UNIVERSITY OF CALIFORNIA

China and the U.S. Compete for Global Techno-Security Dominance

Tai Ming Cheung

Summary

In the struggle for global geo-strategic and geo-economic supremacy between the United States and China, the techno-security sphere where economics, technological innovation, and national security meet has become a principal battleground. Two contrasting models are pitted against each other: China's state-led top-down approach and the United States' market-driven bottom-up system. 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 brief examines the underpinnings of U.S.-China great power techno-security competition and assesses what the countries' different approaches imply for future techno-security rivalry.

IGCC

IGCC Policy Brief
July 2022

The Nature of the U.S.-China Techno-Security Rivalry

Today's rivalry between the United States and China extends across the entire spectrum of their relationship, but nowhere are the battle lines more clearly drawn than in the techno-security sphere, which encompasses efforts to build up technological, defense, and national security capabilities. In the long-term contest for supremacy in this domain, the U.S. and China have forged formidable techno-security states: innovation-centered, security-maximizing regimes that prioritize the building of technological, defense, and national security capabilities to meet expansive national security requirements based on heightened threat perceptions and the powerful influence of domestic pro-security coalitions.

China's progress in this effort, in terms of pace, scale, and quality of output, has been impressive. At the outset of the reform drive, in the 1990s, the Chinese defense science, technology, and innovation system was in a spiraling decline and could only produce outdated foreign-derived weapons. By the second half of the 2010s, select pockets of excellence within the defense innovation system began to turn out advanced armaments that only the likes of the United States are able to do, such as stealth fighter aircraft and large-sized aircraft carriers and the strike planes that fly off their decks.

The United States, though late to recognize the challenge posed by China, is now mobilizing to counter Chinese influence.

The long-term outcome of the U.S.-China techno-security competition will hinge on whoever is most effective in harnessing their constituent core strengths while mitigating against critical weaknesses.

While the two countries draw upon profoundly contrasting tenets, attributes, and approaches, they do share comparable strategic designs and desired outcomes for the configuration of their sprawling techno-security ecosystems. Moreover, unlike in the Cold War when the United States far outmatched the Soviet Union economically and technologically, the gap between the United States and China in economic, human resource, and technological capabilities is much narrower.

From an ideological perspective, the U.S. techno-security state is anchored in a deeply held anti-statist ethos that emphasizes limited government and an expansive leading role for the private sector. The Chinese techno-security state on the other hand is overwhelmingly statist with the party-state dominating ownership, control, and management. Though these distinctions are broadly true, the anti-statist versus statist divide between the two countries is not completely black and white. Strong pro-statist forces in the United States have allowed the government to exert a powerful influence in making and shaping the techno-security state. In China, pro-market forces have steadily gained acceptance and prominence, although the techno-security state has lagged in opening up compared to other parts of the economy.

Nonetheless, the United States and Chinese techno-security states are designed, configured, and operated very differently from each other. Their divergent approaches make for an intriguing matchup.

