

The Intelligentized Security Dilemma:
Systems Destruction Warfare, Technological Entanglement, and the Erosion of Strategic Stability

By
Alyssa I. Agard

Agard Research Associates Inc. - Research Division

March 2026

PREPRINT



© 2026 Alyssa I. Agard. All rights reserved.

The Intelligentized Security Dilemma: Systems Destruction Warfare, Technological Entanglement, and the Erosion of Strategic Stability © 2026 by Alyssa I. Agard is licensed under CC BY-NC-ND 4.0. To view a copy of this license, visit <https://creativecommons.org/licenses/by-nc-nd/4.0/>

© 2026 Alyssa I. Agard. All rights reserved.

The Intelligentized Security Dilemma: Systems Destruction Warfare, Technological Entanglement, and the Erosion of Strategic Stability © 2026 by Alyssa I. Agard is licensed under CC BY-NC-ND 4.0. To view a copy of this license, visit <https://creativecommons.org/licenses/by-nc-nd/4.0/>

No part of this publication may be reproduced, distributed, or transmitted in any form or by any means, including photocopying or other electronic or mechanical methods, without prior written permission of the copyright owner, except as permitted by the Creative Commons license.

Abstract	4
Introduction	5
The Decline of Classical Deterrence	7
The PLA’s Strategy for Success: Systems Destruction and Intelligentization	7
<i>Systems Confrontation and the Evolution of Chinese Warfighting</i>	9
<i>Systems Destruction Warfare</i>	9
<i>Intelligentized Warfare and Algorithm Confrontation</i>	10
<i>Operational Concepts for Large-Scale Combat Operations</i>	10
The Orbital Security Dilemma: Space as the Critical Domain	10
The Cognitive Domain: Ai, Cyber, And the Speed of Thought	14
<i>AI, Decision Compression, and Strategic Stability</i>	14
<i>Cyber Operations and Contested Escalation Pathways</i>	15
<i>Cognitive Domain Operations and Information Sovereignty</i>	15
The Quantum Race: Erasing the Fog of War	17
<i>Quantum Sensing and the Survivability of Second-Strike Forces</i>	17
<i>Quantum Radar and the Erosion of Stealth</i>	18
<i>Quantum Communications and Secure Networks</i>	18
<i>Policy Approaches to Quantum Dominance</i>	19
Hypersonics And the Compression of Crisis Time	20
Entanglement and the New Era of Counterforce	22
Internal Friction: A Net Assessment.....	24
<i>The Modernization Trajectory</i>	24
<i>Organizational Constraints</i>	24
<i>Technology and Doctrine Gaps</i>	25
<i>Military-Civil Fusion</i>	25
<i>Assessing the Net Strategic Risk</i>	26
Reimagining Stability.....	27
<i>Conclusion</i>	27

Abstract

The People's Liberation Army's (PLA) operational framework Systems Destruction Warfare (体系破击战), combined with artificial intelligence, quantum sensing, hypersonic weapons, and counterspace capabilities, is reshaping the logic of strategic deterrence. This article argues that the convergence of these advancements creates an "intelligentized" security dilemma characterized by compressed decision timelines, the integration of nuclear, conventional, and space architectures, and nonlinear escalation pathways that render Cold War stability models obsolete. Tracing PLA doctrinal evolution from mechanization through informatization (信息化) to intelligentization (智能化), the analysis examines how each technological domain contributes to an increasingly unstable strategic environment and, critically, how these domains compound one another within a single operational framework. The article further evaluates the internal frictions constraining PLA modernization, including corruption, personnel shortfalls, and gaps between doctrinal ambition and technological integration, assessing their implications for the net strategic risk. The analysis concludes that the greatest threat lies not in any single technology but in the synergistic interaction of destabilizing capabilities within a doctrine that exploits systemic vulnerabilities, and proposes domain specific governance mechanisms tailored to the compound dynamics identified.

Keywords: Systems Destruction Warfare, intelligentized warfare, security dilemma, strategic stability, People's Liberation Army, artificial intelligence, quantum sensing, hypersonic weapons, counterspace operations, nuclear deterrence, escalation dynamics, military-civil fusion

Introduction

The framework of strategic stability that has governed great power competition for nearly half a century rests on assumptions that emerging technologies are systematically dismantling. Cold War deterrence theory presumed a bipolar international order in which rational state actors maintained secure second strike nuclear capabilities, ensuring that mutual vulnerability produced restraint.¹ Today, that paradigm confronts a fundamentally different strategic landscape characterized by multipolarity, the blurring of nuclear and conventional boundaries, and the accelerating integration of artificial intelligence (AI), quantum sensing, hypersonic weapons, and counterspace capabilities into military operations. The People's Liberation Army (PLA) has embraced a doctrinal framework known as Systems Destruction Warfare (体系破击战) that exploits these technologies within an integrated operational concept, evolving from mechanization through informatization (信息化) to what PLA theorists term "intelligentization" (智能化). The central question this article addresses is whether the convergence of this concept with emerging technologies has created an "intelligentized" security dilemma, rendering traditional deterrence and stability models obsolete.

Existing scholarship has examined the individual dimensions of this transformation. Analysts have explored the stability-instability paradox in East Asia, the implications of AI for nuclear command and control, the weaponization of outer space, and the strategic consequences of hypersonic proliferation.²

Recent work has addressed "wormhole" escalation pathways that bypass traditional escalation ladders and the application of security dilemma theory to multipolar dynamics. However, the literature has largely treated these developments in isolation, failing to account for the compounding effects when these technologies converge within a single operational framework.

This article addresses that gap by analyzing how Systems Destruction Warfare, amplified by AI, quantum technologies, hypersonic systems, and counterspace operations, creates a security dilemma whose constituent parts reinforce one another. This analysis applies security dilemma theory across multiple technological domains to assess how offensive and defensive indistinguishability, compressed decision timelines, and dual use ambiguity interact within a single doctrinal framework. By tracing these dynamics sequentially through the space, cyber, quantum, and hypersonic domains, the analysis reveals compounding and synergistic effects that domain specific studies in isolation cannot capture.

The article is structured in eight sections. The first examines the decline of classical deterrence theory in a complex, multipolar world. The second analyzes the PLA's doctrinal framework of Systems Destruction Warfare and intelligentization as a theory of victory. Sections three through six assess the destabilizing dynamics within the space, cyber and AI, quantum, and hypersonic domains, respectively. The seventh section examines technological entanglement and the new era of counterforce, while the eighth evaluates the internal frictions constraining PLA modernization as a net assessment counterargument. The article concludes by proposing domain specific governance mechanisms

¹ Robert Jervis, "Cooperation Under the Security Dilemma," *World Politics* 30, no. 2 (January 1978): 167-70, 198; Daniel H. Wang, "Death of a Doctrine: The End of Classical Deterrence in a Complex Multipolar World" (master's thesis, Missouri State University, 2025), 31.

² Ulrich Kühn, "Strategic Stability in the 21st Century: An Introduction," *Journal for Peace and Nuclear Disarmament* 6, no. 1 (2023): 1-2.

suited to the compound dynamics the preceding analysis identifies.

The Decline of Classical Deterrence

The foundational logic of Cold War strategic stability rested on a bipolar international order in which two nuclear armed superpowers maintained secure second strike capabilities, producing a condition of mutual vulnerability that incentivized restraint. This conceptual architecture, rooted in Mutually Assured Destruction and rational actor models, provided a degree of predictability that governed great power competition for nearly half a century.³ The concept of strategic stability has come under immense pressure as nuclear multipolarity, novel technologies, arms control crises, and a growing acceptance of softer behavioral norms have collectively eroded its foundations.⁴ The binary nuclear world of the Cold War has given way to an emerging multipolar order in which multiple nuclear-armed states, each shaped by distinct strategic cultures and escalation thresholds, compete across overlapping domains.⁵ A concept developed for unique bilateralism now faces the difficult task of reflecting very different strategic postures, alliance dynamics, and historical experiences across an expanding set of nuclear actors.⁶ Strategic misperception risk increases as more players enter the nuclear arena, each pursuing unique ambitions under incomplete information about adversaries' intentions and capabilities.⁷

Beyond the structural shift from bipolarity to multipolarity, the theoretical framework governing escalation dynamics has proven inadequate. Cold War era scholarship produced the stability-instability

paradox as a framework for understanding conflict escalation. This concept holds that strategic stability, underwritten by nuclear arsenals and mutual assured destruction, may paradoxically make it safer for states to engage in violence at lower levels of conflict.⁸ This paradox is particularly significant in the ongoing competition between the United States and China. Here, maritime geography delineates the primary conflict zone, and advancements in precision-strike capabilities increase the likelihood of limited conventional warfare compared to the land theater of Cold War Europe.⁹ If conventional conflict erupted, intentional limited nuclear use may be more likely in East Asia than Europe, given fewer high value targets and the greater plausibility of managing escalation in a maritime setting.¹⁰ The paradox reveals a disturbing trajectory in which conditions enabling limited conventional and nuclear conflict become more permissive in the century's most consequential strategic competition.

The inadequacy of existing escalation models extends beyond the stability-instability paradox. Traditional conceptualizations of escalation as a stepwise progression along a predictable ladder, with clear thresholds separating sub conventional, conventional, and nuclear responses, no longer capture the dynamics of the current security environment.¹¹ The escalation "wormhole" concept captures how rival states can unintentionally cross from sub-conventional friction to strategic-level conflict through swift, nonlinear sequences driven by the search for asymmetric leverage amid an increasingly dispersed

³ Wang, "Death of a Doctrine," 31; Jervis, "Cooperation Under the Security Dilemma," 187, 198; Keir A. Lieber and Daryl G. Press, "The End of MAD? The Nuclear Dimension of U.S. Primacy," *International Security* 30, no. 4 (Spring 2006): 7-9.

⁴ Kühn, "Strategic Stability," 1-2.

⁵ Wang, "Death of a Doctrine," 47-49.

⁶ Kühn, "Strategic Stability," 3.

⁷ Wang, "Death of a Doctrine," 49.

⁸ Henrik Stålhane Hiim and Øystein Tunsjø, "The U.S.-China Stability-Instability Paradox: Limited War in East Asia," *International Security* 50, no. 1 (Summer 2025): 153.

⁹ Hiim and Tunsjø, "U.S.-China Stability-Instability Paradox," 154.

¹⁰ Hiim and Tunsjø, "U.S.-China Stability-Instability Paradox," 154-55, 179.

¹¹ Rebecca Hersman, "Wormhole Escalation in the New Nuclear Age," *Texas National Security Review* 3, no. 3 (Summer 2020): 104-106.

global power structure.¹² The consolidation of warning, surveillance, and communication systems into a single conventional and nuclear ecosystem implies that opponents might struggle to understand intentions during a crisis, incentivizing preemptive action.¹³ In this setting, minor conflicts can rapidly escalate into major wars in unpredictable and challenging ways, making traditional crisis management models dangerously incomplete.¹⁴ Escalation wormholes are inherently catastrophic and unstable, reflecting a security landscape in which technology and asymmetry have outpaced the conceptual tools designed to manage conflicts.

