SOCIAL PRISM

Volume 3(7), 2026, 45-69
Online ISSN: 3006-8886
Print ISSN: 3006-8878

Emerging Military Technologies and Strategic Stability in the Indo-Pacific: A Policy Analysis of U.S.–China Strategic Rivalry

Shahar Bano[1], Aijaz Ahmed Shaikh[2]

[1]*M.S Scholar, Institute of International Relations and Peace Studies, Shah Abdul Latif University, Khairpur Mirs, Email: shaharbanosoomro7@gmail.com*
[2]*Assistant Professor, Institute of International Relations and Peace Studies, Shah Abdul Latif University, Khairpur Mirs, Email: aijazshaikh@salu.edu.pk*

Abstract

The accelerating competition between the United States and China in emerging military technologies including artificial intelligence-enabled decision-making, autonomous and unmanned systems, hypersonic delivery vehicles, offensive cyber capabilities, and counter-space systems, is altering the operational and perceptual conditions that underpin strategic stability in the Indo-Pacific. This article undertakes a qualitative, problem-oriented policy analysis, informed by Strategic Stability Theory (SST), of the pathways through which these technologies affect crisis stability, arms-race stability, and deterrence stability in the U.S.–China relationship. Drawing on a verified, tiered evidence base of U.S. and Chinese official documents including annual DoD reports on Chinese military and security developments, DoD strategy summaries, China's white papers on national defense and arms control, and official Chinese and multilateral submissions on military applications of artificial intelligence, together with independent research institutions and the peer-reviewed strategic-stability literature, the analysis finds that emerging technologies compress decision timelines, deepen conventional-nuclear entanglement, increase the vulnerability of nuclear command-and-control (NC2) infrastructure, and generate technological uncertainty that existing bilateral and multilateral governance mechanisms have not kept pace with. These effects are shown to derive substantially from reciprocal, security-seeking behavior on both sides rather than from the unilateral conduct of either power. The article identifies the resulting governance gap as the central policy problem, develops and systematically evaluates three categories of policy response, a bilateral technology incidents protocol, domain-specific confidence-building measures, and multilateral/Track-1.5 governance engagement, against explicit criteria of effectiveness, feasibility, urgency, implementation difficulty, and escalation sensitivity, and proposes an implementation framework specifying responsible actors, mechanisms, and time horizons. The article concludes that reducing the probability of inadvertent or uncontrolled escalation requires deliberate, reciprocal investment in technology-specific crisis-management and confidence-building architecture, rather than the elimination of underlying strategic competition, which lies beyond the scope of feasible near-term policy.

Keywords: Artificial Intelligence, Conventional-Nuclear Engagement, Crisis Management, Emerging Military Technologies, Governance Gap, Hypersonic Weapons, Policy Analysis, Strategic Stability

Received 12 July 2026; Revised 20 August 2026; Accepted 26 August 2026; Published (online) 04 September 2026

Corresponding Author Email: shaharbanosoomro7@gmail.com
DOI: https://doi.org/10.69671/socialprism.3.7.2026.215

Online ISSN: 3006-8886
Print ISSN: 3006-8878

Introduction

Background

The Indo-Pacific strategic environment is undergoing a technology-driven transformation of the operational and perceptual conditions within which deterrence and crisis management must function. Artificial intelligence-enabled targeting systems, hypersonic glide vehicles capable of sustained maneuvering flight at Mach 5 and above, systems that blend conventional and nuclear delivery functions, offensive cyber operations with potential effects on nuclear command-and-control infrastructure, and counter-space capabilities are being developed and, in several domains, operationally fielded by both the United States and China (U.S. Department of Defense [DoD], 2025). Both governments have identified technological advantage as a central pillar of national security. Technology has been a key component of national security for both governments. DoD's annual reports to Congress highlight continued U.S. investment in autonomous, hypersonic, and space capabilities against China (DoD, 2024a, 2025), and China's defense white paper and military-civil fusion strategy emphasize the "intelligentization" of warfare as a key component of the competition with the United States (State Council Information Office of the People's Republic of China [SCIO], 2019).

These developments are important for strategic stability, not so much because they introduce new weapons into current arsenals, but because they change the temporal, operational and perceptual conditions on which classical deterrence theory, developed during the relatively slow-paced nuclear competition of the Cold War, relies. The compressed decision timelines, unclear dual-use signatures, and the increasing complexity of conventional and nuclear systems alter the nature of how crises might unfold and how each side would likely interpret the other's actions in the event of a crisis (Horowitz, 2019; Geist & Lohn, 2018; Acton, 2018a).