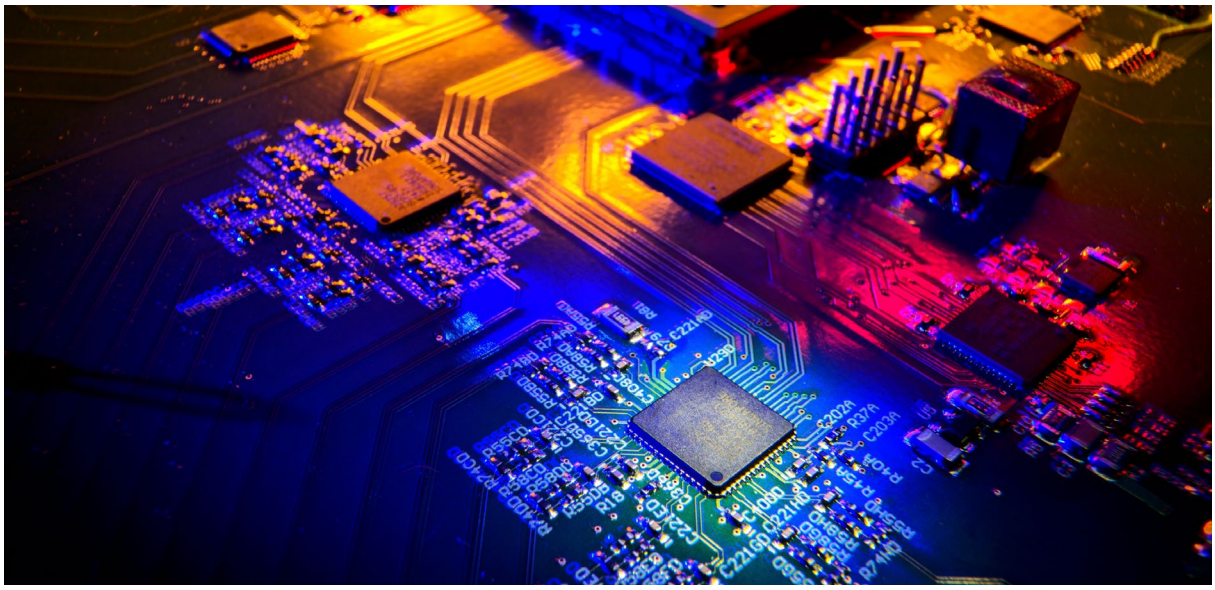

Photo: U.S. Government, CC0 1.0

The Concept of the Techno-Security State

The techno-security state refers to an innovation-centered, security-maximizing regime that prioritizes the building of technological, defense, and national security capabilities to meet expansive national security requirements based on heightened threat perceptions and the powerful influence of domestic pro-security coalitions.

In the small number of studies that have been conducted centered on the role of the technology-security nexus in state development, five factors stand out as being especially important in helping to explain the make-up and performance of techno-security states.[1]

First is the coordination of leadership and management entities within the techno-security ecosystem, which could be either decentralized bottom-up, centralized top-down, or a combination of the two. Second is the nature of the governance regime employed by the state to secure the participation of enterprises and other actors. Is it by incentives and rewards or through control and penalties? Third is the degree of hybridization taking place between public and private institutions and between the civilian and defense/military sectors. Fourth is the nature of threat perceptions and the threat environment. And fifth, is the role of techno-nationalist ideology and strategies including, at one end of the spectrum, statist-minded regimes that believe that only a state-controlled and closed-door approach to technological innovation can safeguard national security, economic competitiveness, and international status, and, at the other, anti-statist regimes that are market-oriented, self-reliant, and technologically advanced, but are willing to share their technological capabilities for profit and strategic advantage.

[1] These studies include: Etel Solingen, Ed, *Scientists and the State: Domestic Structures and the International Context* (University of Michigan Press, 1994); 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); Richard Samuels, *Rich Nation, Strong Army* (Ithaca, N.Y.: Cornell University Press, 1994); and Linda Weiss, *America Inc.? Innovation and Enterprise in the National Security State* (Ithaca, N.Y.: Cornell University Press, 2014).

The Chinese Techno-Security State: Drivers and Approaches

Since coming to power at the 18th Party Congress in 2012, Chinese President Xi Jinping has significantly elevated the importance of national security and technological innovation in the country's overall priorities and established an expansive techno-security state. A vast program of military strengthening, military-civil fusion, and economic securitization, based upon his strategic and ideological vision and under his close personal control through direct command of key institutions, has placed innovation and security at the heart of the country's future.

Dire Threat Perceptions Drive Chinese Techno-Security Innovation

What is driving Xi to build this fierce and wide-ranging techno-security state? In China, pessimistic perspectives on the country's global situation are pervasive among Chinese leaders. The Chinese authorities have used deepening concerns over the external security environment since the late 1990s, and 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. Though China's 14th Five Year Plan (FYP) does not explicitly identify the United States as the chief culprit responsible for China's worsening international security situation, speeches given by Xi around the time that the 14th FYP was being drafted make clear that the United States was considered the main adversary. These perceptions of the U.S. threat have only grown more dire, pressing, and expansive under Xi's tenure and are a hugely powerful existential motivating factor in driving the development of the Chinese techno-security state.

State-led Market Coordination Drives Innovation

Centralized top-down coordination has been instrumental to many of China's signature strategic technological achievements from nuclear weapons and ballistic missiles to the manned space program and high-performance computers. This top-down approach to governance is being revamped and reprioritized from foreign absorption to promote original, homegrown innovation. 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.

