The Jervis Forum

H-Diplo | Robert Jervis International Security Studies Forum

Roundtable 18-18

Fiona S. Cunningham, *Under the Nuclear Shadow: China's Information-Age Weapons in International Security*. Princeton University Press, 2025. ISBN: 978-0-691-26102-7.

6 November 2026 | PDF: https://issforum.org/to/jrt18-18 | Website: rjissf.org

X: @HDiplo | BlueSky: @h-diplo.bsky.social | Mastodon: @HDiplo

Editor: Diane Labrosse
Commissioning Editor: Ryan Grauer
Production Editor: Christopher Ball
Pre-Production Copy Editor: Tatiana Kasperski

Contents

Introduction by Alexandre Debs, Yale University 2

Review by Nicholas D. Anderson, George Washington University 8

Review by Elsa B. Kania, CNAS Technology and National Security Program and the Penn Project on the Future of U.S.-China Relations 13

Review by Oriana Skylar Mastro, Stanford University 20

Review by Phillip C. Saunders, National Defense University and Johns Hopkins School of Advanced International Studies 26

Response by Fiona S. Cunningham, University of Pennsylvania 30

© 2026 The Authors | CC BY-NC-ND 3.0 US

Review by Oriana Skylar Mastro, Stanford University

Chinese military modernization and its implications for regional and global security are one of the most important theoretical and policy questions of our generation. Yet given the increasing opacity of the Chinese system, language barriers, and the complexity of the military platforms, systems and operations involved, research into Chinese military strategy and policy is challenging. In this context, the contributions of Fiona Cunningham's book, *Under the Nuclear Shadow: China's Information-Age Weapons in International Security*, to international relations theory as well as the understanding of the Chinese military cannot be overstated.

Cunningham starts with what she refers to as the limited-war dilemma, or the challenge of using military force to achieve political aims without triggering nuclear war. She argues that, unlike other states that have historically sought either decisive conventional victory or the credible threat of nuclear first use, China has pursued a third path: "strategic substitution," in which states seek substitutes, specifically information-age weapons, that can provide coercive leverage when conventional or nuclear options are inadequate (3-4). These weapons promise strategic effects by introducing escalation risks, but they only generate leverage if they are deliberately configured within a coercive force posture.

In her theory of strategic substitution, the independent variable is the presence (or absence) of a leverage deficit, with the key mechanism being a state's search for coercive leverage under the constraints of conventional inferiority and doubts about the credibility of nuclear threats. The dependent variable is whether a state decides to pursue a substitute, such as one of the three information-age weapons for coercive leverage she names: cyber, space, and precision-guided munitions. In the case of China, Cunningham emphasizes that once Beijing realized that it faced a leverage deficit, its response was shaped by two constraints not faced by many other nuclear-armed states: China's lagging conventional military capabilities and a suboptimal nuclear arsenal for retaliation (8-9). These limitations led China to adopt strategic substitution.

Having these information-age weapons, however, or even weapons that share their characteristics (for instance, she argues that "long-range bomber aircraft carrying conventional munitions are another obvious alternative," 26), does not equip a state with coercive leverage. Coercive leverage from information-age weapons arises only when they are deployed in ways that explicitly generate escalation risks. They must be configured into a force posture that threatens attacks on strategic targets that could generate a risk of escalation, including nuclear war. This can be done in two ways: 1) through a brinkmanship posture, which is a high-risk, high-reward posture that reduces the cost of achieving coercive bargaining leverage; or 2) through a calibrated escalation posture, which imposes higher costs to generate leverage but places safeguards around the coercive use of information-age weapons in order to partially control, and hence lower, escalation risks. The choice between these postures depends on factors such as technological availability, civil-military relations, institutional adaptation, and vulnerability to retaliation in kind (9-10).

© 2026 The Authors | CC BY-NC-ND 3.0 US

Cunningham does a stellar job of building out the theory and its observable implications. She also uses Chinese-language sources and an analysis of Chinese force posture over the past three decades, beginning with the 1995–1996 Taiwan Strait crisis, to convincingly show that China has indeed pursued cyber, space, and precision-guided weapons in a search for coercive leverage against a conventionally, and nuclear superior, adversary, the United States. This main finding is supported by my own research, which evaluates how the unique challenges of a rising power create disincentives for emulation and instead cause a country like China to exploit vulnerabilities and gaps in the great power's capabilities and pursue new pathways to power, which I refer to as entrepreneurship.[1] China's pursuit of anti-access area denial (A2AD) weapons, which are the military lexicon for Cunningham's term of information weapons, is undeniably a more efficient and effective way to deter US intervention and military counteraction as China attempts to establish itself as the dominant power in Asia.