Research Problem

The central problem this article addresses is not simply that emerging military technologies are dangerous, but that the bilateral and multilateral institutions historically responsible for managing U.S.–China strategic stability, arms control, and crisis communication were designed for an earlier technological and political environment and have not adapted to the speed, ambiguity, and cross-domain effects these technologies introduce. The absence of any bilateral understanding governing cyber operations against NC2-adjacent infrastructure, and the absence of a binding international agreement constraining lethal autonomous weapons, together indicate a widening gap between the pace of technological change and the institutional capacity to manage its consequences. This governance gap, rather than the technologies themselves or the intentions of either government, constitutes the policy problem this article analyzes.

Research Question

How do emerging military technologies affect strategic stability in the U.S.–China relationship in the Indo-Pacific, and what policy measures could realistically reduce technology-driven escalation risks?

Online ISSN: 3006-8886
Print ISSN: 3006-8878

Research Objectives

To analyze how emerging military technologies, affect strategic stability in the U.S.–China relationship in the Indo-Pacific, and to evaluate feasible policy measures for reducing technology-driven escalation risks.

Significance of the Study

The study contributes to several bodies of scholarship and policy debate. Theoretically, it extends classical Strategic Stability Theory (Jervis, 1989; Schelling, 1966) to a multi-domain technological environment by identifying how compounding technological uncertainty interacts with, rather than sits apart from, each of SST's three classical dimensions. Empirically, it consolidates recent, source-verified official and institutional data on emerging military technology developments relevant to the Indo-Pacific. For the U.S.–China strategic competition literature, it offers a symmetrical framework for analyzing how each side's capabilities and doctrine are likely to be perceived by the other. For policy and governance debates, it provides a systematically evaluated set of near-term measures rather than a general call for risk reduction.

Scope

The analysis focuses on the U.S.–China strategic rivalry in the Indo-Pacific and on the subset of emerging military technologies with demonstrated, well-documented implications for crisis, arms-race, or deterrence stability: artificial intelligence, autonomous and unmanned systems, hypersonic delivery systems, conventional-nuclear entanglement, cyber operations affecting NC2 infrastructure, and space and counter-space capabilities. Technologies whose military strategic-stability effects remain speculative or too early-stage to support a documented risk pathway, most notably cryptographically relevant quantum computing and the broader semiconductor competition that enables several of the technologies above are deliberately excluded from the core analysis in Section 4, though export controls on advanced computing hardware are noted briefly in Section 4.1 where they bear directly on the AI competition analyzed there. These exclusions are acknowledged as important adjacent issues but are not treated as independent strategic-stability domains here, because the available evidence does not yet support the same kind of documented risk-pathway analysis applied to the six technologies retained. The article does not attempt a comprehensive survey of all military applications of the included technologies.

Research Methodology and Policy Analysis Approach

Research Approach

This article is a qualitative, evidence-based, problem-oriented policy analysis based on Strategic Stability Theory. The above elements are different and should not be confused. The research and analytical method used here is policy analysis, which organizes the inquiry into a sequence of steps that includes defining a policy problem, generating policy options, and systematically assessing policy options against explicit criteria to produce actionable and feasible recommendations (Bardach & Patashnik, 2020; Weimer & Vining, 2017). The theory used in that approach, however, is Strategic Stability Theory, which provides the categories of analysis under which the strategic impact of new military technologies can be evaluated, such as crisis stability, arms-race

Online ISSN: 3006-8886
Print ISSN: 3006-8878

stability, and deterrence stability (Jervis, 1989; Schelling, 1966). The theory identifies and explains emerging risks; the policy-analysis approach structures that response to them.

Data and Sources

The analysis relies on a documentary evidence base organized into three tiers, consistent with standard practice in qualitative security-studies policy analysis (Bardach & Patashnik, 2020).