The security dilemma is the theoretical lens through which these destabilizing dynamics can be most coherently analyzed. A security dilemma occurs when a state implements measures to bolster its security, which frequently provokes reactions from other states, ultimately leading to a diminution rather than an enhancement of the initial state's security.¹⁵ In an anarchic international system, states must provide for their own survival, yet many of their actions, including weapons procurement and the creation of new military technologies, inevitably reduce the security of others.¹⁶ This dynamic may produce security spirals in which competing states drive armament and elevate the risk of conflict, even when all parties prefer the status quo. The intensity of the security dilemma varies with factors including geography, military technology, military doctrine, and the degree to which offensive and defensive capabilities can be distinguished.¹⁷ In the emerging strategic landscape of artificial intelligence, quantum sensing, hypersonic delivery systems, and counterspace operations, the distinction between

offensive and defensive postures grows increasingly ambiguous, heightening the potential for an intensified security dilemma. The convergence of these technologies within the PLA's Systems Destruction Warfare doctrine generates a new, "intelligentized" iteration of the security dilemma, one whose compound effects the following sections examine in turn.

¹² Hersman, "Wormhole Escalation," 96.

¹³ Hersman, "Wormhole Escalation," 103.

¹⁴ Hersman, "Wormhole Escalation," 107.

¹⁵ Anders Wivel, "Security Dilemma," in *International Encyclopedia of Political Science*, ed. B. Badie, D. Berg-Schlosser, and L. Morlino (Thousand Oaks, CA: Sage Publications, 2011), 2389.

¹⁶ Wivel, "Security Dilemma," 2389-91.

¹⁷ Wivel, "Security Dilemma," 2389-90.

The PLA's Strategy for Success: Systems Destruction and Intelligentization

Systems Confrontation and the Evolution of Chinese Warfighting

The PLA's contemporary approach to warfare reflects a fundamental reconceptualization of armed conflict, emerging from careful study of post Cold War American military operations.¹⁸ The Gulf War (1990-1991) and Kosovo War (1998-1999) demonstrated to PLA analysts that contemporary warfare is no longer a battle among individual units, service branches, or weapons platforms, but rather a clash between opposing operational systems.¹⁹ Chinese military publications have since designated this mode of fighting as systems confrontation (体系对抗), a concept that has pervaded the PLA's doctrine, professional military education, and official defense white papers for more than two decades.²⁰ The PLA's modernization has proceeded through three stages: mechanization, which focused on advanced machinery; informatization, which incorporated networks and data systems; and intelligentization, which aims to integrate artificial intelligence and autonomous systems into military operations.²¹ Systems confrontation extends the battlefield well beyond the traditional land, sea, and air domains to include orbital space, cyber operations, the

electromagnetic environment, and the cognitive arena, reflecting a comprehensive appreciation of the multidomain character of modern warfare.²² PLA doctrinal literature consistently designates systems confrontation as the foundational operational approach for joint campaigns in informatized conditions. The implications for the intelligentized security dilemma are profound: the PLA understands warfare not as destroying individual platforms or units but as severing the linkages holding an opponent's operational architecture together.²³

Systems Destruction Warfare

The PLA's theory of victory within the systems confrontation framework is systems destruction warfare, which has supplanted annihilation warfare as the principal means of achieving strategic objectives.²⁴ The core concept revolves around an operational system that serves as the primary framework for warfare, connecting organizations, functional processes, and networks to facilitate integrated joint-service combat in all domains.²⁵ Within this framework, the operational system functions through five interdependent subsystems responsible for command, the application of firepower, information confrontation, reconnaissance and intelligence collection, and operational support.²⁶ Rather than seeking the physical destruction of enemy forces, systems destruction warfare aims to attain victory by paralyzing an adversary's operational system so that it loses its integrated resistance capabilities.²⁷ This

¹⁸ Jeffrey Engstrom, *Systems Confrontation and System Destruction Warfare: How the Chinese People's Liberation Army Seeks to Wage Modern Warfare* (Santa Monica, CA: RAND Corporation, 2018), iv.

¹⁹ Engstrom, *Systems Confrontation and System Destruction Warfare*, 10, 15-16.

²⁰ Engstrom, *Systems Confrontation and System Destruction Warfare*, 11.

²¹ Joshua Baughman, "The Path to China's Intelligentized Warfare: Converging on the Metaverse Battlefield," *The Cyber Defense Review* 9, no. 3 (Fall 2024): 30.

²² Engstrom, *Systems Confrontation and System Destruction Warfare*, ix; Edmund J. Burke et al., *People's Liberation Army Operational Concepts* (Santa Monica, CA: RAND Corporation, 2020), 8.

²³ Engstrom, *Systems Confrontation and System Destruction Warfare*, 11.

²⁴ Engstrom, *Systems Confrontation and System Destruction Warfare*, 119.

²⁵ Burke et al., *People's Liberation Army Operational Concepts*, 8.

²⁶ Burke et al., *People's Liberation Army Operational Concepts*, 8.

²⁷ Burke et al., *People's Liberation Army Operational Concepts*, 8; Engstrom, *Systems Confrontation and System Destruction Warfare*, 119-120.

strategy emphasizes targeted, accurate, and decisive actions against the core elements of enemy systems, including leadership bodies, command and control centers, and information networks.²⁸ The primary operational necessity in systems destruction warfare is to seize information dominance through network warfare to disrupt enemy command while degrading adversary control over operations.²⁹

Intelligentized Warfare and Algorithm Confrontation

The transition from informatization to intelligentization represents the PLA's most ambitious doctrinal evolution. This shift reflects the Xi Jinping administration's strategic assessment that advances in artificial intelligence present a rare opportunity to overtake competitors at a critical technological turning point.³⁰ Since 2019, even as informatization efforts continue, the PLA has accelerated its focus on integrating artificial intelligence, quantum computing, large-scale data processing, cloud based infrastructure, and unmanned autonomous capabilities into its warfighting architecture.³¹ PLA theorists envision that intelligentized warfare will transform the confrontation mode from system confrontation to algorithm confrontation (算法对抗), where superior algorithms dominate through human-computer hybrid operations and neural network decision making.³²

In this perspective, the cognitive domain is seen as the next crucial arena following the physical and information domains, with decision making

transitioning from individual human thought to incorporation with collective intelligence in the cloud.³³ The concept of a "cloud brain" (云脑) envisions AI as a digital assistant capable of collecting intelligence, discerning enemy intentions, and overseeing operations across domains at speeds beyond human capacity.³⁴ PLA theorists project that the shift to intelligentized warfare will unfold over approximately three decades. This progression moves through initial, intermediate, and advanced stages, each incrementally integrating greater autonomous capabilities into the PLA's operational architecture.³⁵

Operational Concepts for Large-Scale Combat Operations

The doctrinal architecture of systems destruction warfare translates into three linked operational concepts: war control through information dominance, expansion of war space across domains, and target centric warfare aimed at destroying an adversary's operational system.³⁶ In the context of large scale combat operations, China aims to merge military and civilian strengths, with the PLA employing advanced technologies for decisive victories that exploit enemy vulnerabilities through precision strikes synchronized across multiple services and operational domains.³⁷ The PLA's core operational concept, Multidomain Precision Warfare, embodies this approach by fusing information from all services to identify and strike critical enemy vulnerabilities.³⁸ Campaign design centers on discovering, recognizing, and targeting

²⁸ Burke et al., *People's Liberation Army Operational Concepts*, 8-10.

²⁹ Engstrom, *Systems Confrontation and System Destruction Warfare*, 119; Mark Cozad et al., *Gaining Victory in Systems Warfare: China's Perspective on the U.S.-China Military Balance* (Santa Monica, CA: RAND Corporation, 2023), 76.

³⁰ Masaaki Yatsuzuka, "PLA's Intelligentized Warfare: The Politics on China's Military Strategy," *Security & Strategy* 2 (January 2022): 25.

³¹ Baughman, "Path to China's Intelligentized Warfare," 29-30; P. K. Mallick, *Defining China's Intelligentized Warfare and Role of Artificial*

Intelligence (New Delhi: Vivekananda International Foundation, 2021), 20.

³² Burke et al., *People's Liberation Army Operational Concepts*, 21.

³³ Yatsuzuka, "PLA's Intelligentized Warfare," 27-28.

³⁴ Burke et al., *People's Liberation Army Operational Concepts*, 21.

³⁵ Yatsuzuka, "PLA's Intelligentized Warfare," 28.

³⁶ Burke et al., *People's Liberation Army Operational Concepts*, 9.

³⁷ T2COM, *How China Fights in Large-Scale Combat Operations*, T2COM OE Threat Assessment 1-1 (U.S. Army, 2025), 1.

³⁸ T2COM, *How China Fights in Large-Scale Combat Operations*, 1.

enemy networks to achieve operational paralysis, with main objectives including leadership nodes, command and control systems, and information hubs.³⁹ In anticipation of potential foreign intervention, China has enhanced its integrated counter-intervention strategy to deter and defeat adversarial forces through information operations, efforts to secure air and maritime superiority, and targeted strikes on deployment routes and logistical networks.⁴⁰

The doctrinal architecture outlined above establishes the operational logic through which the intelligentized security dilemma manifests. Systems destruction warfare integrates space, cyber, quantum, and hypersonic capabilities as interdependent vectors for paralyzing an adversary's operational system. The following sections examine how each domain generates destabilizing dynamics that compound within this unified framework.

³⁹ Burke et al., *People's Liberation Army Operational Concepts*, 8-9; Engstrom, *Systems Confrontation and System Destruction Warfare*, 119.

⁴⁰ T2COM, *How China Fights in Large-Scale Combat Operations*, 1-2.

The Orbital Security Dilemma: Space as the Critical Domain

The transformation of outer space from a relatively benign operational environment into a contested warfighting domain represents one of the most consequential shifts in contemporary security affairs. For decades, a combination of norms, technical limitations, and the relatively modest military and economic value of orbital assets sustained a fragile sanctuary in space.⁴¹ This stability has diminished as the increased reliance of traditional military capabilities on space support and the rising economic significance of space have rekindled early space-age concerns about orbital conflict.⁴² The resulting dynamic constitutes what Townsend terms the "orbital security dilemma," in which efforts to protect space assets are perceived as threatening, triggering cycles of action, reaction, and overreaction that produce suboptimal armaments and heightened conflict risk.⁴³ The belief that offense prevails in space complicates this dilemma, stemming from the notion that threatening space targets is cheaper and easier than defending them and that differentiating space systems as offensive or defensive weapons remains difficult.⁴⁴ While the offense defense balance in space is more accurately neutral than offense dominant, the misconception of offense dominance eliminates viable reassurance strategies and compels states into competitive stances, exacerbating the orbital security dilemma.

The difficulty of applying traditional deterrence concepts to the space domain further compounds this instability. A RAND framework identifies three space deterrence types: denial-dominant, using resilience and defenses to prevent adversary advantages; mixed deterrence, combining defenses with offensive capabilities; and offense dominant, emphasizing punishment through counterspace weapons to degrade adversary systems.⁴⁵ No single deterrence strategy is likely to be entirely effective against a capable adversary, as each approach has its own distinct vulnerabilities and required investments.⁴⁶ Deterrence difficulties worsen because controlling satellite positioning and maneuvering fuel is paramount; the side that launches space attacks first may gain a decisive advantage given attribution challenges and the rapid pace of orbital campaigns.⁴⁷ Antisatellite capabilities have expanded well beyond kinetic direct ascent missiles to include laser dazzling, high powered microwave interference, cyber intrusions, and frequency jamming, enabling states to operate below retaliatory thresholds in what analysts describe as gray zone warfare.⁴⁸ This diversification renders deterrence calculations exceedingly complex, as adversaries can degrade space capabilities through means that are difficult to detect, attribute, or classify as acts of war.

