development outlays, compared to 36 percent at its height in 1960.²¹

Moreover, the Pentagon has gone from being a first adopter of technologies to being increasingly an investor in technology research. This shift means that many technologies originate in the civilian sphere and are subsequently—and often belatedly—adapted for defense and dual-use applications. Although this is cost-effective and allows access to a more extensive pool of innovation, the U.S. techno-security system risks becoming a follower rather than a leader unless it steps up to fill the gaps in defense-specific areas where the commercial sector is reluctant or unable to participate.

If these trends persist, the U.S. techno-security system could find its influence and place in the U.S. innovation system increasingly marginalized. This change has already happened in the corporate sector. By the second half of the 2010s, the top five U.S. technology companies, such as Google, Amazon, and Apple, spent ten times more annually on research and development than the top five U.S. defense prime contractors, including Lockheed Martin, Boeing, and Raytheon.²² This growing imbalance in the public-private relationship could lead firms to decide that doing business with the U.S. government is not sufficiently lucrative and encourage them to focus instead on more profitable commercial markets domestically and internationally, including in China. Reinvigorating the public-private relationship will be critical in any effort by the United States to credibly compete against China over the long term.

In the past few years, the Defense Department has taken some initial steps to improve this situation. For example, whereas U.S. venture capital invests heavily in later-stage hardware

20 “Robot-Soldiers, Stealth Jets and Drone Armies: The Future of War”, *Financial Times*, November 15, 2018, <https://www.ft.com/content/442de9aa-e7a0-11e8-8a85-04b8afea6ea3>; and Tai Ming Cheung, “Strengths and Weaknesses of China’s Defense Industry and Acquisition System and Implications for the United States”, Acquisition Research Program, Naval Postgraduate School, March 31, 2017. The Cheung study examined the acquisition cycles of 4 Chinese major weapons programs, which were the Chengdu J-20 fighter aircraft, the Luyang-Class 052C/D destroyer, the Shenyang J-15 fighter, and the Y-20 Transport, and it showed it took between 11 years to 18 years from project start-up to operational deployment.

21 “The Global Research and Development Landscape and Implications for the Department of Defense”, Congressional Research Service, June 28, 2021, <https://sgp.fas.org/crs/natsec/R45403.pdf>

22 Department of Defense Emerging Technology Strategy: A Venture Capital Perspective, Silicon Valley Defense Working Group, April 2019, <https://static1.squarespace.com/static/5f82250a85dd3125aeba053d/t/5fb279560e8bbf646f9357e8/1605532000435/DOD+Emerging+Tech+Strategy+from+a+VC+Perspective+SVDWG.pdf>

companies, there is a deficit in funding for early-stage hardware companies. Launched in March 2021, the Defense Department's National Security Innovation Capital fund seeks to redress this underinvestment in trusted capital for early-stage dual-use hardware startups while also accelerating technology development and fending off adversarial investment in critical defense technologies. Its focus is on product development and production, filling a gap between proof of concept and production. The scale of such an effort is, however, small, at \$15 million per year.²³

More recently, in December 2022, the Defense Department established an Office of Strategic Capital to align and scale private capital for national defense.²⁴ In particular, the office seeks to identify gaps in private investment in the technology priorities established by the Department of Defense and to address these deficits through leveraged instruments issued by the Small Business Investment Corporation.

Collaboration with Global Partners Is Increasingly Necessary

As the world's most advanced techno-security power, the U.S. has been the dominant exporter of advanced technology, knowledge, and industrial products in both the military and civilian spheres. The possession of a comprehensive world-class science and technology base, especially in the defense technological arena, has meant that the U.S. has traditionally had little appetite for acquiring foreign technology or know-how. This sense of industrial and technological superiority led to a fierce and enduring techno-nationalist ideology and posture in which the U.S. viewed itself as head and shoulders above the rest of the world.

The global technological landscape has, however, changed rapidly in the 21st century with the advent of a diverse array of emerging technologies, many of which have defense and dual-use applications. With its shrinking overall share of global research and development investment, the United States has found that it is increasingly difficult and costly to keep abreast of technological advances in all the key domains, which has made collaboration with foreign partners increasingly attractive and necessary. This cooperation is taking place in areas such as 5G, quantum computing, and communications—areas where China has been especially active and is vying for global leadership.²⁵

Techno-nationalist primacy, though, has been deeply entrenched within the institutional culture of the U.S. techno-security system for so long that a fundamental shift toward a more collaborative techno-globalist approach is likely to encounter entrenched resistance

23 By contrast, the United Kingdom government invests \$137 million annually in its National Security Strategic Investment Fund.

24 "Secretary of Defense Establishes Office of Strategic Capital," (U.S. Department of Defense, December 1, 2022), <https://www.defense.gov/News/Releases/Release/Article/3233377/secretary-of-defense-establishes-office-of-strategic-capital/>

25 Lisa Curtis, Jacob Stokes, Joshua Fitt, and Andrew Adams, *Operationalizing the Quad* (Center for a New American Security, June 2022), https://s3.amazonaws.com/files.cnas.org/CNAS+Report-IPS-Quad_Final.pdf

and will take time to implement effectively. There have been occasional attempts to establish the foundations of a more globalist-oriented techno-security approach. The formation of the security compact known as AUKUS (Australia, United Kingdom, and United States) in 2021—centered on advanced defense and dual-use capabilities—is the most recent and promising opportunity for the rise of a U.S. globalist-oriented techno-security regime.²⁶ Earlier initiatives—such as the National Technology and Industrial Base (NTIB) initiative designed to create stronger relationships between the United States, Australia, Canada, and the United Kingdom—have yet to gather steam.²⁷ Such efforts face a myriad of bureaucratic hurdles, including the application of the International Traffic in Arms Regulations (ITAR) and other export controls.

Indeed, in recent years U.S. defense firms have chosen to develop a series of new, cutting-edge weapon systems abroad. For example, Boeing developed the MQ-28 *Ghost Bat* unmanned aerial vehicle (UAV) in Australia through its Boeing Australia subsidiary.²⁸ More recently, Anduril Australia teamed with Royal Australian Navy and the Australian Defense Science and Technology Group (DSTG) to produce the *Ghost Shark* unmanned undersea vehicle (UUV).²⁹ Although Australian military interest and investment in such systems clearly played a role in the decisions to develop them on allied soil, so too did the fact that doing so would limit the application of ITAR restrictions to the programs.

One area in which the U.S. has traditionally been able to pursue a more collaborative partnership with foreign allies is in controlling the spread of sensitive technologies.³⁰ To respond to the technological challenges of the Soviet Union and Japan in the 20th century, the U.S. established several institutional frameworks to control the flow of technologies and know-how to these countries, especially the Coordinating Committee for Multilateral Export Controls. These regimes worked effectively in their own spheres, but the integrated civil-military challenge posed by China requires the U.S. government to develop a more robust and whole-of-government approach than the current ad hoc and underdeveloped intra-agency process.

26 The White House, Implementation of the Australia-United Kingdom-United States Partnership (AUKUS), April 5, 2022, <https://www.whitehouse.gov/briefing-room/statements-releases/2022/04/05/fact-sheet-implementation-of-the-australia-united-kingdom-united-states-partnership-aukus/>

27 Stew Magnuson, “US-UK-Canada-Australia Industrial Base Initiative Yet to Gather Steam,” National Defense, September 9 2019, available at <https://www.nationaldefensemagazine.org/articles/2019/9/9/us-ukcanada-australia-industrial-base-initiative-yet-to-gather-steam>

28 Valerie Insinna, “US Air Force to Start New Experiments with Boeing’s MQ-28 Ghost Bat Drone,” Breaking Defense, October 5, 2022, available at <https://breakingdefense.com/2022/10/us-air-force-to-start-new-experiments-with-boeings-mq-28-ghost-bat-drone/>

29 Gabriel Honrada, “Ghost Shark: Australia UUV Built to Bite and Scare China,” *Asia Times*, December 18, 2022, available at <https://asiatimes.com/2022/12/ghost-shark-australia-uuv-aims-to-bite-and-scare-china/>

30 Emma Rafaelof, *Unfinished Business: Export Control and Foreign Investment Reforms, U.S.-China Economic and Security Review Commission*, June 2021, https://www.uscc.gov/sites/default/files/2021-06/Unfinished_Business-Export_Control_and_Foreign_Investment_Reforms.pdf

The U.S. has been revamping these legacy regimes through incremental reforms such as the 2018 Foreign Investment Risk Review Modernization Act and a revamped export control regime. Nonetheless, there is still a gaping hole in the dual-use and strategic emerging high-technology domains that requires a new, wholly dedicated institutional mechanism that can respond more effectively and deal with this arena.