While I agree with Cunningham's general analysis of the state and development of the Chinese military, I would like to use this roundtable to gain greater perspective on several aspects of the argument. Therefore, this review will delve deeper into the core claims upon which her theory rests, not to challenge the overall argument, which I find convincing, but to engage with the author on related aspects of the theoretical argument.

Cunningham's first core claim is that information-aged weapons revive the strategic utility of escalation risks even under conditions of nuclear stalemate. Unlike nuclear weapons, which are often too catastrophic to credibly threaten in limited conflicts, information-age weapons are calibrated tools of coercion: they are sufficiently destructive and unpredictable to make threats meaningful yet restrained enough to avoid automatic escalation to nuclear war (10). Their strategic use introduces ambiguity—"the threat that leaves something to chance"—in a way that nuclear threats alone often fail to do.[2] Moreover, their use places the burden of further escalation on the adversary. If a nuclear-armed opponent responds to an information-age-weapons attack with nuclear retaliation, such a response would likely be viewed as disproportionate.

But this claim relies on the assumption that information-age weapons are more escalatory than conventional weapons. My understanding is precisely the opposite. Indeed, Chinese thinkers often prefer non-kinetic, non-attributable, reversable attacks in space and cyber domains because decisive US responses are unlikely and non-credible. Deterring Chinese attacks on US space assets is difficult precisely because they are likely to be significantly impactful in operational terms but are not likely to cross thresholds that cause escalation. The US defense community has gone through different frameworks as it tries to counter the un-escalatory nature of space and cyberattacks, including cross-domain deterrence (threatening retaliation in another domain) and deterrence through resilience (reducing the operational impact through defense and/or redundancy), which is the current focus.

---

[1] Oriana Skylar Mastro, *Upstart: How China Became a Great Power* (Oxford University Press, 2024).
[2] Thomas C. Schelling, *The Threat That Leaves Something to Chance* (RAND Corporation, 1959), https://www.rand.org/pubs/historical_documents/HDA1631-1.html.

© 2026 The Authors | CC BY-NC-ND 3.0 US

Conventional attacks that are easily attributable, irreversible, and lead to the death of Americans are far more escalatory than activities in the space and cyber realm. This is why Chinese planning for the implementation of cyber, space, and precision-guided weapons mostly focuses on utility in a traditional interstate context against military targets, such as fixed bases or surface ships. While theoretically these, like other weapons, could be used to "cause rapid, large-scale effects" (26), Chinese policy documents focus on using them against military targets to impact power projection versus attacks against civilian targets that would "terrorize [the] population" (28). While some of them do note that the use of these weapons includes a nuclear escalation risk, the same is the case for conventional attacks, especially if they are against dual-use targets. It is unclear why a counterspace exchange would more plausibly lead to nuclear war (38) than, for example, a naval battle that leads to the deaths of thousands of people.

Given this distinction, are conventional precision-guided munitions best characterized as "information-age weapons" alongside offensive cyber operations and counterspace weapons? Cunningham argues that they should be because their reliance on information systems in execution is a core feature. Information-age weapons, she says, include "data about the location of the target…laser marking of a target…infrared, radio-frequency, or electro-optical sensors…" (25). But in this age of Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR), almost every weapon, including submarines, aircraft, drones, and even ground forces, relies on information networks for successful execution. Modern militaries operate on a network-centric paradigm in which weapons, sensors, and command nodes are tightly integrated. The US Department of Defense manages more than 15,000 networks and seven million computing devices to support this integration, and NATO appraises C4ISR as the backbone of its ability to conduct major joint operations.[3] This reliance was reflected in the global C4ISR market, which was valued at US$131.5 billion in 2024 and is projected to reach nearly US$191 billion by 2033, with similar growth seen in related markets such as network-centric warfare.[4]

Other characteristics that are used to distinguish "information-age" weapons are also debatable, such as the claim that "information-age weapons are readily accessible to nuclear armed states" (56). Not only is the technology different, but variations across nuclear-weapon state capabilities suggest otherwise. France, for instance, has nuclear weapons, but not sophisticated cyber/space weapons; and DPRK has nuclear weapons

[3] Antoinette King, "Network-centric U.S. Military Systems and the Rise of CMMC," *Security Systems News*, August 28, 2020, https://www.securitysystemsnews.com/article/network-centric-us-military-systems-cmmc; Andrea Gilli and Mauro Gilli, *Appraising the State of Play of C4ISR Infrastructure within NATO* (Hague Centre for Strategic Studies, May 2025), https://hcss.nl/wp-content/uploads/2025/05/Appraising-the-State-of-Play-of-C4ISR-Infrastructure-within-NATO-HCSS-2025-1.pdf.