The development and deployment of antisatellite capabilities by both powers have heightened concerns about an arms race extending beyond the atmosphere. The lack of clear international norms governing space militarization increases the potential for misunderstandings, miscalculations, and

⁴¹ Brad Townsend, "Strategic Choice and the Orbital Security Dilemma," *Strategic Studies Quarterly* 14, no. 1 (Spring 2020): 65.

⁴² Townsend, "Strategic Choice and the Orbital Security Dilemma," 64.

⁴³ Townsend, "Strategic Choice and the Orbital Security Dilemma," 65-67, 87.

⁴⁴ Townsend, "Strategic Choice and the Orbital Security Dilemma," 75-76.

⁴⁵ Stephen J. Flanagan et al., *A Framework of Deterrence in Space Operations* (Santa Monica, CA: RAND Corporation, 2023), 30.

⁴⁶ Flanagan et al., *A Framework of Deterrence in Space Operations*, 30-31.

⁴⁷ Paul Szymanski, "Techniques for Great Power Space War," *Strategic Studies Quarterly* 13, no. 4 (Winter 2019): 87-90.

⁴⁸ Alexandra Stickings, "The Normalisation of Anti-Satellite Capabilities," *Air and Space Power Review* 22, no. 2 (2019): 33-34.

unintentional escalation.⁴⁹ Space-based centers of gravity, including satellites, ground facilities, launch sites, and communication networks, are vulnerable to preemptive action, and threats to these assets can trigger a “use it or lose it” mentality that incentivizes striking first.⁵⁰ The dual use nature of space technology exacerbates instability by creating what Vaynman and Volpe describe as intertwined detection and disclosure constraints on arms control. Distinguishing military from civilian applications requires intrusive monitoring, and verification risks revealing sensitive security information.⁵¹ This tension has frustrated efforts at space arms control; a 1984 Reagan administration report acknowledged that because antisatellite capabilities are inherent in systems designed for other missions, verifying compliance with a comprehensive prohibition was impossible.⁵² The lack of a precise definition of peaceful purposes in the 1967 Outer Space Treaty compounds verification challenges, as states can develop military applicable programs while claiming peaceful intent, fueling suspicion that incentivizes secrecy over transparency.⁵³

The destabilizing effects of space militarization are not confined to great power competition but extend to secondary powers, whose entry into the domain creates additional vectors of regional instability. The democratization of space and dual use technology is increasing the number of actors capable of developing antisatellite capabilities, whether through dedicated weapons programs or repurposed civilian systems.⁵⁴ Pakistan’s space program illustrates the ambitions and

vulnerabilities of emerging space states in a region already defined by acute nuclear rivalry and a history of conventional conflict.⁵⁵ Despite setbacks in satellite development and a shortage of trained professionals, Pakistan’s ballistic missile technology and strategic rivalry with India offer potential pathways toward developing a satellite launch vehicle.⁵⁶ As more states gain the ability to interfere with space assets, deterrence becomes harder and escalation potential grows in a domain where shared orbital geography means one state’s actions impact all others.⁵⁷ As antisatellite capabilities spread, the distribution of power in space will shift in ways that existing deterrence frameworks for bilateral or trilateral competition cannot address.⁵⁸

The orbital security dilemma is not a self-contained phenomenon. Within systems destruction warfare, space assets underpin the command, reconnaissance, and information subsystems the doctrine targets for paralysis. A state fearing the loss of its early warning and communication architecture faces pressure not only to strike first in orbit but to accelerate decision making across all connected domains, feeding directly into the decision compression dynamics examined next.

⁴⁹ Ameema Khalid, “Strategic Vulnerabilities in Space: U.S.-China Militarization and the Risks to Global Strategic Stability,” *Journal of Advanced Military Studies* 16, no. 2 (Fall 2025): 29.

⁵⁰ Khalid, “Strategic Vulnerabilities in Space,” 37.

⁵¹ Jane Vaynman and Tristan A. Volpe, “Dual Use Deception: How Technology Shapes Cooperation in International Relations,” *International Organization* 77, no. 3 (Summer 2023): 599–604.

⁵² Vaynman and Volpe, “Dual Use Deception,” 621.

⁵³ Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies, opened for signature January 27, 1967, 610 U.N.T.S.

205, art. IV; Khalid, “Strategic Vulnerabilities in Space,” 45; Vaynman and Volpe, “Dual Use Deception,” 604.

⁵⁴ Stickings, “Normalisation of Anti-Satellite Capabilities,” 33.

⁵⁵ Sannia Abdullah, “Pakistan’s Space Program: From Sounding Rockets to Satellite Setbacks,” *Space and Defense* 12, no. 2 (June 2021): 47; Zia Mian, R. Rajaraman, and M. V. Ramana, “Early Warning in South Asia: Constraints and Implications,” *Science and Global Security* 11 (2003): 124.

⁵⁶ Stickings, “Normalisation of Anti-Satellite Capabilities,” 33;

Abdullah, “Pakistan’s Space Program,” 45-46, 52.

⁵⁷ Townsend, “Strategic Choice and the Orbital Security Dilemma,” 85.

⁵⁸ Stickings, “Normalisation of Anti-Satellite Capabilities,” 38.

The Cognitive Domain: Ai, Cyber, And the Speed of Thought

AI, Decision Compression, and Strategic Stability

AI integration into military operations introduces destabilizing dynamics extending beyond tactical advantage, particularly where AI intersects with Nuclear Command, Control, and Communications (NC3) systems. AI in military and nuclear contexts alters strategic stability under traditional deterrence frameworks by compressing operational tempos and reducing time for human decision making during crises.⁵⁹ Integrating AI with NC3 early warning systems risks compressing decision making timeframes and introducing network vulnerabilities that could undermine stability, even as AI promises to enhance the existing nuclear enterprise qualitatively.⁶⁰ Advances in artificial intelligence, remote sensing, hypersonic delivery, and autonomous systems enhance the velocity, accuracy, destructive power, and resilience of strategic nonnuclear weapons, intensifying destabilization among nuclear armed nations.⁶¹ These advances create new paths for horizontal and vertical inadvertent escalation, intensifying risks of destabilizing doctrinal changes among regional nuclear powers that consider limited nuclear use to deter conventionally superior adversaries.⁶² AI's influence at tactical and strategic levels is not binary; it raises risks that AI decision-support systems may substitute for human critical

thinking, empathy, and intuition needed for sound strategic judgment.⁶³

The cognitive and heuristic burdens imposed by the digitized information ecosystem considerably amplify these escalation risks. The complexity and unpredictability central to Clausewitz's "fog of war" heighten the risk of unintended escalation by obscuring battlefield awareness, blurring the distinction between offensive and defensive actions, and amplifying fears of surprise or preemptive strikes. As speed, unpredictability, complexity, and mental stress become inherent in executing military operations on a digital battlefield, relying solely on sound human judgment to avert command and control breakdowns seems increasingly precarious.⁶⁴ Chinese analysts often overestimate American military AI capabilities relative to open source assessments, mirroring Soviet anxieties about the missile gap and potentially intensifying Beijing's perception that AI technology is strategically destabilizing.⁶⁵ In a world where information about power dynamics is flawed and uneven, and where motives exist to distort perceptions, the likelihood of negotiation diminishes and conflict increases.⁶⁶ AI enhanced cyber operations against nuclear-state command systems, whether for counterforce operations or limited strikes, could trigger preemptive actions driven by fears of losing retaliatory capability.⁶⁷

⁵⁹ James Johnson, *Artificial Intelligence and Nuclear Stability: Understanding AI's Impact on Military Escalation Dynamics and Strategic Deterrence*, GC REAIM Expert Policy Note Series (The Hague: The Hague Centre for Strategic Studies, 2025), 4-7.

⁶⁰ James Johnson, *Artificial Intelligence and the Future of Warfare: The USA, China, and Strategic Stability* (Manchester: Manchester University Press, 2021), 203.

⁶¹ James Johnson, "Inadvertent Escalation in the Age of Intelligence Machines: A New Model for Nuclear Risk in the Digital Age," *European Journal of International Security* 7, no. 3 (2022): 349.

⁶² Johnson, "Inadvertent Escalation," 349.

⁶³ Johnson, *Artificial Intelligence and the Future of Warfare*, 203.

⁶⁴ Johnson, "Inadvertent Escalation," 345-46.

⁶⁵ Johnson, "Inadvertent Escalation," 349-52.

⁶⁶ Johnson, "Inadvertent Escalation," 352.

⁶⁷ Johnson, "Inadvertent Escalation," 354; Johnson, *Artificial Intelligence and the Future of Warfare*, 203.

Cyber Operations and Contested Escalation Pathways

The cyber domain adds further complexity to the intelligentized security dilemma, as battlefield transparency demands new approaches to concealment. As battlespaces become more transparent through cellular surveillance, social media aggregation, and ubiquitous sensors, new methods to mask military movements have become operationally imperative.⁶⁸ The concept of cyber smoke screens, disrupting local internet and cellular networks to conceal military maneuvers, illustrates how defensive tactical actions acquire strategic significance in an all domain operational environment.⁶⁹ The United States has acknowledged the need for ongoing engagement in cyberspace; U.S. Cyber Command has embraced cyber persistence, actively contesting adversary efforts to achieve strategic outcomes through cumulative tactical impacts.⁷⁰ The erosion of America's dominant position in cyberspace, marked by fragmentation and Russian and Chinese power campaigns, has required a Relative Power Erosion Framework using national power elements for strategic cyber operations.⁷¹ This cyber competition, which remains below the armed-conflict threshold, demonstrates how the cognitive domain has evolved into a continuous arena for great power contestation rather than one that activates only during kinetic hostilities.

However, the escalatory potential of cyber operations remains contested in the scholarly literature, and the challenge of governing military AI

adds further urgency to these dynamics. Decades of research have demonstrated that cyber conflict typically does not serve as a pathway toward escalation in the international system; survey experiments suggest that cyber-response options are more often chosen to de-escalate conflicts than to intensify them.⁷² Cyber operations can serve as alternatives to war, enabling states to show resolve, alter information balance, and curb adversary behavior with minimal escalation risk when used instead of military options.⁷³ However, this deescalatory potential depends on the development of governance frameworks capable of managing the risks inherent in AI powered military platforms. Effective governance of military AI requires frameworks that address both technical failures and operational misuse, spanning the spectrum from informal mutual commitments to formal treaties and transparency mechanisms between nuclear armed states.⁷⁴ Shared definitions, agreed upon behavioral standards, and reliable lines of communication between adversaries are prerequisites for preventing AI-related military incidents from escalating into broader conflict.⁷⁵

Cognitive Domain Operations and Information Sovereignty

The information warfare dimension of the cognitive domain further compounds these challenges, as generative AI enables new forms of gray zone conflict that operate beneath conventional deterrence thresholds. The 2024 Taiwanese presidential election revealed how Chinese state and nonstate actors

⁶⁸ Dan G. Cox, "The Need for a Cyber Smoke Screen: A Tactical Action that Instantly Becomes Strategic in an All-Domain Operation," *The Cyber Defense Review* 9, no. 3 (Fall 2024): 17-18.

⁶⁹ Cox, "Need for a Cyber Smoke Screen," 22.