Tier 1: Primary Official sources comprises U.S. government documents (the DoD's annual reports to Congress on Chinese military and security developments, the DoD's *Defense Space Strategy Summary*, the DoD's *2023 Cyber Strategy Summary*, the White House's *America's AI Action Plan*, the successive DoD announcements and memoranda establishing the Replicator initiative, and Admiral Samuel Paparo's 2025 posture statement to the House Armed Services Committee as commander of U.S. Indo-Pacific Command) and Chinese and multilateral government documents (the State Council Information Office's defense and arms-control white papers, the State Council's *New Generation Artificial Intelligence Development Plan* and 2026 statements on emerging industries, China's Ministry of Foreign Affairs position paper on outer space, and China's and the UN's own submissions on military applications of artificial intelligence and lethal autonomous weapons). These establish what each government officially states about its own intentions and priorities; they are treated as authoritative evidence of declaratory policy and programmatic fact, not as objective evidence that either government's interpretation of the strategic situation is correct.

Tier 2: Strategic and Institutional sources comprises reports from RAND, the Carnegie Endowment, CSIS, the Secure World Foundation, NATO Allied Command Transformation, the Congressional Research Service, the Congressional Budget Office, and CISA, used primarily for interpretation and cross-checking of official claims rather than as primary evidence of capability.

Tier 3: Peer-reviewed Academic literature supplies the theoretical apparatus of Strategic Stability Theory, deterrence, and the security dilemma. A fourth category of multilateral and regional documents (UN, ASEAN, and Outer Space Treaty materials) situates the bilateral relationship within its broader institutional context.

Analytical Procedure

The analysis proceeds through eight sequential steps: (1) identification of the major emerging military technologies relevant to U.S.–China strategic stability in the Indo-Pacific; (2) identification of their potential strategic effects; (3) assessment of these effects using the SST framework developed in Section 3; (4) identification of governance and institutional gaps relevant to each technology; (5) definition of the resulting policy problem; (6) identification of potential policy options; (7) evaluation of these options against explicit criteria; and (8) formulation of policy recommendations and an implementation framework. This sequence ensures that policy recommendations are derived from, and traceable to, the preceding empirical and theoretical analysis rather than introduced independently of it.

Policy Evaluation Criteria

The policy options outlined in Section 7 are assessed in Section 8 against five clear criteria. Effectiveness questions whether the measure would likely decrease the strategic-stability threat it is

Online ISSN: 3006-8886
Print ISSN: 3006-8878

meant to address. Political feasibility examines whether the measure is feasible in the U.S. and China as a result of domestic and bilateral political conditions. Urgency is asking the question of how fast the underlying risk needs to be acted on. Implementation difficulty is a question of the institutional, technical or verification requirements of the measure. Escalation sensitivity questions whether the measure itself might engender new mistrust, whether it might be seen as one-sided, or whether it might be seen as an escalation risk apart from the problem it is intended to address. These criteria are not numerically scored, but rather applied qualitatively based on the preceding analysis, which is partly qualitative. The uncertainty of the evidence on which it is based does not support.

Limitations

Several limitations are common to the qualitative policy analysis of contemporary security issues, and apply to this analysis. First, it relies on publicly available information; classified military capabilities and internal deliberations on both sides are not directly observable, and open-source assessments including official ones, may be incomplete or reflect institutional incentives. Second, the details of a capability can change between analysis and publication due to the pace of technological change. Third, strategic perceptions and threat assessments on both sides are not directly measured, but rather inferred from doctrine, statements, and actions, and the analysis does not fully confirm how the other side's planners interpret the capabilities of the other side in specific scenarios. Fourth, the use of qualitative criteria like “feasibility” or “effectiveness” in the process of policy evaluation always requires some analytical judgment that quantitative methods would not remove, but would manifest differently. Fifth, as mentioned in Section 2.2, several items that were initially thought to be topically relevant were not matched to a verifiable, precisely dateable publication and were therefore corrected or dropped, and not cited on an approximate basis; this reduces the number of secondary interpretive material incorporated, not the reliability of what is cited. Sixth, and as noted in Section 1.6, the article deliberately excludes technologies such as quantum computing and the broader semiconductor competition among them whose strategic-stability effects are plausible but not yet documented with the same specificity as the six domains retained. These limitations counsel appropriate caution in the confidence attached to specific findings and recommendations, without undermining the value of a systematic qualitative assessment of publicly available evidence.