The Chinese Techno-Security System

Rising threat perceptions, centralized, top-down coordination, and techno-nationalist dependence are the principal drivers in the development of the Chinese techno-security system.³¹ The Chinese authorities have used deepening concerns over the external security environment since the late 1990s, especially the grand techno-security threat posed by the United States, as a catalyst to ramp up the development of its techno-security capabilities. This has especially been the case in areas such as strategic deterrence and anti-access/area-denial capabilities. These perceptions of the U.S. threat have only grown more dire, pressing, and expansive under Xi's tenure over the past decade and are a hugely powerful existential motivating factor in driving the development of the Chinese techno-security system.

Centralized top-down coordination has been instrumental to many, if not most, of China's signature strategic technological achievements, from nuclear weapons and ballistic missiles to the manned space program and high-performance computers. This approach is now being revamped and reprioritized from foreign absorption to original innovation so that it continues to play a leading long-term role. But a key and intentionally designed limitation of this model is that it can only manage a select number of high-priority strategic and defense-related projects.

The principal governance model of the Chinese techno-security system is of a highly centralized planning system that relies on directly enforced administrative controls from state and party agencies and the use of penalties to ensure compliance by enterprises, research institutes, and other actors. This central planning system was first established in the 1950s during the rule of Mao Zedong, and its Socialist-dominant design, operational norms, and institutional culture were directly copied from the Soviet Union, which during this period enjoyed pervasive influence in the development of the Chinese techno-security system.

There was some rollback of this pervasive state control in the post-1978 reform era and a willingness to open up to market-based initiatives, but state planning, management, and intervention have remained extensive because the techno-security ecosystem continues to be overwhelmingly under state ownership. Efforts to shift from direct to more indirect modes of governance gained traction starting in the 21st century, with the state focusing

31 For more information, see Tai Ming Cheung, *Innovate to Dominate: The Rise of the Chinese Techno-Security State* (Ithaca; Cornell University Press, 2022).

its attention on setting broad, high-level developmental directions instead of hands-on micro-management.

A fundamental paradox of the Chinese techno-security system is that although it is intensively techno-nationalist, and thus champions self-reliance, it has also been highly dependent on the importation of foreign technology and know-how. To resolve this contradiction, self-reliance is a long-term aspirant objective and the importation of foreign capabilities is of immediate and near-term priority.

This techno-nationalist dependence has been a key characteristic of the Chinese techno-security system's developmental catch-up strategy from the 1950s to the present day. Under Xi, however, there has been a heightened priority on achieving original homegrown innovation, and self-reliance may see techno-nationalist dependence become a less important force in supporting the Chinese techno-security state's race to the global innovation frontier. Gaining access to and leveraging foreign technology and knowledge will, however, continue to be an essential feature for the foreseeable future, especially for other parts of the techno-security ecosystem that are still catching up. Techno-nationalist dependence is a well-proven low-risk, high-reward development strategy that provides a safeguard, while forging an original innovation capacity is a long-term, high-risk endeavor.

However, the long-term viability of the techno-nationalist dependence model will be put in grave doubt if U.S.-led efforts to reduce significantly and perhaps fully decouple technological relations with China are carried out. Before the U.S.-China relationship turned acrimonious in the late 2010s, the two countries enjoyed broad and deep economic interdependence and societal engagement. Although the U.S. and Chinese techno-security ecosystems had far fewer interactions because of tight restrictions imposed by their governments, considerable cooperation and transactions took place on matters deemed to not infringe on national security concerns. This more permissive climate became an early casualty of the intensifying great power rivalry, and policy debates have turned to how far the two countries should decouple from each other.

The implications of decoupling are markedly different in the techno-security realm compared to the economic or academic spheres. In the non-security arenas, decoupling is costly and detrimental to both sides.³² In the techno-security domain, however, the circumstances are more asymmetric. China is a clear beneficiary from being able to access the United States for advanced technology and knowledge, while the advantages for the United States are mixed at best. In the aggregate, though, the U.S. techno-security state would be far less negatively impacted by decoupling than its Chinese counterpart.

32 For more information, see U.S. Chamber of Commerce China Center and Rhodium Group, *Understanding U.S. – China Decoupling: Macro Trends and Industry Impacts* (February 2021), https://www.uschamber.com/sites/default/files/024001_us_china_decoupling_report_fin.pdf.

The Chinese techno-security state is no stranger to decoupling. The current situation represents the third occasion where it has faced a far-reaching shutdown in access to critical technologies and know-how since the founding of the People's Republic in 1949. The first time was in the 1960s when the Soviet Union abruptly cut off industrial and technical assistance to China, especially to the techno-security establishment. This severely affected the development of the nascent Chinese techno-security base, but forced the country to urgently step up its efforts at technological self-reliance.³³ The second time was in the aftermath of the June 1989 Tiananmen Square crackdown when the United States and the European Economic Community (the forerunner to the European Union) imposed economic sanctions and halted all military cooperation with China. This cutoff in U.S.-China military technological engagement has continued to the present day. Consequently, the Chinese authorities are well aware of what decoupling means and what steps to take to mitigate the fallout.

Decoupling would only be the opening gambit, however. The next phase would be a competition to gain dominance in the resultant bifurcated global technological order.³⁴ This would require the United States and China to recruit partners, build alliances, and establish their own techno-security orders. The United States has a powerful advantage because it played a central role in establishing the existing global techno-security order. But the current revolution in global technology affairs offers a window of opportunity for China to stake a leadership claim on emerging domains such as 5G, AI, quantum technology, cybersecurity, clean energy, and biotechnology. Forging a winning multilateral coalition will not be easy for these techno-nationalist-minded countries.

33 Zhihua Shen and Yafeng Xia, *Between Aid and Restriction: Changing Soviet Policies Toward China's Nuclear Weapons Program, 1954–1960* (Washington, D.C.: Woodrow Wilson Center, May 2012), p. 52.

34 On the issue of bifurcation and the need of the United States to form strong multilateral technological alliances with close allies, see China Strategy Group, *Asymmetric Competition: A Strategy for China and Technology* (Fall 2020), <https://assets.documentcloud.org/documents/20463382/final-memo-china-strategy-group-axios-1.pdf>. This group is made up of influential U.S. technology leaders and policy researchers that includes Eric Schmidt, former CEO of Google.