⁷⁰ Thomas F. Lynch III, "Forward Persistence in Great Power Cyber Competition: Military Assets in a Relative Power Erosion Framework," *The Cyber Defense Review* 9, no. 3 (Fall 2024): 92.

⁷¹ Lynch, "Forward Persistence," 96.

⁷² Brandon Valeriano and Benjamin Jensen, "De-escalation Pathways and Disruptive Technology: Cyber Operations as Off-Ramps to War," in

Cyber Peace: Charting a Path Toward a Sustainable, Stable, and Secure Cyberspace, ed. Scott J. Shackelford, Frédérick Douzet, and Christopher Ankersen (Cambridge: Cambridge University Press, 2022), 64-65.

⁷³ Valeriano and Jensen, "De-escalation Pathways," 87.

⁷⁴ Melanie W. Sisson et al., *Steps Toward AI Governance in the Military Domain* (Washington, DC: The Brookings Institution, 2025), 5-6.

⁷⁵ Sisson et al., *Steps Toward AI Governance*, 7.

leveraged generative AI to produce disinformation, from deepfakes to manipulated language models, designed to shape electoral outcomes.⁷⁶ These activities represent a progression beyond the PLA's earlier Three Warfares (三战) approach, consolidating psychological influence, media manipulation, legal coercion, and technological exploitation into a unified cognitive domain framework designed to shape how adversary populations perceive events.⁷⁷ AI driven fake news, deepfakes, and weaponized social media campaigns undermine deterrence and military planning, as emerging technologies layered onto legacy NC3 systems introduce new avenues for error, distortion, and manipulation.⁷⁸ Taiwan's response, combining new legislation, public education on information verification, and investment in domestic AI capabilities to protect its information environment, demonstrates both the seriousness of the challenge and the difficulty of constructing adequate defenses.⁷⁹

The convergence of AI driven information warfare, cyber operations, and compressed nuclear decision timelines blurs the boundaries between peace and conflict, defense and offense, conventional and nuclear thresholds. Consider a crisis scenario: degradation of space based early warning shortens the window for AI compressed decisions, while cognitive domain operations simultaneously corrupt the information on which those decisions depend. The question then becomes whether the concealment sustaining survivable deterrent forces can endure the next technological pressure, the subject of the following section.

⁷⁶ Sarah Mobilio, "GenAI in the 2024 Taiwan Presidential Election: Lessons for Democracies," *The Cyber Defense Review* 9, no. 3 (Fall 2024): 51-52.

⁷⁷ Mobilio, "GenAI in the 2024 Taiwan Presidential Election," 53.

⁷⁸ Johnson, *Artificial Intelligence and the Future of Warfare*, 203; James Johnson, "Revisiting the 'Stability-Instability Paradox' in AI-Enabled

Warfare: A Modern-Day Promethean Tragedy Under the Nuclear Shadow," *Review of International Studies* (2024): 10.

⁷⁹ Deborah S. Karagosian, "Reimagining the Future," *The Cyber Defense Review* 9, no. 3 (Fall 2024): 11.

The Quantum Race: Erasing the Fog of War

The intensifying U.S.-China rivalry over quantum technologies represents a key axis of 21st century strategic competition, with implications extending beyond computing into sensing, communications, and national security.⁸⁰ The United States and China pursue quantum information science leadership through distinct models of development. Washington's approach distributes quantum research across a network of government agencies, commercial enterprises, and universities, each pursuing largely autonomous lines of inquiry.⁸¹ China utilizes a state-driven approach that integrates scientific advancements with industrial and strategic goals through centralized planning and national research facilities.⁸² China's earliest breakthroughs came in quantum communications, driven by national security needs: the Micius quantum satellite launch in 2016, the Beijing to Shanghai Quantum Communication Backbone, and the Jiuzhang and Zuchongzhi quantum computers.⁸³ A strategic rival's early advancement in quantum technology is concerning, as being first would boost their reputation, enable them to lead in setting network standards, and create opportunities for government cyber campaigns.⁸⁴ The quantum race thus constitutes not merely a technological competition but a strategic contest whose outcome will shape the

balance of power across multiple domains of warfare and intelligence.⁸⁵

Quantum Sensing and the Survivability of Second-Strike Forces

Among the most consequential applications of quantum technology is quantum sensing, which exploits the sensitivity of quantum states to detect physical phenomena with precision exceeding that of classical instruments. Quantum magnetometers and gravimeters promise to revolutionize intelligence, surveillance, and reconnaissance by detecting magnetic and gravitational signatures of objects that current sensors cannot reliably identify.⁸⁶ Researchers anticipate that Superconducting Quantum Interference Device magnetometers could detect submarines from six kilometers away, compared to hundreds of meters achievable by classical magnetic anomaly detectors mounted on helicopters or aircraft.⁸⁷ Portable atomic magnetometers capable of noninvasive detection through barriers and underwater environments expand the potential for submarine tracking and mine detection. Coastal sensor arrays could establish denial zones, potentially undermining the near invulnerability of ballistic missile submarines that undergird nuclear second strike capabilities.⁸⁸ However, significant engineering challenges remain, as sensors that can detect the faintest magnetic or gravitational changes also absorb vibrations, thermal drift, electromagnetic clutter, and platform noise. Quantum inertial sensors

⁸⁰ Graham Allison et al., *The Great Tech Rivalry: China vs the U.S.* (Cambridge, MA: Belfer Center for Science and International Affairs, Harvard Kennedy School, 2021), 14-16.

⁸¹ Joseph Federici and Matthew Dagher-Margosian, *Vying for Quantum Supremacy: U.S.-China Competition in Quantum Technologies* (Washington, DC: U.S.-China Economic and Security Review Commission, November 18, 2025), 8.

⁸² Federici and Dagher-Margosian, *Vying for Quantum Supremacy*, 8.

⁸³ Federici and Dagher-Margosian, *Vying for Quantum Supremacy*, 8-9; Juljan Krause, *The Quantum Race: U.S.-Chinese Competition for Leadership in Quantum Technologies*, IGCC Policy Brief (La Jolla, CA: UC Institute on Global Conflict and Cooperation, 2024), 4-5.

⁸⁴ Krause, *The Quantum Race*, 8.

⁸⁵ Federici and Dagher-Margosian, *Vying for Quantum Supremacy*, 8-10.

⁸⁶ Hideki Tomoshige and Phillip Singerman, *Quantum Sensing and the Future of Warfare: Five Essential Reforms to Stay Competitive* (Washington, DC: Center for Strategic and International Studies, 2025), 1-3.

⁸⁷ Michal Krelina, "Quantum Technology for Military Applications," *EPJ Quantum Technology* 8, art. 24 (2021): 38.

⁸⁸ Sarah Yasmin Hussain, "Application of Quantum Magnetometers to Security and Defence Screening" (PhD diss., University College London, 2018), 82; Krelina, "Quantum Technology for Military Applications," 38.

using magnetic and gravitational navigation offer passive, jam resistant positioning that complements rather than replaces existing Global Navigation Satellite Systems.⁸⁹

Quantum Radar and the Erosion of Stealth

Quantum radar, grounded in the principle of quantum illumination, employs entangled photon pairs to detect targets with minimal radar cross sections, even in high noise and jamming environments. This capability has the potential to negate the advantages that stealth technology currently confers. Quantum radio frequency sensing technologies, particularly those based on Rydberg atoms and nitrogen-vacancy centers, offer enhanced sensitivity, self calibration, and resistance to jamming across a wide frequency range from kilohertz to terahertz.⁹⁰ For states confronting adversaries fielding fifth generation stealth aircraft, quantum radar addresses a critical vulnerability: existing systems perform poorly against platforms engineered to reduce electromagnetic visibility through geometric design, energy absorbing surface materials, and cross section reduction methods.⁹¹ The erosion of stealth directly intensifies the security dilemma. States that have invested heavily in low observable platforms as survivable delivery systems face the prospect that a core pillar of their deterrent posture is depreciating, incentivizing either preemptive use or costly force structure diversification.

Beyond detection of stealth platforms, incorporating quantum clocks into radar systems

enhances their ability to identify and track small, slow moving objects such as drones over long distances. Quantum transducers that convert microwave signals into optical frequencies further extend these gains, enabling radar systems to achieve higher sensitivity and resolution across greater ranges.⁹² Nevertheless, quantum radar deployment faces major obstacles: current entangled photon generation rates remain far below operational requirements, and prototypes are too fragile for the vibration, temperature, and noise of combat environments.⁹³ Assertions that quantum radar will immediately render stealth aircraft or submarines obsolete should be approached with skepticism. The technology will more likely mature into hybrid systems paired with conventional sensors, enhancing detection in specific operational environments rather than transforming air defense architectures wholesale.⁹⁴ Even incremental gains in detection capability alter the counterforce calculus examined in section seven, as marginal improvements in sensing compound with precision strike advances to narrow the survivability margin on which deterrence depends.

Quantum Communications and Secure Networks

Quantum communications built on Quantum Key Distribution (QKD) exploit quantum state properties to transmit cryptographic keys with provable security, as any interception disturbs the photons and reveals the intrusion to both parties.⁹⁵ The integration of QKD into satellite communications marks a significant advancement, as space based quantum links offer

⁸⁹ Ryan S. Cassel, William G. Tobias, and Bonnie L. Marlow, *Quantum vs. Classical Complementary PNT: Are Quantum Sensors the Next Big Thing for PNT, or Are They Overhyped?* (McLean, VA: MITRE, 2023), 1, 9.

⁹⁰ Michal Krelna, "Quantum-Enhanced Radars and Electronic Warfare: Use Cases and Timelines," *JAPCC Journal*, no. 37 (2024): 29–30.

⁹¹ Rajat Singha, "Quantum Radar for Future Indian Air Defence: Comparative Evaluation and Implementation Prospects," *International Journal of Engineering Research and Technology* 15, no. 1 (January 2026): 1-2.

⁹² Krelna, "Quantum-Enhanced Radars and Electronic Warfare," 32–33.

⁹³ Krelna, "Quantum Technology for Military Applications," 20.

⁹⁴ Tomoshige and Singerman, *Quantum Sensing and the Future of Warfare*, 7-8.

⁹⁵ Kristina Aileen Meier, Raymond Thorson Newell, and Nicholas Dallmann, "Space-Based Quantum Networks Are an Essential Component of Future Architecture for Distributed Quantum Computers and Quantum-Enhanced Secure Communication" (Los Alamos, NM: Los Alamos National Laboratory, May 1, 2023), 1-2.

transmission losses orders of magnitude lower than those of terrestrial fiber optic networks, facilitating the distribution of encryption keys over continental and intercontinental distances.⁹⁶ China's 2016 launch of the Micius satellite demonstrated satellite-to-ground quantum key distribution and entanglement distribution, establishing Beijing as an early global leader in space based quantum communications infrastructure.⁹⁷ In contrast, the United States lacks a large scale quantum satellite mission, a deficiency that researchers at Los Alamos National Laboratory have identified as a potential national security concern given the accelerating capabilities of other nations.⁹⁸ Beyond point to point encryption, quantum networking offers the capability to link quantum computers spread across different locations, significantly boosting computing power and facilitating distributed quantum sensing with heightened sensitivity for military and intelligence purposes.⁹⁹

Policy Approaches to Quantum Dominance

The differing policy frameworks that Washington and Beijing employ to achieve quantum leadership highlight deeper structural and philosophical distinctions that influence the course of their strategic rivalry. China's fourteenth five year plan prioritized quantum technology, and while exact spending remains unclear, Beijing claims to spend eight times more than the United States on quantum research, with defined national goals driving sustained investment.¹⁰⁰

⁹⁶ "The Use of Quantum-Based Technologies for Secure Satellite Communications in Support of European Union Space Security and Defence" (master's thesis, University of Glasgow, University of Trento, Charles University, 2023), 64.