Controlled interdependence has been the principal governance model used by the Chinese techno-security state since its inception. This refers to the adoption of a central 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. While there has been some relaxation and roll-back of this pervasive state control in the post-1978 reform era, 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 its attention on setting broad high-level developmental directions instead of hands-on micro-management. This is what Barry Naughton describes as "grand steerage," in which the Chinese authorities have issued numerous development "plans" that refer to "initiatives that involve real expenditure of resources to achieve concrete outcomes."[2]

Naughton points to a slew of techno-industrial policies such as the 2006–2020 Medium and Long-Term Science and Technology Development Plan, Strategic Emerging Industries initiative, and the Innovation-Driven Development Strategy as examples of this grand steerage, which would fall within the purview of the techno-security state.

This less direct but still significant engagement of the state in economic management combined with more effective coordination with market mechanisms can be labelled as steered interdependence. Another newly emerging example of this steered interdependence approach is the "New-Whole-of-Nation System" concept, which has been especially applied to the development of key science and technology projects. The New-Whole-of-Nation System mechanism, which began to be rolled out toward the end of the 2010s, seeks to acquire investment funds by tapping financial markets using asset securitization and government guidance funds as key vehicles. If the New-Whole-of-Nation System approach becomes widely adopted, it would mark an important shift from the heavy hand of the state to a more balanced and coordinated state-market partnership. However, the Chinese government's harsh regulatory crackdown in 2021 against private-sector big technology companies such as Alibaba, Tencent, and Bytedance has called into question whether these tentative moves towards a steered interdependence have ended and the Xi administration has returned instead to imposing more heavy-handed direct state control mechanisms.[3]

Barriers to Hybridization But Strong Political Will to Achieve It

Hybridization has yet to make a significant impact on the Chinese techno-security state, but the foundations for a robust and expansive military-civil fusion (MCF) framework have been laid since the second half of the 2010s. The Chinese ambition is that its hybrid MCF model will become as extensively developed as in the United States within the next decade or so. While the structural barriers to realizing this goal are high, the top-level political will to achieve this, as exemplified by Xi's active leadership of the MCF initiative, means the prospects for success are positive. The challenge for the United States is whether it can stay ahead through revamping its civil-military integration setup and find ways to undermine the Chinese effort.

Moving Towards Self Reliance

The heightened priority of 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. But gaining access to and leveraging foreign technology and knowledge will continue to be an essential feature for the long term, 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 and provides a safeguard, while the forging of an original innovation capacity is a long-term high-risk endeavor.

[2] Barry Naughton, The Rise of China's Industrial Policy: 1978-2020 (Mexico City: Universidad Nacional Autónoma de México, 2021). And Barry Naughton, "Grand Steerage," in Thomas Fingar and Jean C. Oi (Eds), *Fateful Decisions: Choices That Will Shape China's Future* (Stanford, C.A.: Stanford University Press, 2020), 54. Other analysts like Nicholas Lardy also point to the resurgent role of the state in economic development, especially in resource allocations and boosting the importance and reach of the state sector. See Nicholas R. Lardy, *The State Strikes Back: The End of Economic Reform in China* (Washington, D.C.: Peterson Institute for International Economics, January 2019).

[3] Barry Naughton, "What's Behind China's Regulatory Storm", *Wall Street Journal*, 12 December 2021, https://www.wsj.com/articles/what-is-behind-china-regulatory-storm-11638372662?st=2ohpcyanvekked9&reflink=desktopwebshare_twitter

BOX 1

The Risks of Decoupling—for China and the U.S.

The long-term viability of China's techno-nationalist ambitions will be put in grave doubt if the U.S.-led effort to significantly reduce and perhaps fully decouple technological relations with China is 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. While the U.S. and Chinese techno-security ecosystems had far fewer interactions because of tight restrictions imposed by their governments, there was still considerable cooperation on matters deemed to not infringe on national security.

The implications of decoupling are markedly different in the techno-security realm compared to the economic or academic spheres. In non-security arenas, decoupling is costly and detrimental to both sides.[4] 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. In the aggregate though, the U.S. techno-security state would be far less negatively impacted by decoupling than its Chinese counterpart.

Photo: Chris from Shenzhen, China, CC BY-SA 2.0

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. This would require the United States and China to find a stable of 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, artificial intelligence (AI), quantum technology, cybersecurity, clean energy, and biotechnology. Forging a winning multilateral coalition will not be easy for either country.

[4] 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 U.S. Techno-Security State: Drivers and Approaches

Growing Recognition of the China Threat

U.S. threat perceptions and responses to China's techno-security rise, typically a catalytic factor that exerts a powerful influence in spurring the techno-security state into action, only had a peripheral impact until the late 2010s. As China ramped up its efforts at innovation and military modernization from the beginning of the 2000s, U.S. assessments were that they posed little strategic threat as Chinese capabilities were far behind. The United States was also consumed by the global war on terror and threats emanating from the Middle East after the September 11, 2001, terrorist attacks. This meant that security worries over China, especially over escalating tensions across the Taiwan Strait, which had begun to gain heightened attention by U.S. leaders at the turn of the 21st century, were relegated in priority.