CHAPTER 3

The Transformation of the Chinese Defense Industrial Base and Comparing the U.S. and Chinese Defense Industries

Since the beginning of the 21st century, the Chinese defense industry has engineered a remarkable turnaround in its technological, industrial, and economic fortunes. Between the 1980s and the end of the 1990s, as China single-mindedly focused on economic development and drastically cut back on defense priorities, the defense industrial base suffered a severe and prolonged drop in demand for its products and services. By the turn of the millennium, the Chinese defense industry was weighed down by a mountain of crippling debt, most of its production capacity and armament line-up was woefully out-of-date, there was little appetite or support for innovation, its political clout had withered, and it struggled to win orders, even from the PLA.³⁵

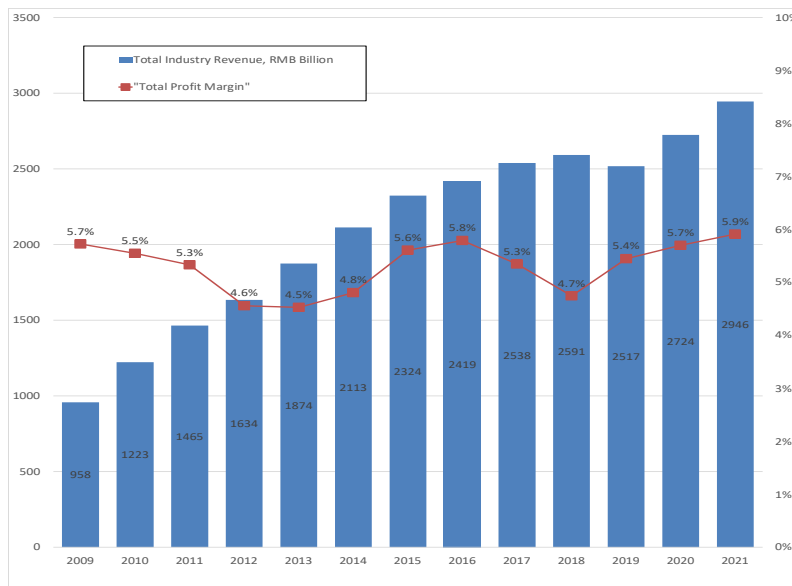
The defense industry's fortunes began to rebound in the opening years of the first decade of the 21st century as China's leaders ordered a major military buildup, especially in strategic deterrence capabilities, to address mounting geo-strategic and security challenges that threatened core interests. These threats came from two inter-related sources: 1) Taiwan's efforts to separate itself from the Chinese mainland and seek independence; and 2) the ability of the U.S. to attack China with global precision strike capabilities, which was clearly demonstrated in a long-range U.S. bombing attack that heavily damaged the Chinese Embassy in Belgrade, Yugoslavia, in 1999. With China still largely cut off from

35 For a detailed history, see Tai Ming Cheung, *Fortifying China* (Ithaca, N.Y.: Cornell University Press, 2013).

access to Western defense and dual-use markets because of sanctions in response to the 1989 Tiananmen Square crackdown, the Chinese authorities had little choice but to turn to its languishing domestic defense industrial base to step up and meet these urgent military requirements.

This resurgence of demand from the PLA, combined with high-level political support, has led to a remarkable recovery and transformation of the Chinese defense industry over the past two decades. Industry-wide profits and revenues have been surging annually, a broad and deep array of advanced weapons and equipment is coming off the production lines, and the research, development, and engineering pipeline is bulging.³⁶ The defense industry's total revenues have nearly tripled between 2009 and 2021 from Rmb 958 billion (\$141.4 billion to Rmb 2.946 trillion (\$434.8 billion) (see chart). This momentum looks set to continue through the 2020s as China faces mounting security and geo-strategic challenges.

FIGURE 2: REVENUES AND PROFITS OF THE CHINESE DEFENSE INDUSTRY, 2009-2021



Source: Data comes from defense company websites, government websites (National Audit Office), and media reports.

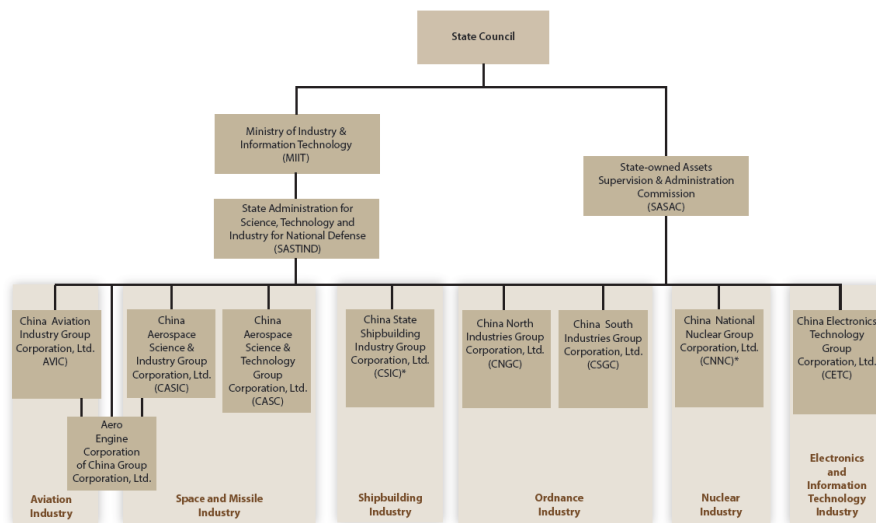
Efforts to reform and modernize the Chinese defense industry have centered on revamping its state-owned corporations. Between the 1950s and the end of the 1990s, these entities were formidable obstacles to innovation because they were all-powerful state bureaucracies that protected their institutional interests by preserving the central planning system that had allowed them to flourish. It was not until the beginning of the 2000s that the central

36 Tai Ming Cheung, "Keeping Up with the Jundui: Reforming the Chinese Defense Acquisition, Technology, and Industrial System," in Phillip C. Saunders, Arthur S. Ding, Andrew Scobell, Andrew N.D. Yang, and Joel Wuthnow (editors), *Chairman Xi Remakes the PLA* (Washington, DC: National Defense University Press, 2019).

government decided to undertake major reforms to transform these loss-making entities into more market-driven enterprises. Since then, these corporations have been slimmed down, allowed to shed heavy debt burdens, and given access to new sources of investment, especially from the capital markets. They are now engaged in ambitious expansion strategies to become global arms and strategic technology champions.

Combined with a strong pickup in defense and civilian orders, these corporations have become profitable since the mid-2000s. The annual profitability of the Chinese defense industry between 2009 and 2019 has hovered in a narrow range of between 4.5 percent and 5.8 percent (see Figure 2). Around three-quarters of the Chinese defense industry's annual revenue comes from civilian operations, such as automobiles, and white goods, such as washing machines and refrigerators. The aviation, space/missile, defense electronics, and naval sectors have been the chief beneficiaries of this rising tide of defense procurement, while the ordnance industry has enjoyed considerable success from the sales of civilian products such as motor vehicles.³⁷

FIGURE 3: CHINESE DEFENSE INDUSTRY ORGANIZATION CHART, 2023



Source: Authors.

These defense industrial behemoths have found strong and sustained political support from the highest levels of civilian and military leadership since the end of the 1990s for their efforts to expand significantly and upgrade their scientific, technological, and industrial capabilities. This support has translated into the elevation of defense industrial issues to the top of government priorities, significant increases in the allocation of financial,

37 For more insight, see Nan Tian and Fei Su, *Estimating the Arms Sales of Chinese Companies*, SIPRI Insights on Peace and Security, No. 2020/2, January 2020, https://www.sipri.org/sites/default/files/2020-01/sipriinsight2002_1.pdf.

human capital, and other resources, enactment of a range of regulations, policies, and plans to support defense industrialization and innovation, and active leadership intervention to tackle structural obstacles that have often stymied progress.³⁸

The Political Clout of the Defense Industry

The political clout of the defense industry has grown since the mid-2010s, especially in the last few years, as political leaders and senior bureaucrats with close ties to the defense industry have been promoted to prominent positions in central Party, state, and military institutions as well as at the provincial level. This growth harkens back to the Maoist era of the 1950s and 1960s when the defense industrial apparatus wielded considerable political influence at the highest levels of the political process, including competing against the all-powerful People's Liberation Army for control over resources and programs.³⁹ However, the defense industry faction's fortunes and clout sharply declined after China switched focus to economic development in the late 1970s, which led to a far-reaching shrinking of the defense industrial base.

The re-emergence of the defense industry faction as a political power center is still in its early stages, but if it is able to continue to raise its profile and influence, then this could see more resources flowing into the defense industrialization process. One especially noteworthy appointment was that of Jin Zhuanlong to head the Ministry of Industry and Information Technology (MIIT) in June 2022. MIIT is responsible for the management and oversight of China's industrial and high-technology economy, including the defense industrial sector. Jin, who has served much of his career in the defense industry, including as the deputy director of the State Administration for Science, Technology, and Industry for National Defense (SASTIND) between 2005 and 2008, is the first member of the defense industry faction to be elevated to this powerful position.