⁹⁷ Federici and Dagher-Margosian, *Vying for Quantum Supremacy*, 8-9; Krelina, "Quantum Technology for Military Applications," 39.

⁹⁸ Meier, Newell, and Dallmann, "Space-Based Quantum Networks," 1-2.

⁹⁹ Michal Krelina and Denis Dúbravčík, "Quantum Technologies for Air and Space (Part 3 of 3): Quantum for ISR and PNT: Use Cases and Timelines," *JAPCC Journal* (2024): 38-39; Federici and Dagher-Margosian, *Vying for Quantum Supremacy*, 7.

The United States has advanced quantum development through the National Quantum Initiative Act of 2018 and subsequent coordination mechanisms, directing federal investment via the DOE, NSF, and defense agencies. However, the decentralized nature of this approach can fragment efforts across competing institutional priorities.¹⁰¹ Comparative analysis shows the U.S. framework, driven by market competition, emphasizes private sector innovation, while China's collectivist approach prioritizes government coordination and alignment of quantum technology with national security and economic objectives.¹⁰²

The implications of the quantum race extend beyond any single capability to the broader architecture of deterrent stability. Quantum sensing threatens to strip away the concealment on which submarine based second strike forces depend, while the orbital security dilemma generates preemptive incentives against early warning systems and AI driven decision compression shortens crisis timelines. A state confronting these three pressures simultaneously faces an escalation calculus in which restraint carries existential risk. What remains is the temporal margin for crisis deliberation, and it is precisely this margin that hypersonic weapons collapse.

¹⁰⁰ Center for Strategic and International Studies, *Report from CSIS Commission on U.S. Quantum Leadership* (Washington, DC: Center for Strategic and International Studies, 2025), 20.

¹⁰¹ National Quantum Initiative Act, Pub. L. No. 115-368, 132 Stat. 5092 (2018); Hideki Tomoshige and Phillip Singerman, *Progress Toward Practical Areas of Quantum Technology* (Washington, DC: Center for Strategic and International Studies, 2025), 5-7; Shangkun Wang and Chunle Ni, "Comparative Analysis of Quantum Technology Policies in the United States and China: Strategic Directions and Philosophical Foundations," *Quantum Reports* 8, no. 1 (2026): 2-3.

¹⁰² Wang and Ni, "Comparative Analysis of Quantum Technology," 12-14.

Hypersonics And the Compression of Crisis Time

The development of hypersonic weapons represents a defining challenge to existing defense architectures, driven by the enduring strategic imperative of speed in modern warfare.¹⁰³ Hypersonic weapons, defined as those traveling at Mach 5 or higher, fall into two categories: hypersonic cruise missiles using scramjet engines, and hypersonic glide vehicles that use rockets to reach altitude and speed before gliding to targets.¹⁰⁴ Three characteristics render these systems strategically transformative: speed, range, and survivability, as they operate at altitudes below traditional intercontinental ballistic missile flight profiles but above the engagement envelopes of most contemporary air defense systems.¹⁰⁵ Their high maneuverability and unpredictable flight paths compound the challenge for defenders, as these weapons cover approximately one mile per second, compressing detection, assessment, and response time beyond existing defensive frameworks.¹⁰⁶ Over the past two decades, China and Russia have exploited a lapse in American strategic focus to rapidly develop, test, and deploy these weapons, producing a capabilities gap that directly threatens the existing deterrent architecture.¹⁰⁷

The strategic drivers behind Chinese and Russian hypersonic programs reflect distinct but complementary motivations rooted in countering American military advantages. The People's Republic of China (PRC) considers hypersonic weapons crucial for restricting access and denying area usage in the

South China Sea, forcing U.S. forces to maintain standoff distances that would limit military responsiveness in a Taiwan contingency.¹⁰⁸ China's operational hypersonic portfolio includes the DF-17 medium range ballistic missile designed to carry the conventional or nuclear armed DF-ZF hypersonic glide vehicle, complemented by the nuclear-capable Starry Sky-2 system.¹⁰⁹ Russia has prioritized hypersonic development to defeat United States missile defense systems, fielding the Kinzhal air-launched missile, the Tsirkon sea-launched system, and the Avangard strategic glide vehicle designed to strike key command and control centers.¹¹⁰ Both states have declared hypersonic weapons capable of carrying conventional or nuclear payloads, creating ambiguity in crisis decision making, as states receiving a launch may be unable to determine warhead type and default to worst-case assumptions.¹¹¹

Compressed response timelines and payload ambiguity render the rational deliberation assumed by classical deterrence theory impossible. A hypersonic strike against early warning assets could collapse the detection window space systems are meant to provide. The speed of delivery pushes NC3 decision making beyond human cognitive capacity. And dual use payload ambiguity merges with quantum erosion of second strike concealment, leaving a defender unable to determine whether an incoming strike is conventional or nuclear, unable to rely on concealed retaliatory forces, and without time to deliberate. It is this convergence, rather than any single domain's

¹⁰³ Jonah S. Bhide, "Hypersonic Weapons: Strategic Drivers and Policy Proposals," *Space and Defense* 12, no. 2 (June 2021): 75.

¹⁰⁴ Eric Pratson, *The Need for Speed: The Case for Continued Development of Hypersonic and Directed Energy Weapons* (Washington, DC: National Defense University, Dwight D. Eisenhower School for National Security and Resource Strategy, 2023), 3.

¹⁰⁵ Pratson, *The Need for Speed*, 3.

¹⁰⁶ Pratson, *The Need for Speed*, 3.

¹⁰⁷ Pratson, *The Need for Speed*, iv, 1.

¹⁰⁸ Pratson, *The Need for Speed*, 5, 25; Bhide, "Hypersonic Weapons," 76-78.

¹⁰⁹ Pratson, *The Need for Speed*, 5.

¹¹⁰ Pratson, *The Need for Speed*, 6; Julia L. Diamond, "Russian Development of New Hypersonic Weapons: Drivers and Implications," *Space and Defense* 12, no. 2 (June 2021): 19-20.

¹¹¹ Pratson, *The Need for Speed*, 26.

instability, that constitutes the intelligentized security dilemma.

Entanglement and the New Era of Counterforce

The technological developments examined in the preceding sections do not operate in isolation; rather, they converge to undermine the survivability of nuclear arsenals upon which deterrence depends. Advances rooted in the computer revolution, particularly leaps in weapons accuracy and remote sensing, have rendered nuclear arsenals worldwide more susceptible than ever before in the history of the atomic era.¹¹² Hardening has been fundamentally refuted by improvements in delivery system precision, while concealment faces erosion from a sensor technology revolution threatening mobile and submarine based forces.¹¹³ Five trends are producing unprecedented transparency: the proliferation of sensing platforms, advances in computing power, improvements in the networking of sensors with command systems, gains in sensor resolution across multiple spectra, and an increase in data transmission speed.¹¹⁴ This new counterforce environment reopens the question of whether enhanced disarming-strike capabilities strengthen deterrence or trigger arms racing and preemptive incentives that exacerbate crisis instability.¹¹⁵

These counterforce trends impose acute challenges on nuclear planners tasked with maintaining credible deterrence amid technological disruption. Deploying weapon systems that will remain survivable for decades while offensive technologies improve at accelerating rates represents

an extraordinary challenge in planning.¹¹⁶ Simultaneous advances in precision conventional strike, missile defense, antisubmarine warfare, and cyber operations compound the vulnerability of retaliatory arsenals, raising questions about the wisdom of arms reductions that shrink the number of targets an attacker must destroy.¹¹⁷ Rather than being a permanent aspect of the international system, the nuclear stalemate now seems contingent and potentially reversible. The paradox is that restraint in force modernization may leave states dangerously exposed, while the pursuit of survivability through expansion risks triggering the security spirals that arms control was designed to prevent.¹¹⁸

The destabilizing effects of counterforce advancements reverberate across regional theaters, where nuclear rivalries compound the risks of inadvertent escalation. South Asia illustrates this dynamic: the Pakistan-India rivalry, marked by four wars since 1947 and nuclear acquisition in 1998, presents persistent escalation danger where territorial disputes, asymmetric capabilities, and absent crisis communication intersect with growing arsenals.¹¹⁹ The pattern of recurring crises, from the wars of 1947, 1965, and 1971 through the Kargil conflict of 1999, underscores the persistent danger of escalation in a nuclear-armed dyad lacking robust crisis management mechanisms.¹²⁰

In Northeast Asia, a U.S. China military confrontation would present acute risks, as space and cyber assets integral to both nations' command and intelligence systems create pressure for preemptive

¹¹² Keir A. Lieber and Daryl G. Press, "The New Era of Counterforce: Technological Change and the Future of Nuclear Deterrence," *International Security* 41, no. 4 (Spring 2017): 9-10.

¹¹³ Lieber and Press, "New Era of Counterforce," 10, 18.

¹¹⁴ Lieber and Press, "New Era of Counterforce," 32-34.

¹¹⁵ Lieber and Press, "New Era of Counterforce," 12, 48-49.

¹¹⁶ Brooke Mitchell, "Nuclear Planning in an Uncertain World," *Space and Defense* 12, no. 2 (June 2021): 58-60.

¹¹⁷ Lieber and Press, "New Era of Counterforce," 12; Mitchell, "Nuclear Planning in an Uncertain World," 62.

¹¹⁸ Lieber and Press, "New Era of Counterforce," 48-49; Mitchell, "Nuclear Planning in an Uncertain World," 62-64.

¹¹⁹ Jahan Zaib Adil, Mehar Sohail, and Shazad Farid, "Pak-India War Crisis: A Historical and Strategic Analysis," *The Critical Review of Social Sciences Studies* 3, no. 3 (2025): 131-32.

¹²⁰ Adil, Sohail, and Farid, "Pak-India War Crisis," 131-35.

nonnuclear strikes driven by fear of losing these capabilities.¹²¹ China's deployment of nuclear and conventional medium range ballistic missiles with dual purpose bases and sensors complicates American differentiation between nuclear and conventional targets, while Chinese officials might perceive strikes on dual use infrastructure as efforts to dismantle their nuclear deterrent.¹²² Blurred nuclear thresholds, interacting with counterspace and cyber vulnerabilities, create cascading escalation risks that underscore the inadequacy of existing crisis management frameworks.¹²³ A Taiwan contingency would compound these pressures by forcing the PLA to balance its primary focus against competing requirements across theaters, introducing uncertainty into an already fragile escalatory calculus.¹²⁴ The convergence of counterforce technology, entangled force architectures, and multitheater demands creates a security environment in which the distinction between conventional and nuclear conflict has grown perilously thin.¹²⁵

¹²¹ Vincent A. Manzo, "After the First Shots: Managing Escalation in Northeast Asia," *Joint Force Quarterly* 77 (2nd Quarter 2015): 91-92.

¹²² Manzo, "After the First Shots," 97.

¹²³ Manzo, "After the First Shots," 97-98.

¹²⁴ Joel Wuthnow, *System Overload: Can China's Military Be Distracted in a War over Taiwan?*, China Strategic Perspectives, no. 15 (Washington, DC: National Defense University Press, 2020), 4-6.