Theoretical Framework: Strategic Stability Theory

Classical Strategic Stability Theory

Strategic Stability Theory (SST), in its classical Cold War formulation, identifies three analytically distinct but interacting dimensions of stability (Jervis, 1989; Schelling, 1966). Crisis stability refers to the absence of incentives for either party to strike first during a crisis; it is degraded when either side perceives an advantage in preemption. Arms-race stability refers to the absence of incentives to expand or qualitatively improve forces in response to the other side’s developments; it is degraded by action-reaction dynamics in which each side’s investments are read by the other as requiring a compensatory response. Deterrence stability refers to the maintenance of credible second-strike capability sufficient to make retaliation assured, removing any incentive to strike first out of fear of losing the ability to retaliate at all. These dimensions interact: a decline

Online ISSN: 3006-8886
Print ISSN: 3006-8878

in crisis stability creates incentives to expand or harden forces, producing arms-race instability, which in turn can generate new first-strike incentives in a reinforcing cycle.

Emerging Technologies and Strategic Stability

Emerging military technologies bear on each of these three dimensions, generally simultaneously, though the specific mechanism differs by technology and is analyzed in detail in Section 4. Technologies that compress the time available for human deliberation during a crisis such as AI-enabled targeting or hypersonic delivery bear on crisis stability. Technologies that are dual-use, or whose development by one side plausibly compels compensatory investment by the other, bear on arms-race stability. Technologies that threaten the survivability of second-strike forces or of the command-and-control infrastructure needed to employ them whether through precision-strike, cyber, or counter-space means, bear on deterrence stability.

Compounding Technological Uncertainty

Across the technologies examined in Section 4, a recurring pattern emerges that this article treats as an important refinement to the classical framework rather than a fourth independent dimension: the pace and opacity of simultaneous multi-domain technological change generates a form of compounding uncertainty that degrades all three classical dimensions at once rather than acting through any single one of them. Because both the United States and China are developing capabilities across artificial intelligence, autonomy, hypersonic, cyber, and space simultaneously, and because each side's programs are only partially observable to the other, neither side can reach a confident assessment of relative capability or of the survivability of its own second-strike forces, the specific dynamic that Levite et al. (2021) document in detail for the U.S.–China cyber-nuclear command, control, and communications relationship. This uncertainty manifests through unresolved questions about relative capability, second-strike survivability, warning time, the integrity of command-and-control systems, attribution of ambiguous incidents, and the location of escalation thresholds that neither side has clearly signaled to the other.

Analytical Framework

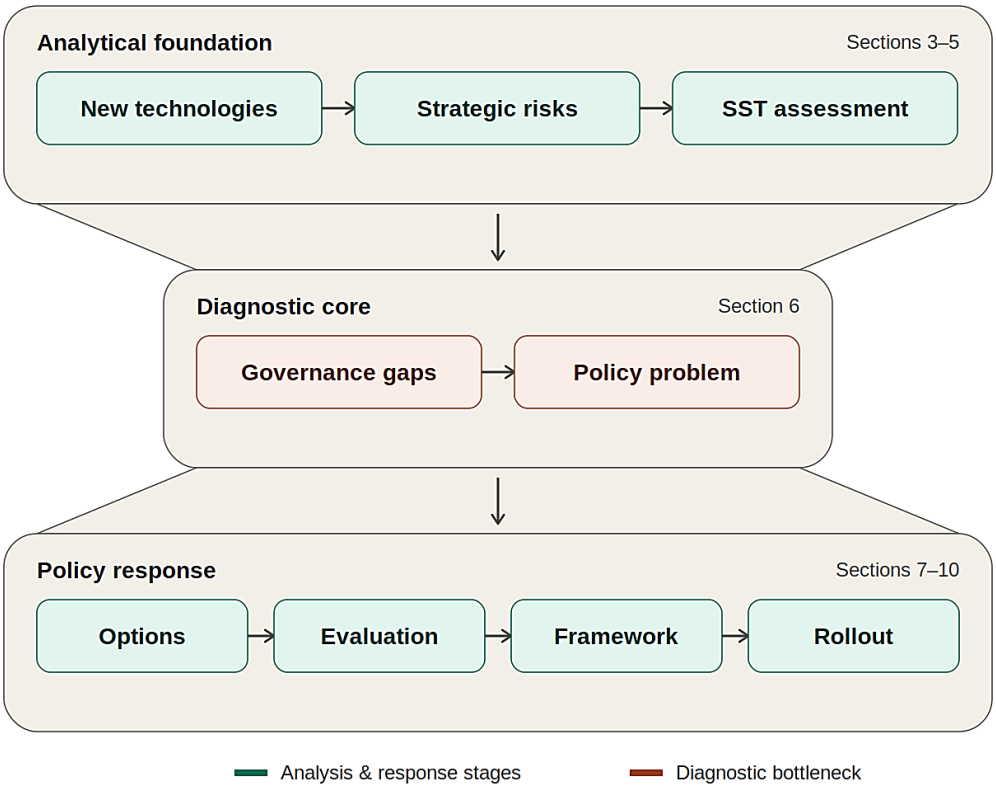
The article adopts the following analytical chain to structure the technology-specific analysis in Section 4 and the subsequent policy analysis:

Technology → Stability Mechanism → SST Dimension → Governance Problem → Policy Response.

For each technology examined, the analysis identifies the mechanism through which it affects strategic stability, the SST dimension(s) engaged, the existing governance arrangement (if any) meant to address the resulting risk, and the type of policy response the analysis of that gap implies. This chain provides the connective structure between the empirical, theoretical, and policy-analytic components of the article.

SOCIAL PRISM
Online ISSN: 3006-8886
Print ISSN: 3006-8878

Figure 1: Policy Analysis Model: From Emerging Military Technologies to Implementation



Source: Author's Own

Policy analysis model figure showing analytical foundation narrowing to a diagnostic core and then broadening into policy response

The figure depicts the analytical chain that structures this article: an analytical foundation (technologies, technology-driven risks, and the Strategic Stability Theory assessment; Sections 3–5) that narrows into a diagnostic core (governance and institutional gaps and policy problem definition; Section 6), which in turn broadens into policy response (options, evaluation, framework, and implementation; Sections 7–10).

Emerging Military Technologies and Strategic Stability

Each technology domain examined below is analyzed using a common six-part structure: (A) the technological development itself and how the United States and China are developing or employing it; (B) the strategic-stability mechanism through which it operates; (C) a specific risk pathway that could lead to escalation; (D) how each side is likely to perceive the other's related capabilities; (E) the governance gap relevant to the technology; and (F) the type of policy response its analysis implies. Consistent with the source hierarchy set out in Section 2.2, the technological-development component of each subsection draws principally on Tier 1 official U.S. and

Online ISSN: 3006-8886
Print ISSN: 3006-8878

Chinese documents, so that the article establishes what each government itself states about its programs before turning to independent interpretation of their strategic-stability implications.

Artificial Intelligence

A. Technological Development: Both governments have designated artificial intelligence a priority military and national technology. The White House's *America's AI Action Plan* frames AI leadership and computing infrastructure as central to U.S. strategic competitiveness (White House, 2025). On the Chinese side, the State Council's *New Generation Artificial Intelligence Development Plan* set 2030 as the target date for China to become a world leader in AI theory, technology, and application (State Council of the People's Republic of China, 2017), and China's 2019 defense white paper frames "informatized" and increasingly intelligent warfare as a central direction of PLA modernization (SCIO, 2019); China's March 2026 statements on nurturing emerging and future industries and its 2026 government work report both reaffirm AI and advanced computing as national priorities notwithstanding external pressure (State Council of the People's Republic of China, 2026a, 2026b). That external pressure includes a series of 2025 U.S. Bureau of Industry and Security actions tightening restrictions on advanced computing semiconductors and associated foundry due-diligence and anti-diversion requirements aimed at limiting China's access to the computing hardware that underwrites large-scale AI development (Bureau of Industry and Security [BIS], 2025a, 2025b). AI functions less as a discrete weapon system than as an enabling technology that increases the speed, scale, and reach of the other capabilities examined in this section, which is why the underlying computing competition is noted here despite falling outside this article's core scope, as explained.

B. Strategic Stability Mechanism: AI-driven processing reduces the "kill chain" from hours to minutes or seconds from detection to decision to strike, and thus the time available for human decision makers to intervene (Horowitz, 2019). It is mainly a crisis-stability mechanism, but also on arms-race stability as the other side's AI investment is read as a call for a counter-response.

C. Risk Pathway: Geist and Lohn (2018) outline two related ways in which AI could exacerbate nuclear risk: AI decision-support systems could provide decision makers with pre-formulated recommendations in a crisis situation under time pressure, which may not encourage independent verification; AI sensor fusion or deception, such as spoofed data or degraded sensor inputs, could create false warning signals that existing crisis-communication protocols were not designed to handle.