The defense industry faction achieved even more political success at the 20th Chinese Communist Party National Congress in October 2022, when several former high-level defense industry executives were promoted to senior political positions. Four of them were elected to the 24-member Politburo, which is one of the most prestigious and powerful political decision-making bodies in the Chinese leadership system, second only to the Politburo Standing Committee. These four Politburo members are:

- Ma Xingrui, Xinjiang Party Secretary, who spent much of his career working in the space industry and state defense industrial administration;
- Zhang Guoqing, Guangdong Party Secretary, who was general manager of NORINCO, one of China's two principal ordnance corporations between 2008 and 2013;

³⁸ Cheung, *Fortifying China*.

³⁹ For more information, see Cheung, *Fortifying China*.

- Yuan Jiajun, Chongqing Party Secretary, who has worked in the space sector for much of his career; and
- Gen. Zhang Youxia, Central Military Commission Executive Vice-Chairman, who was in charge of the PLA's armament management system between 2012 and 2017.

The defense industry faction currently accounts for 17 percent of Politburo membership, the highest it has ever achieved.

TABLE 1: MEMBERS OF THE DEFENSE INDUSTRY FACTION IN THE CHINESE LEADERSHIP SYSTEM, 2023

Name	Party Status	Institutional Affiliation	Defense Industry Connection
Jin Zhuanglong	Central Committee member	Minister, Ministry of Industry and Information Technology	SASTIND Deputy Director, 2005-2008
Ma Xingrui	Politburo member	Xinjiang Party Secretary	SASTIND Director, 2013-2014; General Manager, China Aerospace S&T Corp., 2007-2011
Zhang Guoqing	Politburo member	Guangdong Party Secretary	General Manager, NORINCO, 2008-2013
Yuan Jiajun	Politburo member	Chongqing Party Secretary	President, Chinese Academy of Space Technology, 2003-2014
Zhang Qingwei	Central Committee member	Hunan Party Secretary	SASTIND Director, 2008-2009; General Manager, China Aerospace S&T Corp., 2001-2007
Zhang Youxia	Politburo member	Executive Vice Chairman, Central Military Commission	Portfolio includes dealing with defense industrial matters
Hao Peng	Central Committee member	Minister, State-Owned Assets Supervision and Administration Commission	General Manager, AVIC Lanzhou Flight Control Instrument General Factory, 1995-1999

Source: Cheng Li, "The Careers of China's Rocket Scientists in the Party Leadership," Brookings Institution, 18 July 2022, <https://www.chinausfocus.com/2022-CPC-congress/the-careers-of-chinas-rocket-scientists-in-the-party-leadership/>; "China's Xi Stacks Government With Science and Tech Experts Amid Rivalry With U.S.," Wall Street Journal, 18 November 2022;

Defense Financial Innovation in China

China's defense industry has benefitted greatly since the early 2010s from innovative ways to acquire access to new sources of financial investment beyond its traditional dependence on state budget allocations. The most important and lucrative approach is asset securitization

(AS, known in Chinese as 资产证券化 or *zichan zhengquanhua*), in which defense firms tap the domestic stock market and state investors to raise funds. Annual average asset securitization funds raised by defense firms between 2012 and 2020 amounted to the equivalent of 17.6 percent of the official defense budget (see chart).

TABLE 2: ASSET SECURITIZATION FUNDS RAISED BY CHINESE DEFENSE CORPORATIONS AS A RATIO OF THE OFFICIAL CHINESE DEFENSE BUDGET

Year	Asset Securitization Funds Raised by Defense Corporations U.S.\$ bn (Rmb bn)	Official Defense Budget U.S.\$ bn (Rmb bn)	Asset Securitization Funds as a Ratio of Official Defense Budget
2013	27.3 (288.4)	120 (741.1)	22.7%
2014	24.4 (168.4)	135 (829)	18%
2015	55.5 (383)	145 (908.8)	38.3%
2016	9.9 (68.3)	147 (976)	6.7%
2017	29.9 (206.3)	154 (1,044)	19.4%
2018	37 (255.3)	170 (1,128)	21.8%
2019	2.8 (19.3)	176 (1,213)	1.6%
2020	22.3 (153.9)	184 (1,270)	12.1%
Annual Average Funds Raised	23.6 (156.5)	154	17.6%

Source: Data comes from defense company websites, media reports, and stock brokerage reports.

The first defense AS deal took place in 2013 by the China Shipbuilding Industry Corporation (CSIC), which undertook an RMB 8.5 billion (US\$1.38 billion) private share placement with ten Chinese parties to acquire production facilities to manufacture warships. More than one-third of funds, or RMB 3.275 billion (US\$533 million), was earmarked for the acquisition of medium and large surface warships, conventional submarines, and large landing ships, while RMB 2.66 billion (US\$433 million) was designated for arms trade-related undertakings and civil-military industrialization projects. The remaining RMB 2.54 billion (US\$413 million) was set aside as working capital.⁴⁰ CSIC explained that the funds would “satisfy the development and manufacture of a new generation of weapons and equipment,” adding that “we need urgent large-scale technological improvements and need to expand our financing

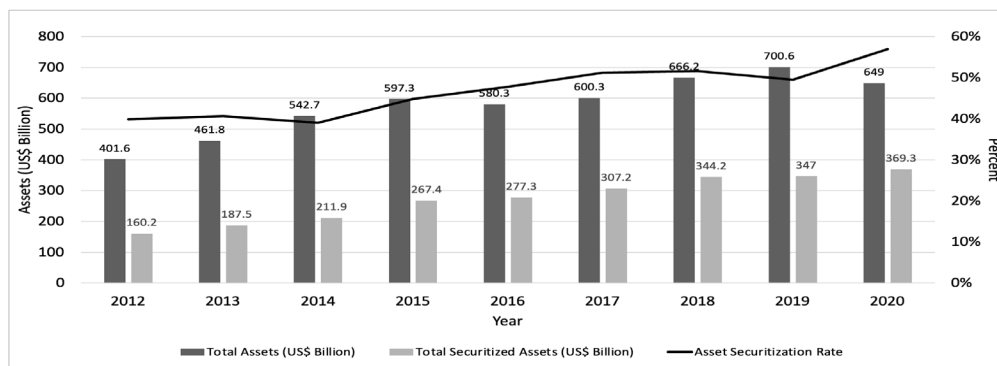
40 “CSIC Releases Plan for 8.48 Billion Set, Creates Precedent for Defense Asset Injection” [中国重工84.8亿定增预案出炉 开创重大军工资产注入先河], *Shanghai Securities News*, September 11, 2013, <http://finance.sina.com.cn/stock/s/20130911/023716724295.shtml>.

channels.⁴¹ Dalian Shipyard, one of the CSIC facilities that received proceeds from the share placement, built the country's first domestically designed aircraft carrier. Subsequently, all other defense conglomerates began issuing public and private equity offerings and bond issuances, although at widely varying levels of intensity.

The average AS rate among defense conglomerates reached 56.9 percent by the end of 2020 (see Figure 4 and Table 2). Aviation Industry Corporation of China (AVIC) led the way with an AS ratio of 83.14 percent. In second place was China South Industries Group Corporation (CSGC), with a ratio of 70.1 percent, closely followed by China State Shipbuilding Corporation (CSSC), with an AS rate of 69.3 percent. These ratios show that the aviation, shipbuilding, and ordnance sectors have warmly embraced AS as a key source of fundraising.

By contrast, the defense electronics and space and missile industries have been far more tentative in leveraging the capital markets. One possible reason is that they have a less pressing need for investment capital compared to their much larger industrial counterparts in the aviation, shipbuilding, and ordnance sectors. The China Aerospace Science and Industry Corporation (CASIC) had the lowest AS rate in 2020, at 14 percent, while the China Aerospace Science and Technology Corporation's (CASC) ratio was 20.8 percent as of 2019. China Electronics Technology Corporation (CETC) had an AS rate of 31.8 percent in 2020, which was still well behind the leading pack. The ordnance sector is split down the middle: whereas CSGC has been very keen, China North Industries Group Corporation (CNGC) has been far more conservative, with an AS rate of only 29.35 percent by 2020.