The United States only elevated China to the top of its threat list with the unveiling of the Third Offset Strategy in 2014, which was intended to address the erosion in U.S. military technological superiority caused by initiatives such as China's so-called anti-access/area-denial capabilities.

Public-Private Partnerships and Investment in Techno-Security R&D

In contrast to China's governance approach of controlled interdependence, the U.S. has governed its techno-security state through governed interdependence. The U.S. uses incentives and rewards like cost sharing to ensure that private firms meet requirements, thereby allowing national security-focused problems to be addressed while also satisfying the goals of private sector, which are absorbing risk and ensuring profitability.

The mutually rewarding partnership between the public and private sectors has been a particularly important driver of U.S. economic and technological performance. However, the public-private relationship has become increasingly stale and less central and relevant in the 21st century. This threatens to turn this pillar of strength into a source of weakness.

First, the defense acquisition system has become increasingly rigid and risk-adverse, which has meant that business is mostly carried out with long-time trusted contractors. The result is that the techno-security state, and especially the defense establishment, is isolated from large portions of the most innovative and thriving commercial sectors of the economy.
Second, the U.S. techno-security state 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 (R&D) has eroded. Many technologies originate in the civilian sphere and are subsequently—and often belatedly—adapted for defense and dual-use applications. While this is cost-efficient and allows access to a more extensive pool of innovation, the U.S. techno-security state 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, especially in the highly fluid intersection between economics, trade, investment, technology, defense, and national security.

Reinvigorating the public-private relationship will be critical in any effort by the United States to credibly compete against China over the long term.

Collaboration with Global Partners is Increasingly Necessary

Another driver of the success of the U.S. techno-security state is techno-nationalist primacy—engagement with foreign countries—which has played a secondary role in the development of the U.S. techno-security state but offers considerable potential going forward as the United States promotes technology and industrial relationships with advanced allied countries.

As the world's most advanced techno-security power since World War II, the United States has been the dominant exporter of advanced technology, knowledge, and industrial products, both in the military and civilian spheres. Having a comprehensive world-class science and technology base, especially in the defense technological arena, has meant the United States has had little appetite to acquire foreign technology or know-how. This has led to the building of a fierce and enduring techno-nationalist ideology and posture.

But the global technological landscape has undergone rapid change 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 R&D 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. But the U.S. national technology and industrial base has faced substantial political, legislative, and bureaucratic hurdles from within the techno-security state, for example, in the limiting of technology-sharing arrangements, such as cooperation agreements with Canada, the United Kingdom, and Australia. Techno-nationalist primacy has been deeply entrenched within the institutional culture of the U.S. techno-security state for so long that a more collaborative techno-globalist approach is likely to continue to encounter stiff resistance and will take time to effectively implement. Further, the U.S. government will need to develop a more robust and joint whole-of government approach than the ad hoc and underdeveloped process that currently exists.

Conclusion

The U.S. techno-security state in the opening years of the 2020s remains much stronger and more innovative than its Chinese counterpart. This dominance is being steadily eroded, however, by U.S. institutional sclerosis, far-reaching global technological changes, and China's intensive pace of techno-security development. Revitalizing key components of the U.S. techno-security state, especially the acquisition process and techno-nationalist primacy, will allow the United States to retain its global leadership over the long-term, although the gap with China will continue to shrink. The United States will need to undertake more transformative reforms to stay well ahead. Much will also depend on how serious the United States is about dealing with the long-term Chinese techno-security challenge to its national security and global leadership role given numerous competing domestic and international demands.

For China, the revamping of the techno-security state under Xi has seen the gap steadily close with the United States and the global technology frontier. But even more significant structural changes will be required to successfully transition from catching up to gaining parity or leading. Moving more of the techno-security ecosystem from controlled interdependence to steered interdependence will be essential. Allowing hybridization to be fully implemented will also be a vital step. The enhancement of the centralized top-down coordination model will be especially important in the race for the development of emerging core technologies as active early state intervention can play a more effective and decisive role than bottom-up market support. The Chinese techno-security state will need to address these key deficiencies if it is to mount a realistic challenge against the United States for long-term global techno-security leadership.