¹²⁵ Wuthnow, *System Overload*, 26, 34; Manzo, "After the First Shots," 98-99.

Internal Friction: A Net Assessment

The preceding sections establish the destabilizing potential of the intelligentized security dilemma. However, the PLA's capacity to fully operationalize these capabilities remains constrained by institutional and human capital deficits that temper near term strategic risk without eliminating it. This section assesses those constraints, not as a separate topic but as a net assessment of the gap between the doctrine's ambition and the force that must execute it.

The Modernization Trajectory

At the 19th Party Congress in 2017, Xi Jinping outlined a three stage modernization roadmap: complete basic mechanization and advance informatization by 2020, broadly achieve military modernization by 2035, and build a world class force by mid century.¹²⁶ The PLA undeniably possesses a range of capabilities that rival those of the world's leading militaries, including fifth generation aircraft, the largest naval fleet globally, an expanding nuclear arsenal, and a rapidly advancing proficiency in joint domain warfare.¹²⁷ In this context, the PLA and the United States military stand out as the sole militaries of world class caliber today.¹²⁸ Nonetheless, endemic corruption across PLA procurement, acquisitions, and personnel systems has persisted despite over a decade of aggressive anticorruption enforcement under Xi

¹²⁶ Xi Jinping, "Secure a Decisive Victory in Building a Moderately Prosperous Society in All Respects and Strive for the Great Success of Socialism with Chinese Characteristics for a New Era" (report delivered at the 19th National Congress of the Communist Party of China, October 18, 2017), Xinhua, November 3, 2017, https://www.mfa.gov.cn/web/ziliao_674904/zl_674979/dnzt_674981/qt_zt/twwt/xjipzsjstzyjh/202206/t20220606_10698869.html; Meia Nouwens, "AI and the PLA's New Revolution in Military Affairs: Moving from Weapons Applications toward a Battle Brain," in *The PLA's Long March toward a World-Class Military: Progress, Obstacles, and Ambitions*, ed. Benjamin Frohman and Jeremy Rausch (Seattle: The National Bureau of Asian Research, 2025), 96.

¹²⁷ Evan McKinney, "The PLA as a 'World-Class' Tool of National Power," in *The PLA's Long March toward a World-Class Military:*

Jinping. Systemic graft has penetrated the Rocket Force leadership, the Central Military Commission (CMC) Equipment Development Department, and China's broader defense industrial complex.¹²⁹ This pattern reveals a fundamental tension between the PLA's modernization timeline and the structural deficiencies undermining its realization. This includes absent impartial civilian oversight, immature procurement mechanisms, fraudulent research practices within the defense science ecosystem, and personnel quality lagging behind hardware advances.¹³⁰

Organizational Constraints

The PRC's 2019 defense white paper acknowledged the PLA had not completed mechanization, faced risks from technological surprise and a widening generational gap in military technology, and remained far behind the world's leading armed forces.¹³¹ Endemic corruption, rooted in the absence of impartial civilian oversight mechanisms and independent checks on party authority, remains one of the most corrosive obstacles to the PLA's modernization trajectory.¹³² Since the 18th Party Congress in 2012, Xi's anticorruption campaign has removed dozens of general-grade officers and over a hundred at the corps deputy leader level or above, with recent purges concentrated on the Rocket Force, the CMC Equipment Development Department, and senior executives in state owned defense enterprises.¹³³ In

Progress, Obstacles, and Ambitions, ed. Benjamin Frohman and Jeremy Rausch (Seattle: The National Bureau of Asian Research, 2025), 15-16.

¹²⁸ McKinney, "The PLA as a 'World-Class' Tool of National Power," 23-27.

¹²⁹ James Char, "Corruption and Reliability Concerns in a World-Class PLA," in *The PLA's Long March toward a World-Class Military*, ed. Frohman and Rausch, 31-42.

¹³⁰ Char, "Corruption and Reliability Concerns," 44-50, 53-54.

¹³¹ State Council Information Office of the People's Republic of China, *China's National Defense in the New Era* (Beijing: Foreign Languages Press, July 2019), 4-6.

¹³² Char, "Corruption and Reliability Concerns," 46-47.

¹³³ Char, "Corruption and Reliability Concerns," 31, 42-44.

July 2023, Xi dismantled the entire senior leadership of the PLA Rocket Force and installed replacements with no artillery background, a decision that underscored the depth of his distrust toward the force's highest echelons.¹³⁴ That Xi has found it necessary to continue these purges for over a decade raises fundamental questions about the campaign's efficacy, suggesting that periodic cleanups are less a corrective mechanism than a recurring symptom of centralized single party governance.¹³⁵

Beyond these institutional weaknesses, PLA leaders have conceded that human capital remains a significant liability. Internal evaluations have pointed to gaps in basic warfighting competencies, insufficient infrastructure for realistic training, and a chronic inability to produce enough servicemembers with the technical expertise the force requires.¹³⁶ These shortcomings are further encapsulated in the longstanding critique of officers who cannot adequately evaluate operational conditions, interpret higher level intent, exercise sound tactical judgment, manage forces under pressure, or adapt to unforeseen developments on the battlefield. The PLA's lack of recent combat experience compounds these deficiencies, as the force has been compelled to pursue modernization through theoretical study and simulation rather than operational learning.¹³⁷ Simultaneously, the military faces acute difficulties in recruiting and retaining high caliber technical talent, as private sector employers offer compensation that vastly exceeds military pay scales.¹³⁸

Technology and Doctrine Gaps

Despite the doctrinal priority placed on intelligentization, the gap between aspiration and implementation remains considerable.¹³⁹ Realizing the vision of an AI "battle brain" that functions as a digital staff officer requires breakthroughs in core technologies, development of professional evaluation cadres, massive training data, and robust testing frameworks for intelligent battlefield command systems.¹⁴⁰ Shortcomings in talent hinder the PLA's capability to leverage AI, as challenges in recruiting technically proficient officers and enlisted personnel compete directly with the intense demands of China's growing private technology sector.¹⁴¹ The PLA's identity as a Party army, mandating strict adherence to the Party's absolute leadership and prioritizing political work, may impede the creativity essential for technological innovation. Time spent on political activities detracts from training, and ideological indoctrination may not foster the experimental culture AI integration requires.¹⁴² Despite progress in training realism and expanded science and technology education, the PLA may continue to struggle to match the sophistication required for intelligentized warfare.¹⁴³

Military-Civil Fusion

Xi Jinping has raised Military-Civil Fusion (军民融合) to the level of national strategy, making it the principal mechanism through which Beijing channels the dual use potential of China's vast commercial

¹³⁴ Char, "Corruption and Reliability Concerns," 42-43.

¹³⁵ Char, "Corruption and Reliability Concerns," 50.

¹³⁶ Eric Hundman, "Gaining the Upper Hand in Future Wars? Developing the Personnel of the PLA," in *The PLA's Long March toward a World-Class Military*, ed. Frohman and Rausch, 73-74.

¹³⁷ Hundman, "Gaining the Upper Hand in Future Wars?" 74, 78; Elsa B. Kania, *Chinese Military Innovation in Artificial Intelligence* (testimony before the U.S.-China Economic and Security Review Commission, June 7, 2019), 28, 30.

¹³⁸ Hundman, "Gaining the Upper Hand in Future Wars?" 89, 91; Kania, *Chinese Military Innovation in Artificial Intelligence*, 28.

¹³⁹ Nouwens, "AI and the PLA's New Revolution in Military Affairs," 95.

¹⁴⁰ Nouwens, "AI and the PLA's New Revolution in Military Affairs," 106-7.

¹⁴¹ Kania, *Chinese Military Innovation in Artificial Intelligence*, 28.

¹⁴² Kania, *Chinese Military Innovation in Artificial Intelligence*, 30-31.

¹⁴³ Hundman, "Gaining the Upper Hand in Future Wars?" 89; Kania, *Chinese Military Innovation in Artificial Intelligence*, 28.

technology base into the PLA's modernization efforts.¹⁴⁴ The strategy's scope is considerable: China has leveraged its manufacturing capacity, dominance in dual use energy technologies, and supercomputing achievements to build an industrial base advancing both economic development and military capability.¹⁴⁵ Chinese Communist Party (CCP) leaders have placed advanced manufacturing, AI, aerospace, and other technologies at the core of national development and defense planning, with the Fourteenth Five Year Plan emphasizing deep integration of advanced production with military modernization.¹⁴⁶ Despite these structural advantages, the implementation of Military-Civil Fusion remains uneven. The defense industry has continued to operate with relative inefficiency, while private technology firms have been slow to participate owing to bureaucratic obstacles, fragmented coordination between military and civilian entities, and the procurement corruption documented in the preceding section.¹⁴⁷ The scope of these initiatives indicates systemic advantage potential, but bureaucratic fragmentation and entrenched interests suggest that the strategy's transformative promise remains an ongoing challenge rather than a realized fact.¹⁴⁸

Assessing the Net Strategic Risk

These internal frictions are real and consequential, and they will delay the PLA's full realization of intelligentized warfare. However, they do not negate the destabilizing dynamics identified above. An adversary must plan against the capability trajectory, not merely against present shortfalls. Many compound dynamics, including dual use ambiguity, orbital preemptive incentives, and nuclear conventional

entanglement, exist independently of whether the PLA has perfected its AI "battle brain." Moreover, internal friction creates its own instability: a leadership uncertain about its own systems' reliability may face pressure to act preemptively rather than depend on untested capabilities in combat. The gap between ambition and reality thus compounds the escalation risks the intelligentized security dilemma produces.

¹⁴⁴ Liza Tobin, Addis Goldman, and Katherine Kurata, "System by Design: The Evolution of China's Military-Civil Fusion Strategy," in *The PLA's Long March toward a World-Class Military*, ed. Frohman and Rausch, 119-20.

¹⁴⁵ Tobin, Goldman, and Kurata, "System by Design," 136-37.

¹⁴⁶ Tobin, Goldman, and Kurata, "System by Design," 137.

¹⁴⁷ Kania, *Chinese Military Innovation in Artificial Intelligence*, 29; Tobin, Goldman, and Kurata, "System by Design," 120.

¹⁴⁸ Tobin, Goldman, and Kurata, "System by Design," 120; Char, "Corruption and Reliability Concerns," 50.

Reimagining Stability

Conclusion

The AI competition between Washington and Beijing stems from geopolitical tensions and mutual threat perceptions driving both states toward militarization, as each views the other's advances as existential challenges requiring a response.¹⁴⁹ This competition unfolds in an age of strategic rivalry in which Beijing pursues a strategy integrating aggressive diplomacy, asymmetric economic agreements, technological innovation, and military expenditures to position China for global preeminence.¹⁵⁰ The Department of Defense assesses that Beijing's strategic center remains the First Island Chain; however, as China grows wealthier and more powerful, its military capabilities will extend toward global power projection, aligned with fielding a world-class military (世界一流军队) by 2049.¹⁵¹ Within this trajectory, the convergence of systems destruction warfare with intelligentized capabilities across space, cyber, quantum, and hypersonic domains has rendered the boundaries between peacetime competition, crises, and armed conflict dangerously indistinct.