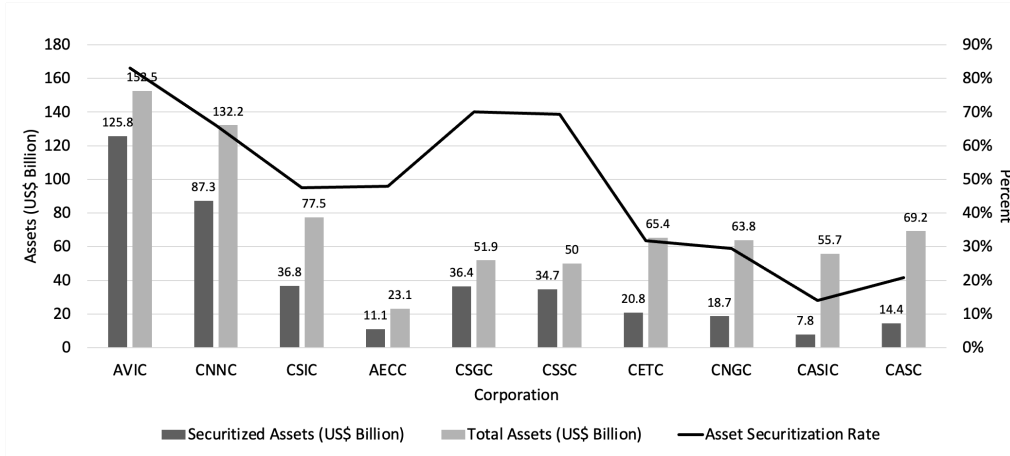
FIGURE 4: ASSET SECURITIZATION TRENDS IN THE CHINESE DEFENSE INDUSTRY, 2012-2020



Source: Data comes from defense company websites, media reports, and stock brokerage reports.

41 "China Navy Plots Course to Stock Market," *Financial Times*, September 11, 2013, <https://next.ft.com/content/4f27d80a-1abb-11e3-a605-00144feab7de>.

FIGURE 5: THE STATE OF ASSET SECURITIZATION AMONG CHINA'S PRINCIPAL DEFENSE INDUSTRIAL CORPORATIONS IN 2020



Source: Data comes from defense company websites, media reports, and stock brokerage reports.

Some Chinese analysts have noted that the AS ratio for U.S. defense prime contractors is between 70 percent and 80 percent and suggest this should be the overall target for the Chinese defense industry. AVIC, CSGC, and CSSC have already reached this level, but the remaining state-owned defense corporations still have some distance to go.

The ten principal state-owned defense corporations raised a combined RMB 2.548 trillion (US\$369.3 billion) between 2012 and 2020, or RMB 283.1 billion (US\$41 billion) on average annually. There has been considerable variation in the amount of funds raised year-over-year (see Figure 5 and Table 3). In 2015, AS deals totaled RMB 357 billion (US\$56.8 billion), but this dropped to just RMB 18 billion (US\$2.6 billion) worth of transactions in 2019 before rebounding to RMB 143.5 billion (US\$20.8 billion) in 2020.

The pace, scale, and reach of AS among Chinese defense enterprises is expected to pick up significantly in the first half of the 2020s, boosted by the three-year reform plan of the state-owned enterprise (SOE) sector by the Chinese government that began in 2020.⁴² One of the central goals of this reform initiative is to promote mixed ownership of SOEs, especially by encouraging private-public ownership of subsidiaries and allowing firms more opportunities to tap the capital markets through AS and other investment instruments. Although this reform effort covers all SOEs, the defense industrial sector will be a major beneficiary, especially companies that have so far lagged behind in the implementation of the AS process. Over the next five years, AS could allow the Chinese defense industry the capacity to raise upward of another RMB 1 trillion (US\$154 billion).

42 "How Will China's SOE Reform Fare with Three Year Action?," Xinhua News Agency, January 29, 2021, http://www.xinhuanet.com/english/2021-01/29/c_139707120.htm.

Weaknesses of the Chinese Defense Industrial Base

Even as the Chinese defense industry has made strong progress in its development since the beginning of the 21st century, there are serious fundamental weaknesses and constraints that, if left unaddressed, will undermine its quest to become a truly world-class technological and industrial powerhouse.⁴³ These problems stem in part from its historical foundations and the problematic efforts to overcome this corrosive legacy. The Chinese defense industry's institutional and normative foundations and workings were copied from the former Soviet Union's command economy—including the flaws that contributed to the Soviet Union's economic woes—and continue to exert a powerful influence today.

Another serious weakness of the Chinese defense industrial system is bureaucratic fragmentation. This is a common characteristic of the Chinese organizational system,⁴⁴ but it is especially virulent within the large and unwieldy defense industrial sector. A key feature of the Soviet approach to defense industrialization that China imported was a highly divided, segmented, and stratified structure and process. There was strict separation between the defense and civilian sectors as well as between defense contractors and military end users, compartmentalization between the conventional defense and strategic weapons sectors as well as among the different conventional defense industrial subsectors, and division between R&D entities and production units. This excessive compartmentalization was driven by an obsessive desire for secrecy and the powerful influence of the deeply ingrained Chinese model of vertical functional systems that encouraged large-scale industries like those in the defense and supporting heavy industrial sectors, such as iron and steel and chemicals, to become independent fiefdoms.

This severe structural compartmentalization is a major obstacle to developing innovative advanced weapons capabilities because it requires consensus-based decision-making through extensive negotiations, bargaining, and exchanges. This management-by-committee approach is cumbersome, risk-averse, and results in a lack of strong ownership, which is critical to ensuring that projects are able to succeed in the thicket of bureaucratic red tape and cutthroat competition for funding.

The research, development, and acquisition system also suffers from compartmentalization along many segments of the acquisition process. Responsibilities for R&D, testing, procurement, production, and maintenance are in the hands of different units, and under-institutionalization has meant that linkages among these entities tend to be ad hoc, with

43 This section draws from the chapter on “Weaknesses in PLA Defense Industries,” in Michael Chase, et al., *China's Incomplete Military Transformation* (Washington, D.C.: RAND Corporation, 2014).

44 Kenneth Lieberthal and Michel Oksenberg, *Policy Making in China: Leaders, Structures, and Processes* (Princeton, N.J.: Princeton University Press, 1988), 35–42. See also Kenneth Lieberthal and David Lampton, eds., *Bureaucracy, Politics, and Decision Making in Post-Mao China* (Berkeley, C.A.: University of California Press, 1992), and David Lampton, ed., *Policy Implementation in Post-Mao China* (Berkeley, C.A.: University of California Press, 1987).

major gaps in oversight, reporting, and information sharing.⁴⁵ The fragmented nature of the acquisition process helps to explain why Hu Jintao was apparently caught by surprise by the first publicized test flight of the J-20 fighter aircraft that occurred during the visit of US defense secretary Robert Gates in January 2011.⁴⁶

Yet another major weakness is that the PLA continues to rely on outdated administrative tools to manage projects with defense contractors in the absence of the establishment of an effective contract management system. The PLA did implement the use of contracts on a trial basis in the late 1980s with the introduction of a contract responsibility system.⁴⁷ These contracts are administrative, however, and have few legal rights because of a lack of a developed legal framework within the defense industry. Consequently, contracts are vague and do not usually define contractual obligations or critical performance issues such as quality, pricing, or schedules. Contracts for complex weapons projects can be as short as one to two pages, according to PLA analysts.⁴⁸

Moreover, the PLA acquisition apparatus is woefully backward in many other management approaches and tools compared to its counterparts in the U.S. and other advanced military powers. It has yet to adopt total life-cycle management methods, for example, and many internal management information systems are on stand-alone networks that prevent effective communications and coordination.