TABLE 1

Key Characteristics of the Chinese and U.S. Techno-Security States

Key Development and Functional Factors

	China	United States
External Threat Perceptions and Threat Environment	*Leading Catalytic Factor:* China assessed U.S. as a high-priority techno-security threat since the end of the 1990s	*Lagging Catalytic Factor:* U.S. was distracted and slow to assess China as a serious techno-security concern until the late 2010s
Leadership and Management Coordination	*Centralized Top-Down Coordination:* Selective authoritarian mobilization and innovation model is a central source of success in the development of China's techno-security state	*Decentralized Bottom-Up Coordination:* Responsibility is divided among multiple, mission-oriented government agencies that coordinate closely together
Governance Regime	*Controlled Interdependence:* This governance model grew out of the Maoist central planning command system culture and relies on administrative controls and the use of penalties to ensure compliance	*Governed Interdependence:* The state uses incentives and rewards like cost sharing to ensure that private firms meet requirements. This design allows national security-focused purpose and mission-oriented problem sets of the techno-security state to be met while also satisfying the goals of the private sector, which are absorbing risk and ensuring profit
Hybridization	*Early-Stage Hybridization:* Military-civil fusion is at a preliminary stage of development, but the public sector will remain the dominant player with the private sector more limited	*Mature-Stage Hybridization:* The merging of public and private institutions in novel ways produces fused hybrid entities. Vehicles include "public interest" firms, federally funded R&D centers, and commercial consortia between industry, academia, and government entities
Techno-Nationalist Ideology and Strategies	*Techno-Nationalist Dependence:* China seeks long-term technological self-reliance but is heavily dependent on foreign technology and know-how in the meantime	*Techno-Nationalist Primacy:* The U.S. is able to meet its own security needs through its domestic techno-security base, but also supplies foreign countries through export and collaboration

TABLE 2

Strengths and Weaknesses of Chinese and U.S. Techno-Security Policy

	China	United States
Strengths	• Xi's motivations and active engagement • Centralized planning and mobilization allows coordination and rapid growth • Absorptive model of technology development	• Public-private partnerships • Strong foundation in science and technology • Exports technology and engages with foreign countries • Anti-statist ideology
Weaknesses	• Relies on administrative enforcement for R&D • Dependence on foreign technology • Party and structural barriers	• Becoming reliant on civilian dual-use technology from a rigid and risk-averse defense acquisition system • Delay in considering China a threat • An increasingly broken political system

Acknowledgements

This brief is an excerpt from *Innovate To Dominate: The Rise of the Chinese Techno-Security State*, available at Cornell University Press, August 2022.

Author

Tai Ming Cheung is director of the University of California Institute on Global Conflict and Cooperation (IGCC) and a professor at the School of Global Policy and Strategy at UC San Diego, where he teaches courses on the international relations and national security of China and Chinese security and technology policy. Among the areas of his research focus include China's efforts to become a world-class science and technology power, and the relationship between geo-economics, innovation, and national security. Dr. Cheung is a long-time analyst of Chinese and East Asian defense and national security affairs, especially defense economic, industrial and science and technological issues.

Dr. Cheung is the author of *Innovate to Dominate: The Rise of the Chinese Techno-Security State* (Cornell University Press, 2022), and *Fortifying China: The Struggle to Build a Modern Defense Economy* (Cornell University Press, 2009); editor of *Forging China's Military Might: A New Framework for Assessing Innovation* (Johns Hopkins University Press, 2014); and co-editor of *The Gathering Pacific Storm: Emerging US-China Strategic Competition in Defense Technological and Industrial Development* (Cambria Press, 2018). He was based Hong Kong, China, and Japan from the mid-1980s to 2002 covering political, economic, and strategic developments in Greater China and East Asia, first as a journalist for the Far Eastern Economic Review from 1988-1993 and subsequently as a political and business risk consultant for a number of companies, including PricewaterhouseCoopers. Dr. Cheung has a PhD in War Studies from King's College, London.

About IGCC

The UC Institute on Global Conflict and Cooperation (IGCC) is a network of researchers from across the University of California and the Los Alamos and Lawrence Livermore national labs who produce and use research to help build a more peaceful, prosperous world. We conduct rigorous social science research on international security, the environment, geoeconomics, nuclear security, and the future of democracy; help to educate and train the next generation of peacemakers; and strive to ensure that what we are discovering contributes to a safer world.