The structural dynamics of this competition align with offensive realist predictions that rising powers seek regional hegemony, as China's policies toward Taiwan and the Belt and Road Initiative reflect an assertive posture to expand influence and constrain American power in the Asia-Pacific.¹⁵² The

intelligentized security dilemma compounds these structural pressures by introducing variables that classical power transition theories did not anticipate: compressed decision timelines, entangled architectures, and algorithm based confrontation. Preparing for this environment requires the analytical and policy communities to examine how great powers leverage the information environment, electromagnetic operations, and cyber capabilities to accumulate strategic advantage below the threshold of armed conflict.¹⁵³

The compound dynamics this article identifies demand governance mechanisms tailored to the specific interactions between domains rather than generic confidence building measures. The governance architecture for managing AI related military crises encompasses a spectrum of instruments, from informal joint declarations through legally binding treaties to structured transparency and communication protocols between adversaries.¹⁵⁴ However, the compounding effects analyzed above point to three priority areas where domain specific interventions could reduce the risk of inadvertent escalation.

First, within the AI and NC3 domain, Washington and Beijing should develop shared classification systems for AI related failures categorized by severity, frequency, and response timelines; jointly agreed parameters identifying AI enabled military behaviors crossing acceptable thresholds; and uniform reporting procedures for incidents involving AI operated platforms. The most

¹⁴⁹ Maria Bega, "The New Arms Race Between China and the US: A Comparative Analysis of AI-Powered Military and Economic Pursuits," *Europolity* 17, no. 2 (2023): 96.

¹⁵⁰ Canadian Security Intelligence Service, *China and the Age of Strategic Rivalry*, World Watch: Expert Notes Series Publication No. 2018-05-02 (Ottawa: Canadian Security Intelligence Service, 2018), 7.

¹⁵¹ U.S. Department of Defense, *Report to Congress on Military and Security Developments Involving the People's Republic of China 2025* (Washington, DC: U.S. Department of Defense, 2025), V.

¹⁵² Kaan Talha Kizilaslan, "The Rise of China: The Taiwan Question, the Belt and Road Initiative and Offensive Structural Realism" (master's thesis, Middle East Technical University, 2023), 164-67.

¹⁵³ Karagosian, "Reimagining the Future," 9-12.

¹⁵⁴ Sisson et al., *Steps Toward AI Governance in the Military Domain*, 5-6.

urgent near term step is securing commitments that a human decision maker retains authority during peacetime interactions between American and PLA forces, directly countering the compressed decision cycles AI integration imposes on nuclear command architectures.¹⁵⁵ The existing institutional foundation for such dialogue, however limited, is the November 2023 Biden-Xi agreement to discuss AI safety, which could be expanded into a structured bilateral working group with a defined technical agenda.¹⁵⁶ Safety standards for AI enabled military systems must ensure human control over final decisions, particularly the use of force, while arms control agreements must expand to address autonomous weapons and AI enhanced command structures.¹⁵⁷

Second, in the space domain, the dual use detection and disclosure dilemma identified by Vaynman and Volpe means that traditional verification mechanisms cannot overcome the ambiguity inherent in orbital systems.¹⁵⁸ A deterrence strategy combining defensive and offensive counterspace actions, resilience measures, and reconstitution to mitigate damage and preserve essential capabilities offers the most promising foundation for stability, though no single approach guarantees success against a capable adversary.¹⁵⁹ This analysis supports investment in resilience based deterrence, including distributed satellite architectures, rapid reconstitution capabilities, and diversified ground station networks. Such measures reduce the preemptive incentives the orbital security dilemma generates rather than relying on punitive

threats that dual use ambiguity makes difficult to credibly communicate.

Third, in the cyber and cognitive domain, research on crisis negotiations indicates that cyber operations can serve as exit ramps for escalating crises, enabling states to demonstrate determination and alter information balances without incurring human casualties that exacerbate conflict.¹⁶⁰ To preserve this deescalatory potential while managing the risks of AI driven information warfare and cognitive domain operations, policymakers should pursue two lines of effort. The first is dismantling the barriers between the nuclear policy and national security communities to ensure that decision makers understand the compound information environment before a crisis. The second is engaging in realistic decision making exercises that simulate the interaction of space, cyber, AI, and hypersonic threats simultaneously rather than in isolation.¹⁶¹

The compound dynamics identified in this article are not static. Each technological domain continues to mature, and the interactions between them will intensify as AI integration accelerates, quantum sensing narrows the margin of concealment, and hypersonic delivery systems proliferate beyond the current handful of states. If the governance mechanisms proposed above are not pursued, the window for establishing shared norms and communication protocols will narrow alongside the decision timelines the technologies themselves compress. The greatest danger was never any single capability; it is the accelerating integration of

¹⁵⁵ Sisson et al., *Steps Toward AI Governance in the Military Domain*, 11-13.

¹⁵⁶ White House, "Readout of President Joe Biden's Meeting with President Xi Jinping of the People's Republic of China," November 15, 2023, <https://bidenwhitehouse.archives.gov/briefing-room/statements-releases/2023/11/15/readout-of-president-joe-bidens-meeting-with-president-xi-jinping-of-the-peoples-republic-of-china-2/>.

¹⁵⁷ Johnson, *Artificial Intelligence and Nuclear Stability*, 9-10.

¹⁵⁸ Vaynman and Volpe, "Dual Use Deception," 607-10.

¹⁵⁹ Flanagan et al., *A Framework of Deterrence in Space Operations*, 30-36.

¹⁶⁰ Valeriano and Jensen, "De-escalation Pathways," 87-88.

¹⁶¹ Hersman, "Wormhole Escalation," 108-9.

destabilizing technologies within a doctrine that targets the architectures on which strategic stability depends.

REFERENCES

- Abdullah, Sannia. "Pakistan's Space Program: From Sounding Rockets to Satellite Setbacks." *Space and Defense* 12, no. 2 (June 2021): 40-57.
<https://doi.org/10.32873/uno.dc.sd.12.02.1072>
- Adil, Jahan Zaib, Mehar Sohail, and Shazad Farid. "Pak-India War Crisis: A Historical and Strategic Analysis." *The Critical Review of Social Sciences Studies* 3, no. 3 (2025): 131–44. <https://doi.org/10.59075/34wptt74>
- Allison, Graham, Kevin Klyman, Karina Barbesino, and Hugo Yen. *The Great Tech Rivalry: China vs the U.S.* Cambridge, MA: Belfer Center for Science and International Affairs, Harvard Kennedy School, 2021.
- Baughman, Joshua. "The Path to China's Intelligitized Warfare: Converging on the Metaverse Battlefield." *The Cyber Defense Review* 9, no. 3 (Fall 2024): 29-36.
- Bega, Maria. "The New Arms Race Between China and the US: A Comparative Analysis of AI-Powered Military and Economic Pursuits." *Europolity* 17, no. 2 (2023): 75–109.
<https://doi.org/10.25019/europolity.2023.17.2.3>
- Bhide, Jonah S. "Hypersonic Weapons: Strategic Drivers and Policy Proposals." *Space and Defense* 12, no. 2 (June 2021): 75-94. <https://doi.org/10.32873/uno.dc.sd.12.02.1075>
- Burke, Edmund J., Kristen Gunness, Cortez A. Cooper III, and Mark Cozad. *People's Liberation Army Operational Concepts*. Santa Monica, CA: RAND Corporation, 2020.
<https://doi.org/10.7249/RRA394-1>
- Canadian Security Intelligence Service. *China and the Age of Strategic Rivalry*. World Watch: Expert Notes Series Publication No. 2018-05-02. Ottawa: Canadian Security Intelligence Service, 2018.
- Cassel, Ryan S., William G. Tobias, and Bonnie L. Marlow. *Quantum vs. Classical Complementary PNT: Are Quantum Sensors the Next Big Thing for PNT, or Are They Overhyped?* McLean, VA: MITRE, 2023.
- Center for Strategic and International Studies. *Report from CSIS Commission on U.S. Quantum Leadership*. Washington, DC: Center for Strategic and International Studies, 2025.
- Char, James. "Corruption and Reliability Concerns in a World-Class PLA." In *The PLA's Long March toward a World-Class Military: Progress, Obstacles, and Ambitions*, edited by Benjamin Frohman and Jeremy Rausch, 30–70. Seattle: The National Bureau of Asian Research, 2025.
- Cox, Dan G. "The Need for a Cyber Smoke Screen: A Tactical Action that Instantly Becomes Strategic in an All-Domain Operation." *The Cyber Defense Review* 9, no. 3 (Fall 2024): 17–25.

- Cozad, Mark, Jeffrey Engstrom, Scott W. Harold, Timothy R. Heath, Sale Lilly, Edmund J. Burke, Julia Brackup, and Derek Grossman. *Gaining Victory in Systems Warfare: China's Perspective on the U.S.-China Military Balance*. Santa Monica, CA: RAND Corporation, 2023. <https://doi.org/10.7249/RRA1535-1>
- Diamond, Julia L. "Russian Development of New Hypersonic Weapons: Drivers and Implications." *Space and Defense* 12, no. 2 (June 2021): 6-39. <https://doi.org/10.32873/uno.dc.sd.12.02.1071>
- Engstrom, Jeffrey. *Systems Confrontation and System Destruction Warfare: How the Chinese People's Liberation Army Seeks to Wage Modern Warfare*. Santa Monica, CA: RAND Corporation, 2018. <https://doi.org/10.7249/RR1708>
- Federici, Joseph, and Matthew Dagher-Margosian. *Vying for Quantum Supremacy: U.S.-China Competition in Quantum Technologies*. Washington, DC: U.S.-China Economic and Security Review Commission, 2025.
- Flanagan, Stephen J., Nicholas Martin, Alexis A. Blanc, and Nathan Beauchamp-Mustafaga. *A Framework of Deterrence in Space Operations*. Santa Monica, CA: RAND Corporation, 2023. <https://doi.org/10.7249/RRA820-1>
- Hersman, Rebecca. "Wormhole Escalation in the New Nuclear Age." *Texas National Security Review* 3, no. 3 (Summer 2020): 90–109. <http://dx.doi.org/10.26153/tsw/10220>
- Hiim, Henrik Stålhane, and Øystein Tunsjø. "The U.S.-China Stability-Instability Paradox: Limited War in East Asia." *International Security* 50, no. 1 (Summer 2025): 152–81. <https://doi.org/10.1162/ISEC.a.8>
- Hundman, Eric. "Gaining the Upper Hand in Future Wars? Developing the Personnel of the PLA." In *The PLA's Long March toward a World-Class Military: Progress, Obstacles, and Ambitions*, edited by Benjamin Frohman and Jeremy Rausch, 72–92. Seattle: The National Bureau of Asian Research, 2025.
- Hussain, Sarah Yasmin. "Application of Quantum Magnetometers to Security and Defence Screening." PhD thesis, University College London, 2018.
- "The Use of Quantum-Based Technologies for Secure Satellite Communications in Support of European Union Space Security and Defence." Master's thesis, University of Glasgow, University of Trento, Charles University, 2023.
- Jervis, Robert. "Cooperation Under the Security Dilemma." *World Politics* 30, no. 2 (January 1978): 167-214. <https://doi.org/10.2307/2009958>
- Johnson, James. *Artificial Intelligence and Nuclear Stability: Understanding AI's Impact on Military Escalation Dynamics and Strategic Deterrence*. GC REAIM Expert Policy Note Series. The Hague: The Hague Centre for Strategic Studies, 2025.