The lack of a transparent pricing system for weapons and other military equipment is another serious weakness that contributes to a deficit of trust between the PLA and the defense industry.⁴⁹ The existing armament pricing framework is based on a “cost-plus” model that dates to the planning economy in which contractors are allowed 5-percent profit margins on top of actual costs.⁵⁰ There are a number of drawbacks to this model that hold back efficiency and innovation. One is that contractors are incentivized to push up costs since it also drives up profits. Another problem is that contractors are not rewarded when they find ways to lower costs, such as through more streamlined management or cost-effective designs or manufacturing techniques. Contracts rarely include performance incentives, discouraging risk-taking and any willingness to adopt new innovative approaches. Yet

45 See Liu Hanrong and Wang Baoshun, eds., *National Defense Scientific Research Test Project Management* (国防科研试验项目管理) (Beijing: National Defense Industry Press (国防工业出版社), 2009).

46 John Pomfret, “Chinese Army Tests Jet During Gates Visit,” *Washington Post*, January 12, 2011; and Elisabeth Bumiller and Michael Wines, “Test of Stealth Fighter Clouds Gates Visit to China,” *The New York Times*, January 12, 2011.

47 Cheung, *Fortifying China*, 83–85.

48 Interview with PLA acquisition specialist, Beijing, November 2011.

49 For a recent effort to estimate the costs associated with Chinese weapon systems, see Jack Bianchi, Madison Creery, Harrison Schramm, and Toshi Yoshihara, *China’s Choices: A New Tool for Assessing the PLA’s Modernization* (Washington, D.C.: Center for Strategic and Budgetary Assessments, 2022).

50 Mao Guohui, ed., *Introduction to the Military Armament Legal System* (军事装备法律制度概论), (Beijing: National Defense Industry Press (北京; 国防工业出版社), 2012), p. 158–59.

another issue is that contractors are dissuaded from making major investments in new technological capabilities or processes because of the low 5-percent profit margin.

To address this long-standing problem, the PLA, Ministry of Finance, and National Development and Reform Commission (NDRC) held a high-level meeting on armament pricing reform in 2009 that concluded that the outdated pricing system had seriously restricted weapons development and innovation.⁵¹ Several reform proposals were put forward that (1) provide incentives to contain costs, (2) switch from accounting procedures that focus on ex post pricing to ex ante controls, and (3) expand from a single pricing methodology to multiple pricing methods. Some of these ideas were incorporated in a document issued after the meeting titled “Opinions on Further Pushing Forward the Reform of Work Concerning the Prices of Military Products.”⁵²

At the beginning of 2014, the General Armaments Department (GAD) announced that it would conduct and expand pilot projects on equipment pricing. These reforms included the strengthening of pricing verification of purchased goods, improving cost controls, shifting from singular to plural pricing models, from “after-purchase pricing” to “whole-process pricing,” and from “individual cost pricing” to “social average cost pricing.”⁵³ These represent modest steps in the pricing reform process, but the PLA will continue to face fierce opposition from the defense industry on this issue.

Lastly, a huge impediment is corruption, which has thrived with the defense industry’s uncertain transition from centralized state planning to a more competitive and indirect management model. PLA leaders have highlighted the defense acquisition system as one of a number of high-risk areas in which corruption can flourish. At the PLA’s annual conference on military discipline inspection work in January 2014, Central Military Commission (CMC) vice-chairman General Xu Qiliang, who heads the PLA’s anti-corruption efforts, pointed out that armament research, production, and procurement was one of two areas that required “better oversight.”⁵⁴ The other area was construction projects.

There has been little public reporting on corruption in the defense industry and acquisition system—many cases involve classified weapons programs—which means that the full magnitude of the problem is impossible to assess. However, occasional cases have been disclosed that hint at the scale of the corruption problem in the defense industry. One of the biggest offenders is China Shipbuilding Industry Corporation (CSIC), which has witnessed the arrest and imprisonment of several of its most senior executives. The most prominent

51 Zong Zhaodun and Zhao Bo, “Major Reform Considered in Work on the Prices of Our Army’s Armaments,” *Liberation Army Daily* [解放军报], November 18, 2009.

52 Ibid. The actual document was not publicly released.

53 Zhang Xiaoqi, “Armament Work: It Is the Right Time for Reform and Innovation,” *Liberation Army Daily*, February 13, 2014.

54 Zhang Qian and Yao Chun, “CMC Vice Chairman Stresses Effective Anti-Corruption,” Xinhua News Agency, January 17, 2014, <http://en.people.cn/90786/8515367.html>.

was Hu Wenming, the corporation's chairman and Communist Party chief during much of the 2010s.⁵⁵ A second top-level executive was Sun Bo, CSIC's general manager, who received a twelve-year prison sentence in 2019.⁵⁶ Sun was in charge of the refurbishment of the Liaoning aircraft carrier, and although he was targeted for corruption, there were media reports that Sun's real crime was espionage. There is no public information to suggest that other defense firms have suffered a similar degree of endemic corruption, but the CSIC case does show that corruption occurs in the Chinese defense industry and can reach to the highest levels and spread widely.

The Impact of the Ukraine War on the Chinese Defense Industry

The Ukraine War holds significant challenges but also opportunities for the Chinese defense industry, even though it has had no direct involvement in the conflict so far. A starting point for Chinese defense industrial decision-makers in assessing the implications of the Ukraine War is how useful the war is as a template for the future technological and industrial underpinnings of military conflict. The war has been a classic 20th Century industrial age model of attritional warfare with pockets of 21st Century high-tech innovation such as networking and the creative use of drones.

The Chinese defense industry's pathway of long-term technological and industrial development is largely laid down by the People's Liberation Army's (PLA) doctrine of "Informatized Local Wars," which is the waging of intensive high-technology wars in an information-centric environment with limited attention paid to industrial era mechanized warfare. This is fundamentally the inverse of the Ukraine War but more aligned with the lessons of other modern conflicts, such as the U.S.-led campaigns against Iraq in 1991 and 2003. As the Chinese defense industry has already invested considerable resources and effort to build an innovation and industrial apparatus in which information-centric and increasingly "intelligentized" (emerging disruptive technological capabilities for the artificial intelligence age) warfare is its central focus, the long-term ramifications of the Ukraine War may be limited.

In applied operational terms, what are the lessons of the Ukraine War for China's military preparedness for a Taiwan contingency and, more broadly, for military strategic competition against the U.S.? One obvious lesson for the PLA is the need to ensure adequate munition stockpiles for prolonged wartime use. As China has not been involved in a major war since 1979, it has little institutional know-how on war sustainment.

55 Teddy Ng, "Former Boss of China Aircraft Carrier Programme in Corruption Probe," *South China Morning Post*, May 15, 2020.

56 Minnie Chan, "12 Years Behind Bars for Corrupt Former Boss of Chinese Warship Builder CSIC," *South China Morning Post*, July 4, 2019.

From a broader developmental perspective, the Russian defense industry and its Soviet predecessor casts a long and influential shadow on the Chinese system. The organizational and industrial foundations of the Chinese defense industrial complex were imported almost wholesale from the Soviet Union in the 1950s, and although there was a break in relations between the two countries from the 1960s to the 1980s, the Soviet legacy remained powerful.

When Sino-Russian defense technological and industrial ties resumed at the beginning of the 1990s, China imported tens of billions of dollars' worth of weapons, components, technological know-how, and industrial capacity from the Russian defense industry, both legally and illicitly. Russia's military-technological imprint is clearly visible across the PLA's front-line arsenal with numerous types of fighter aircraft, transport planes, air defense systems, and naval vessels derived from Russian models.

Beyond these challenges, a golden opportunity has opened up for China to replace Russia as a top-tier arms exporter as the Ukraine War and accompanying Western sanctions will likely turn Russia into a net military importer for the foreseeable future. The timing could not be better, as the Chinese defense industry is in the process of upgrading its brand image from an affordable manufacturer of "good enough" lower-quality arms to an upper-tier builder of advanced generations of state-of-the-art weapons. This could represent a highly lucrative income stream to help support China's ambitious defense transformation if this market grab is successful.