[4] Grand View Research, "C4ISR Market Size, Share & Trends Analysis Report," *Grand View Research*, accessed September 2025, https://www.grandviewresearch.com/industry-analysis/c4isr-market.

© 2026 The Authors | CC BY-NC-ND 3.0 US

and has tested ICBM-range missiles, though their operational reliability and reentry capability remain unproven.[5]

A potentially more accurate and encompassing categorization of space, cyber, and conventional missiles would be weapons designed to impact power projection. Indeed, I would add "operational impact" to the advantages of strategic substitution over the alternatives (48). After witnessing US operations in the Gulf War and Iraq War, Chinese leaders concluded that "one of the most important reasons for the strong combat capability of the U.S. military is its leading position in information technology" and that future wars would require "informatization" of the PLA.[6] Chinese analysts emphasized that US forces were deeply dependent on space-based assets and cyber infrastructure, therefore anti-satellite operations or cyberattacks on command-and-control systems could "destroy the overall function of the enemy's combat forces and achieve the effect of a huge return for a very small investment."[7]

In addition to access to space and cyberspace, the US military relies on fixed bases in the first island chain as well as its navy, in particular aircraft carriers, to constrain China. In other words, the defining characteristic of the three capabilities of space, cyber, and conventional missiles is not their information component, but their ability to disrupt power projection. This categorization is consistent with Cunningham's findings that China did not prioritize other forms of military power, such as strategic bombers, electronic warfare, and special operations forces (SOF), but the logic behind that decision is that they would be higher cost, less defensive, and less impactful on US power projection capabilities than the alternatives.

Cunningham's second core claim is that China's leaders turned to information-age weapons, specifically precision conventional missiles, offensive cyber capabilities, and counterspace weapons, because they promised to have strategic effects that could restore coercive leverage under the shadow of nuclear deterrence (8-9). Unlike most nuclear-armed states that lean on either nuclear threats or decisive conventional victory, China charted this third path and invested in "information-age weapons" as tools of coercion.

Yet a question that goes unanswered throughout the book is whether these weapons are designed to gain coercive leverage or to win wars. This is a critical distinction in Cunningham's theory. If it is the latter, that gives more credibility to the idea that China did choose one of the conventional approaches to the limited war dilemma, that of conventional superiority. Cunningham analyzes the discussions of Chinese leaders

---

[5] Makena Young, "The Evolution of French Space Security," Center for Strategic and International Studies, March 13, 2024, https://www.csis.org/analysis/evolution-french-space-security; Joseph Trevithick, "ICBM Reentry Vehicle Capability Still Unproven by North Korea, U.S. Military Says," *The War Zone*, November 20, 2024, https://www.twz.com/nuclear/icbm-reentry-vehicle-capability-still-unproven-by-north-korea-u-s-military-says.

[6] Mastro, *Upstart*, 96.

[7] Dai Yifang [戴怡芳], ed., *Reflections and Prospects for Military Studies* [军事学研究回顾与展望] (Military Sciences Press [军事科学出版社], 1995), 94.

© 2026 The Authors | CC BY-NC-ND 3.0 US

that show the understanding that conventional wars cannot be fought and won (7). I would argue that these discussions point to the conclusion that the use of US power projection methods to fight and win conventional wars will not work. Instead, Chinese leaders deliberately pursued a different path. They drew the lesson that Moscow's dollar-for-dollar competition with Washington contributed to the Soviet collapse, and that China had to find another way. This meant targeting the unique vulnerabilities created by U.S. reliance on forward bases, long-distance logistics, and carriers, or the A2/AD approach.