- Johnson, James. *Artificial Intelligence and the Future of Warfare: The USA, China, and Strategic Stability*. Manchester: Manchester University Press, 2021.
- Johnson, James. "Inadvertent Escalation in the Age of Intelligence Machines: A New Model for Nuclear Risk in the Digital Age." *European Journal of International Security* 7, no. 3 (2022): 337–59. <https://doi.org/doi:10.1017/eis.2021.23>
- Johnson, James. "Revisiting the 'Stability–Instability Paradox' in AI-Enabled Warfare: A Modern-Day Promethean Tragedy Under the Nuclear Shadow." *Review of International Studies* (2024): 1–19. <https://doi.org/10.1017/S0260210524000767>
- Kania, Elsa B. *Chinese Military Innovation in Artificial Intelligence*. Testimony before the U.S.-China Economic and Security Review Commission, June 7, 2019.
- Karagosian, Deborah S. "Reimagining the Future." *The Cyber Defense Review* 9, no. 3 (Fall 2024): 9–13.
- Khalid, Ameema. "Strategic Vulnerabilities in Space: U.S.-China Militarization and the Risks to Global Strategic Stability." *Journal of Advanced Military Studies* 16, no. 2 (Fall 2025): 26–60. <https://doi.org/10.21140/mcu.20251602002>
- Kizilaslan, Kaan Talha. "The Rise of China: The Taiwan Question, the Belt and Road Initiative and Offensive Structural Realism." Master's thesis, Middle East Technical University, 2023.
- Krause, Juljan. *The Quantum Race: U.S.-Chinese Competition for Leadership in Quantum Technologies*. IGCC Policy Brief. La Jolla, CA: UC Institute on Global Conflict and Cooperation, 2024.
- Krelina, Michal. "Quantum Technology for Military Applications." *EPJ Quantum Technology* 8, art. 24 (2021). <https://doi.org/10.1140/epjqt/s40507-021-00113-y>
- Krelina, Michal. "Quantum-Enhanced Radars and Electronic Warfare: Use Cases and Timelines." *JAPCC Journal*, no. 37 (2024): 27–34.
- Krelina, Michal, and Denis Dúbravčík. "Quantum Technologies for Air and Space (Part 3 of 3): Quantum for ISR and PNT: Use Cases and Timelines." *JAPCC Journal*, no. 38 (2024): 36–43.
- Kühn, Ulrich. "Strategic Stability in the 21st Century: An Introduction." *Journal for Peace and Nuclear Disarmament* 6, no. 1 (2023): 1–8. <https://doi.org/10.1080/25751654.2023.2223804>
- Lieber, Keir A., and Daryl G. Press. "The End of MAD? The Nuclear Dimension of U.S. Primacy." *International Security* 30, no. 4 (Spring 2006): 7–44. <https://doi.org/10.1162/isec.2006.30.4.7>

- Lieber, Keir A., and Daryl G. Press. "The New Era of Counterforce: Technological Change and the Future of Nuclear Deterrence." *International Security* 41, no. 4 (Spring 2017): 9–49. https://doi.org/10.1162/ISEC_a_00273
- Lynch, Thomas F., III. "Forward Persistence in Great Power Cyber Competition: Military Assets in a Relative Power Erosion Framework." *The Cyber Defense Review* 9, no. 3 (Fall 2024): 81–103.
- Mallick, P. K. "Defining China's Intelligentized Warfare and Role of Artificial Intelligence." New Delhi: Vivekananda International Foundation, 2021.
- Manzo, Vincent A. "After the First Shots: Managing Escalation in Northeast Asia." *Joint Force Quarterly* 77 (2nd Quarter 2015): 91–100.
- McKinney, Evan. "The PLA as a 'World-Class' Tool of National Power." In *The PLA's Long March toward a World-Class Military: Progress, Obstacles, and Ambitions*, edited by Benjamin Frohman and Jeremy Rausch, 14–28. Seattle: The National Bureau of Asian Research, 2025.
- Meier, Kristina Aileen, Raymond Thorson Newell, and Nicholas Dallmann. "Space-Based Quantum Networks Are an Essential Component of Future Architecture for Distributed Quantum Computers and Quantum-Enhanced Secure Communication." Technical Report. Los Alamos, NM: Los Alamos National Laboratory, May 1, 2023. <https://doi.org/10.2172/1972170>
- Mian, Zia, R. Rajaraman, and M. V. Ramana. "Early Warning in South Asia: Constraints and Implications." *Science and Global Security* 11, no. 2–3 (2003): 109–50. <https://doi.org/10.1080/08929880390246949>
- Mitchell, Brooke. "Nuclear Planning in an Uncertain World." *Space and Defense* 12, no. 2 (June 2021): 58–66. <https://doi.org/10.32873/uno.dc.sd.12.02.1073>
- Mobilio, Sarah. "GenAI in the 2024 Taiwan Presidential Election: Lessons for Democracies." *The Cyber Defense Review* 9, no. 3 (Fall 2024): 51–63.
- Nouwens, Meia. "AI and the PLA's New Revolution in Military Affairs: Moving from Weapons Applications toward a Battle Brain." In *The PLA's Long March toward a World-Class Military: Progress, Obstacles, and Ambitions*, edited by Benjamin Frohman and Jeremy Rausch, 94–117. Seattle: The National Bureau of Asian Research, 2025.
- Pratson, Eric. *The Need for Speed: The Case for Continued Development of Hypersonic and Directed Energy Weapons*. Washington, DC: National Defense University, Dwight D. Eisenhower School for National Security and Resource Strategy, 2023.
- Singha, Rajat. "Quantum Radar for Future Indian Air Defence: Comparative Evaluation and Implementation Prospects." *International Journal of Engineering Research and Technology* 15, no. 1 (January 2026): 1–4. <https://doi.org/10.5281/zenodo.18296303>

- Sisson, Melanie W., Colin Kahl, Sun Chenghao, and Xiao Qian. *Steps Toward AI Governance in the Military Domain*. Washington, DC: The Brookings Institution, 2025.
- State Council Information Office of the People's Republic of China. *China's National Defense in the New Era*. Beijing: Foreign Languages Press, July 2019.
- Stickings, Alexandra. "The Normalisation of Anti-Satellite Capabilities." *Air and Space Power Review* 22, no. 2 (2019): 32–41.
- Szymanski, Paul. "Techniques for Great Power Space War." *Strategic Studies Quarterly* 13, no. 4 (Winter 2019): 78–104. <https://www.jstor.org/stable/26815047>
- T2COM. *How China Fights in Large-Scale Combat Operations*. T2COM OE Threat Assessment 1-1. U.S. Army, 2025.
- Tobin, Liza, Addis Goldman, and Katherine Kurata. "System by Design: The Evolution of China's Military-Civil Fusion Strategy." In *The PLA's Long March toward a World-Class Military: Progress, Obstacles, and Ambitions*, edited by Benjamin Frohman and Jeremy Rausch, 116–41. Seattle: The National Bureau of Asian Research, 2025.
- Tomoshige, Hideki, and Phillip Singerman. *Progress Toward Practical Areas of Quantum Technology*. Washington, DC: Center for Strategic and International Studies, 2025.
- Tomoshige, Hideki, and Phillip Singerman. *Quantum Sensing and the Future of Warfare: Five Essential Reforms to Stay Competitive*. Washington, DC: Center for Strategic and International Studies, 2025.
- Townsend, Brad. "Strategic Choice and the Orbital Security Dilemma." *Strategic Studies Quarterly* 14, no. 1 (Spring 2020): 64–90. <https://www.jstor.org/stable/26891884>
- U.S. Department of Defense. *Report to Congress on Military and Security Developments Involving the People's Republic of China 2025*. Washington, DC: U.S. Department of Defense, 2025.
- Valeriano, Brandon, and Benjamin Jensen. "De-escalation Pathways and Disruptive Technology: Cyber Operations as Off-Ramps to War." In *Cyber Peace: Charting a Path Toward a Sustainable, Stable, and Secure Cyberspace*, edited by Scott J. Shackelford, Frédérick Douzet, and Christopher Ankersen, 64–93. Cambridge: Cambridge University Press, 2022. <https://doi.org/10.1017/9781108954341.004>
- Vaynman, Jane, and Tristan A. Volpe. "Dual Use Deception: How Technology Shapes Cooperation in International Relations." *International Organization* 77, no. 3 (Summer 2023): 599–632. <https://doi.org/10.1017/S0020818323000140>
- Wang, Daniel H. "Death of a Doctrine: The End of Classical Deterrence in a Complex Multipolar World." Master's thesis, Missouri State University, 2025.

- Wang, Shangkun, and Chunle Ni. "Comparative Analysis of Quantum Technology Policies in the United States and China: Strategic Directions and Philosophical Foundations." *Quantum Reports* 8, no. 1 (2026): art. 9. <https://doi.org/10.3390/quantum8010009>
- White House. "Readout of President Joe Biden's Meeting with President Xi Jinping of the People's Republic of China." November 15, 2023. <https://bidenwhitehouse.archives.gov/briefing-room/statements-releases/2023/11/15/readout-of-president-joe-bidens-meeting-with-president-xi-jinping-of-the-peoples-republic-of-china-2/>.
- Wivel, Anders. "Security Dilemma." In *International Encyclopedia of Political Science*, edited by Bertrand Badie, Dirk Berg-Schlosser, and Leonardo Morlino, 2389–91. Thousand Oaks, CA: Sage Publications, 2011. <https://doi.org/10.4135/9781412959636.n549>
- Wuthnow, Joel. *System Overload: Can China's Military Be Distracted in a War over Taiwan?* China Strategic Perspectives, no. 15. Washington, DC: National Defense University Press, 2020.
- Xi Jinping. "Secure a Decisive Victory in Building a Moderately Prosperous Society in All Respects and Strive for the Great Success of Socialism with Chinese Characteristics for a New Era." Report delivered at the 19th National Congress of the Communist Party of China, October 18, 2017. Xinhua, November 3, 2017. http://www.xinhuanet.com/english/special/2017-11/03/c_136725942.htm.
- Yatsuzuka, Masaaki. "PLA's Intelligitized Warfare: The Politics on China's Military Strategy." *Security & Strategy* 2 (January 2022): 17–36. <https://doi.org/10.1080/13439006.2022.2050546>

ABOUT THE AUTHOR

Alyssa I. Agard is Chairman, President, and CEO of Agard Research Associates Inc. (ARA), a 501(c)(3) nonprofit research institute and think tank based in New Jersey focused on interdisciplinary research, policy analysis, and educational programming in the humanities, social sciences, and defense policy. She is a Master of Public Policy candidate at Rutgers University with a concentration in Foreign Affairs and Defense Policy. Her research interests center on the intersection of military history, strategic studies, civil-military relations, and defense policy, with particular emphasis on Chinese military modernization, intelligitized warfare, and the technological dimensions of great power competition.

DISCLAIMER

The views expressed in this article are those of the author and do not necessarily reflect the official position of Agard Research Associates Inc.

PREPRINT NOTICE

This article is a preprint and has not yet undergone peer review. A revised version has been submitted for publication.

CONTACT

aagard@agardassociates.org or www.agardresearchassociates.org

LICENSE

The Intelligitized Security Dilemma: Systems Destruction Warfare, Technological Entanglement, and the Erosion of Strategic Stability © 2026 by Alyssa I. Agard is licensed under CC BY-NC-ND 4.0. To view a copy of this license, visit <https://creativecommons.org/licenses/by-nc-nd/4.0/>