Prospects for Future China-Russia Defense Technological and Industrial Cooperation

The Ukraine war has temporarily paused the China-Russia defense industrial relationship as Beijing has sought to avoid getting dragged into the conflict and protect its companies from being caught in the proliferation of sanctions that have cut Russia off from the rest of the world. But this hiatus is likely to be short-term, and the question is not if but when, at what scale, and in which domains Sino-Russian techno-security cooperation will resume. This issue flared up in February 2023 when the Biden Administration said that it had intelligence that China was thinking of allowing the supply of lethal military capabilities to Russia, with subsequent media reporting indicating this might cover armed drones and artillery-related armaments.⁵⁷ U.S. officials subsequently said that there was no evidence that China had given the go-ahead for the arms sales.⁵⁸

57 "Blinken Says He Warned China Over Providing Weapons to Russia", *The New York Times*, February 19, 2023, "China Reportedly Negotiating with Russia To Supply Kamikaze Drones", *Spiegel International*, February 23, 2023, and "As China Calls for Peace, U.S. Believes Beijing Is Considering Artillery and Drone Deliveries to Moscow", *The Wall Street Journal*, February 24, 2023.

58 "China Has Not Yet Supplied Arms to Russia in its War with Ukraine, U.S. Officials Say", *The Washington Post*, 26 February 2023.

The development of strategic deterrence capabilities is where there appears to be the greatest convergence of mutual interests between the two countries. These capabilities will be primarily directed against the United States, which is the paramount threat for both Beijing and Moscow. At the 20th Party Congress in October 2022, China’s strongman leader Xi Jinping highlighted the need to “establish a strong strategic deterrence system” that includes the development of unmanned and intelligentized combat capabilities. Russia’s latest defense modernization plans have placed top priority on the development of new generations of intercontinental ballistic missiles, hypersonic missiles, laser weapons, nuclear submarines, and autonomous systems.⁵⁹

The Chinese and Russian defense industries have a far better chance of successfully meeting the challenges of the Ukraine War and the intensifying techno-military competition with the U.S. together than separately. If these two statist defense industries are able to forge together an effective and enduring defense technological and industrial relationship, they will pose a far more complex and credible military challenge to the U.S.

Comparing the U.S. and Chinese Defense Industries

The U.S. and Chinese defense industries dominate the global defense industrial landscape. In the 2022 ranking of the world’s 100 largest defense firms by *Defense News* for revenue for 2021, U.S. defense corporations occupied eight of the top 20 places, including the top five, while Chinese defense primes had seven slots that included three in the top ten. Together, U.S. and Chinese firms accounted for 15 of the top 20 defense corporate positions.

59 Evan Braden Montgomery and Toshi Yoshihara, *Speeding Toward Instability? Hypersonic Weapons and the Risk of Nuclear Use* (Washington, D.C.: Center for Strategic and Budgetary Assessments, 2023), chapter 2.

TABLE 3: U.S. AND CHINESE DEFENSE PRIMES IN THE TOP 20 LIST OF GLOBAL DEFENSE CORPORATIONS

2022 Rank	Company	Country	2021 Defense Revenue (in millions)	2021 Total Revenue (in millions)	Revenue From Defense
1	Lockheed Martin	U.S.	\$64,458.00	\$67,044.00	96%
2	Raytheon Technologies	U.S.	\$41,852.20	\$64,388.00	65%
3	Boeing	U.S.	\$35,093.00	\$62,286.00	56%
4	Northrop Grumman	U.S.	\$31,429.00	\$35,667.00	88%
5	General Dynamics	U.S.	\$30,800.00	\$38,500.00	80%
6	Aviation Industry Corp. of China (AVIC)	China	\$30,155.22	\$80,424.24	37%
8	China State Shipbuilding Corp. (CSSC)	China	\$18,517.72	\$92,573.10	20%
9	China North Industries Group Corp. (NORINCO)	China	\$17,711.93	\$81,648.42	22%
10	L3Harris Technologies	U.S.	\$14,924.00	\$17,814.00	84%
11	China Electronics Technology Group (CETC)	China	\$14,659.22	\$57,629.62	25%
13	China South Industries Group Corp. (CSIGC)	China	\$13,744.95	\$44,349.55	31%
14	China Aerospace Science and Industry Corp. (CASIC)	China	\$13,125.11	\$41,033.41	32%
17	HII	U.S.	\$9,475.00	\$9,524.00	99%
18	China Aerospace Science and Technology Corp. (CASTC)	China	\$9,344.09	\$43,636.74	21%
19	Leidos	U.S.	\$8,032.00	\$13,737.00	58%
Total U.S. Corporate (8)			\$236,063.20	\$308,960.00	76.4%
Total Chinese Corporate (7)			\$117,389.15	\$441,295.08	26.6%

Source: 2022 Top 100 Defense Firms, *Defense News*, 29 August 2022, <https://people.defensenews.com/top-100/>

The top 20 table offers useful insights comparing the U.S. and Chinese defense industrial bases:

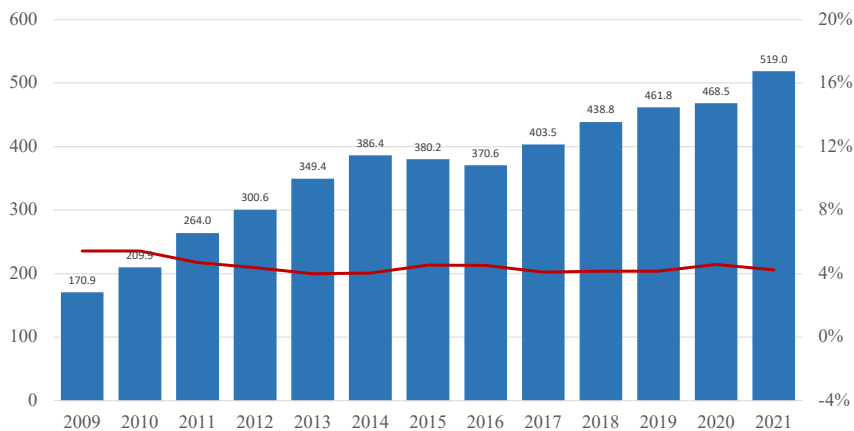
- The U.S. defense industrial base generates twice as much defense revenue as its Chinese counterpart: \$236 billion compared to \$117.4 billion. However, the Chinese defense industrial base earned one-third more total revenue (civilian and defense) than the U.S.: \$441.3 billion vs. \$309 billion.

- Although U.S. defense firms claimed the top 5 rankings based on defense revenue, Chinese firms (CSSC, AVIC, and NORINCO) would occupy the top three slots if measured in total revenue.
- More than three-quarters of total revenue generated by the U.S. defense industrial base comes from defense-related activities. By contrast, only around one-quarter of total revenue of Chinese defense primes is defense-related.
- U.S. and Chinese firms from across the defense industrial economy are represented in the top 20 ranking, including aviation, shipbuilding, space and missiles, electronics, and ordnance sectors.

The largest Chinese defense prime in terms of defense revenue is AVIC, and the story of its robust growth over the past decade or more is characteristic of the improved fortunes of the entire Chinese defense industry during this same period. AVIC enjoys a monopolistic dominance of the Chinese military aviation industry, and its subordinate enterprises are responsible for the production of virtually the entire frontline arsenal of the Chinese air force and naval air force. The Chengdu Aircraft Corp., for example, manufactures the J-10 and J-20 fighter aircraft, while the Shenyang Aircraft Corp. produces the J-11 and J-15 fighter aircraft.

AVIC has enjoyed a sustained period of strong growth in the 21st century. Its annual revenues have risen from Rmb 171 billion in 2009 to Rmb 519 billion in 2021, a tripling in value over 12 years (see Figure 6). Its annual profit margins are between 4-6%. Around one-third of AVIC's total annual revenue comes from defense sales, which is significantly higher than other Chinese defense primes.