Chinese leaders perceive that since the vast majority of modern wars end by negotiated settlement, there is always a coercive leverage component.[8] But Cunningham argues that the explanatory power of strategic substitution would be undermined if China both opted for traditional alternatives (such as focusing exclusively on conventional modernization) or if it pursued information-age weapons for reasons other than coercive leverage (such as to strengthen its conventional military capabilities). But this may dismiss evidence that suggests that China did pursue these information-age weapons to strengthen its conventional military capability. Indeed, the main Chinese campaigns against Taiwan, the Joint Island Landing Campaign and blockade, both employ conventional military capabilities that rely on these information-aged systems to succeed.[9] Other capabilities, such as the expansion of the surface fleet, were given top priority over cyber and space capabilities.[10] The fact that the navy is a service, but the structure for space and cyber has never been a service, suggests that space and cyber have not been the organizational priority for President Xi Jinping.

My last point concerns the policy implications of Cunningham's argument. She hints that China's adoption of strategic substitution does not entirely preclude or replace conventional or nuclear capabilities; rather, it serves as a stopgap while the continued development of those capabilities may eventually offer the option to adopt a different response to the limited-war dilemma (315). Indeed, scholars and policymakers actively debate whether China is merely building to maintain minimum deterrence or moving toward nuclear parity with the United States. US Department of Defense projections suggest that China could field around 1,000 operational nuclear warheads by 2030 and possibly 1,500 by 2035, though other assessments emphasize

[8] Eric Min, *Words of War: Negotiation as a Tool of Conflict* (Cornell University Press, 2025); Oriana Skylar Mastro, *The Costs of Conversation: Obstacles to Peace Talks in Wartime* (Cornell University Press, 2019).
[9] Joel Wuthnow et al., eds., *Crossing the Strait: China's Military Prepares for War with Taiwan* (National Defense University Press, 2022), https://ndupress.ndu.edu/Portals/68/Documents/Books/crossing-the-strait/crossing-the-strait.pdf; Eric Rosenbach et al., *The Autonomous Arsenal in Defense of Taiwan: Technology, Law, and Policy of the Replicator Initiative* (Belfer Center for Science and International Affairs, February 2025), https://www.belfercenter.org/sites/default/files/2025-02/DETS_The%20Autonomous%20Arsenal_1.pdf.
[10] Ronald O'Rourke, *China Naval Modernization: Implications for U.S. Navy Capabilities* (Congressional Research Service, updated 30 January 2024), https://www.congress.gov/crs_external_products/RL/PDF/RL33153/RL33153.276.pdf.

© 2026 The Authors | CC BY-NC-ND 3.0 US

that even under these scenarios China will still lag in qualitative areas such as survivability, delivery systems, and readiness.[11]

I see claims that Beijing is on the verge of nuclear parity as exaggerated and have argued that China's nuclear strategy is distinct; it is built on minimal deterrence, assured retaliation, and a no-first-use pledge, with modernization aimed at survivability and second-strike credibility rather than parity.[12] It is unclear whether Cunningham views this restraint as enduring or temporary. The policy implications for this assessment are profound. If Chinese nuclear restraint is only temporary, US military buildup is a smart response. If not, some strategic approaches could be counterproductive. How then might US efforts to enhance defense, such as the Golden Dome, influence China to adopt a different, less favorable approach?

These questions aside, *Under the Nuclear Shadow* provides a rigorous analysis of how China has responded to the limited-war dilemma and sought coercive leverage in the nuclear age by adopting a strategy of strategic substitution. Through a careful examination of China's development and deployment of precision conventional missiles, offensive cyber capabilities, and counterspace weapons, Cunningham shows that China has pursued fast and credible alternatives to nuclear first use. While strategic substitution has allowed China to manage leverage deficits, Cunningham also highlights ongoing challenges of coordination, entanglement, and the risk of retaliation. Her timely and well-argued book offers important insights for US and allied policymakers navigating the risks of escalation in an era of information-age competition.

[11] U.S. Department of Defense, *Military and Security Developments Involving the People's Republic of China 2022: Annual Report to Congress* (Office of the Secretary of Defense, November 2022), https://media.defense.gov/2022/Nov/29/2003122279/-1/-1/1/2022-MILITARY-AND-SECURITY-DEVELOPMENTS-INVOLVING-THE-PEOPLES-REPUBLIC-OF-CHINA.PDF.

[12] Mastro, *Upstart*, 120-125.

© 2026 The Authors | CC BY-NC-ND 3.0 US