FIGURE 6: FINANCIAL PERFORMANCE OF AVIC, 2009-2021



Source: Data compiled from AVIC website and media reports.

CHAPTER 4

Assessing the U.S.-China Techno-Security Rivalry

This concluding chapter carries out a direct comparative net assessment of the strengths and weaknesses of the U.S. and Chinese techno-security systems to determine their relative standing against each other. Specifically, it examines five key factors that are central to how these systems are organized and perform.⁶⁰

First is the role of external threat perceptions and the threat environment. The pace and scale in the building of techno-security capabilities are closely tied to how states assess the nature and severity of threats to their national security. Second is the nature and configuration of the leadership and management coordination arrangements within a techno-security system, which could be anti-statist-style decentralized bottom-up, statist-oriented centralized top-down, or a combination of these two approaches. Third is the governance regime that regulates the activities of actors within the system. How interventionist are these governing rules, and is their purpose to incentivize or penalize behavior? Fourth is the role of public-private relationships and the level of dual-use civil-military integration between the defense and civilian segments of the economy. Is there close collaboration between state and private entities, especially in the research, industrial, and commercial arenas, and how accessible is the military apparatus for civilian enterprises? Fifth is the nature of the fundamental orientation of the techno-security system between the domestic and external environments. Is the techno-security system dominated by techno-nationalist impulses that emphasize self-reliance and indigenization or is it more inclined to techno-globalist

60 See Linda Weiss, *America Inc.? Innovation and Enterprise in the National Security State* (Ithaca, N.Y.: Cornell University Press, 2014), Mark Z. Taylor, "Toward an International Relations Theory of National Innovation Rates," *Security Studies* 21, no. 1 (2012), and Friedberg, *In the Shadow of the Garrison State*.

engagement where it seeks to cooperate closely with foreign partners and tap into external markets.⁶¹

External Threat Perceptions and Threat Environment: China began to assess the United States as a high-priority techno-security threat in the late 1990s and mobilized its techno-security system quietly to address these concerns, which have only grown more menacing in the past decade. The United States, by comparison, was slow and distracted by the global war on terrorism during the first decade of the 2000s to assess China as a serious techno-security concern. As China ramped up its efforts at innovation and military modernization from the beginning of the 2000s, U.S. assessments of these efforts were that they posed little strategic threat as Chinese capabilities were far behind U.S. levels. The U.S. government did not begin to mobilize its techno-security system until the late 2010s. *The overall assessment is that China was the first mover in the U.S.-China techno-security strategic competition, which allowed it to significantly narrow the gap with the United States.*

Leadership and Management Coordination: China has a well-developed centralized, top-down coordination model that has been a key ingredient in the successful development of the Chinese techno-security system. By contrast, the United States techno-security system follows a more decentralized bottom-up coordination model in which management and oversight responsibility are divided among multiple mission-oriented government agencies that coordinate closely together. *The overall assessment is that the United States has an efficient model ideal for routinized technological development, but China's approach is effective for rapid catch-up and for engaging in high-risk early-stage disruptive technological development.* The big unknown question is whether technological change in the techno-security domain in the coming years will be driven more by incremental or radical technological change.

Governance Regime: The Chinese governance regime relies on state administrative controls and penalties to ensure compliance. Moreover, as discussed in chapter 3, bureaucratic fragmentation, compartmentalization, and systemic corruption are also prominent features of the overall Chinese system. Under the Xi administration, this has translated into frequent and harsh crackdowns against constituencies affiliated with the techno-security system, such as the military and high-technology sectors. The U.S. regime, by contrast, uses more indirect and positive governance mechanisms that emphasize incentives and rewards to ensure compliance by the private sector, such as the ability to make profits. *Overall, the United States has a far superior model, and the governance regime is potentially the critical Achilles heel of the Chinese model.*

Public-Private Relationships and Civil-Military Integration: China at present is in the early stages of forging public-private partnerships and implementing military-civil

⁶¹ For a recent attempt to develop and apply a framework to assess military innovation, see Thomas G. Mahnken, Evan B. Montgomery, and Tyler Hacker, *Innovating for Great Power Competition: An Examination of Service and Joint Innovation Efforts* (Washington, D.C.: Center for Strategic and Budgetary Assessments, 2023).

fusion. The public sector, though, will remain the dominant player, and the private sector will remain confined to a secondary supporting role for the long term. In sharp contrast, the United States has a well-developed and mature model of public-private partnerships and civil-military integration. There is a strong track record of merging public and private institutions in novel ways to produce fused, balanced hybrid entities. *The overall assessment is that the U.S. has a significant advantage with a well-developed, if aging, dual-use integrated model, while China's approach is still in its infancy and will suffer from a structural statist bias in its development.*

Techno-Nationalist vs. Global Engagement Approaches: China seeks long-term technological self-reliance but is heavily dependent on foreign technology and know-how for now. The United States is able to meet its own techno-security needs through its domestic base, but also supplies foreign countries through export and collaboration. *Overall, the United States enjoys a dominant position in the global techno-security order, but needs to do much better to forge collaborative foreign partnerships. China lags by a large margin, although it is making incremental progress in expanding its global techno-security footprint. The international system will be a pivotal arena for long-term techno-security competition between the United States and China and will likely play an outsized influence in shaping the outcome of this competition.*

Overall, the United States is superior in the three categories of public-private partnerships and civil-military integration, governance, and techno-nationalism vs. global engagement. These areas are especially critical for enhancing the performance of the techno-security system by dealing with coordination issues between the state and the private sector as well as facilitating cooperation with foreign countries. If the U.S. is able to build on its present advantages in these three areas and address shortcomings, it is well-placed to maintain and even build upon this leadership.

China is ahead in threat motivation, but the U.S. has finally woken up and made China its undisputed adversary. The problem for the U.S. is whether it can concentrate sufficient resources to deal with China while simultaneously having to meet serious security challenges elsewhere around the world, especially Russia and the Middle East. Lastly, both the U.S. and China are matched evenly in leadership and management coordination, although from opposing anti-statist and statist approaches. How these two techno-security systems each adapt and keep ahead of the rapid revolutionary changes in the techno-security domain will determine which of them will prevail over the long run.

In conclusion, the U.S. techno-security system remains better organized and structured for the long-term techno-security competition than China, but it cannot be complacent and needs to urgently address a raft of structural flaws in its system. As China ramps up its efforts to transform its techno-security capabilities and sets deadlines to achieve its goals over the next 5–10 years, the U.S. has only a limited window of opportunity to act.

LIST OF ACRONYMS

AI	Artificial Intelligence
ARPA	Advanced Research Projects Agency
AS	Asset Securitization
AUKUS	Australia-United Kingdom-United States
AVIC	Aviation Industry Corporation of China
CASIC	China Aerospace Science and Industry Corporation
CASC	China Aerospace Science and Technology Corporation
CCP	Chinese Communist Party
CETC	China Electronics Technology Corporation
CMC	Central Military Commission
CSGC	China South Industries Group Corporation
CSIC	China Shipbuilding Industry Corporation
CSSC	China State Shipbuilding Corporation
DARPA	Defense Advanced Research Projects Agency
DoD	U.S. Department of Defense
DSTG	Australian Defense Science and Technology Group
GAD	General Armaments Department
ITAR	International Traffic in Arms Regulations
MIIT	Ministry of Industry and Information Technology
NASA	National Aeronautics and Space Administration
NDRC	National Development and Reform Commission
NORINCO	China North Industries Group Corporation
NTIB	National Technology and Industrial Base
OSRD	Office of Scientific Research and Development
PLA	People's Liberation Army
PRC	People's Republic of China
R&D	Research and Development
RMB	Renminbi
SASTIND	State Administration for Science, Technology, and Industry for National Defense
SOE	state-owned enterprise
UAV	unmanned aerial vehicle
UUUV	unmanned undersea vehicle



Center for Strategic and Budgetary Assessments

1667 K Street, NW, Suite 900

Washington, DC 20006

Tel. 202.331.7990 • Fax 202.331.8019

www.csbaonline.org