D. U.S.–China Interaction: China's 2018 position paper on regulating military uses of AI, presented under the auspices of the UN Convention on Certain Conventional Weapons, emphasizes the need to ensure that humans retain control over the use of force, and cautions against the use of AI in nuclear command, control, and early-warning systems in particular (United Nations, 2018). China's perspective on artificial intelligence in the military field is included in a 2025 UN General Assembly report that brings together member-state views on the technology's potential to create common threats to international peace and security, which should continue to be a focus of multilateral engagement (United Nations, 2025a). The two governments' declaratory positions on human control are therefore substantially convergent at the level of principle; the more consequential divergence lies in the absence of any bilateral mechanism through which either side could verify the other's compliance with its own stated standard.

Online ISSN: 3006-8886
Print ISSN: 3006-8878

E. Governance Gap: The CCW process that has hosted China's and other states' position papers on military AI since 2018 has not produced a binding agreement (United Nations, 2018, 2025a), and no bilateral U.S.–China understanding translates the two sides' parallel declaratory positions on human control into a verifiable standard for nuclear-adjacent AI applications specifically.

F. Policy Implication: Because both governments own declaratory positions already endorse human control in principle, a narrower bilateral instrument that operationalizes this shared premise for nuclear-adjacent applications, rather than a comprehensive AI arms-control treaty, is the more immediately feasible governance response, addressed in the study.

Autonomous and Unmanned Systems

A. Technological Development: Beyond AI as a decision-making layer, both states are fielding large numbers of physical autonomous and unmanned platforms. The DoD's Replicator initiative directs the rapid fielding of low-cost, attritable autonomous systems across the air and maritime domains, explicitly framed as a response to the scale of the PLA's mass military advantage (DoD, 2024b), with subsequent announcements extending the initiative to additional all-domain attritable autonomous capabilities (DoD, 2024c) and a formal direction-and-execution memorandum establishing a second tranche of the program (DoD, 2024d). Admiral Paparo's 2025 posture statement to the House Armed Services Committee, as commander of U.S. Indo-Pacific Command, identifies attritable autonomous systems as central to the command's operational concept for Indo-Pacific deterrence (Paparo, 2025). On the Chinese side, the DoD's 2025 assessment documents extensive PLA investment in unmanned aerial, surface, and subsurface systems (DoD, 2025).

B. Strategic Stability Mechanism: Mass-produced autonomous platforms affect arms-race stability most directly, since the low unit cost and rapid production timelines both sides describe as advantages of these programs lower the threshold for large-scale acquisition and invite reciprocal buildup (DoD, 2024b; DoD, 2025). Swarming and human-machine teaming concepts also bear on crisis stability where they are integrated into strike or reconnaissance functions that shorten decision timelines, overlapping with the mechanism discussed.

C. Risk Pathway: A dense concentration of low-cost autonomous platforms on both sides of a contested space such as the Taiwan Strait or the South China Sea increases the number of potential incidents involving ambiguous or unauthorized behavior, any one of which could be interpreted as a deliberate probe rather than a system malfunction or navigational error, particularly where swarm coordination logic is not fully transparent even to its operators. This risk is not confined to the U.S.–China dyad: comparative analysis of a 2025 nuclear-armed-state crisis found that the introduction of large-scale drone warfare between rivals generated new categories of ambiguous, hard-to-attribute incidents that existing crisis-management arrangements were not designed to handle (Basit et al., 2025).

D. U.S.–China Interaction: The Replicator initiative is presented in U.S. official communications as restoring conventional deterrence through mass and attritability rather than through any single exquisite platform (DoD, 2024b), a framing directly analogous to China's own emphasis on intelligent and unmanned systems as a means of offsetting adversary advantages in precision and quality (DoD, 2025). Each side's program is described domestically in terms of restoring de-

Online ISSN: 3006-8886
Print ISSN: 3006-8878

terrence, while the other side has reason to read the resulting proliferation of autonomous platforms as expanding the other's operational reach.

E. Governance Gap: Neither the CCW process nor any bilateral channel currently addresses autonomous-system incident notification, identification standards, or de-confliction procedures specific to unmanned platforms operating in contested waters or airspace, despite the rapid increase in the number of such platforms fielded by both sides.

F. Policy Implication: A dedicated unmanned-systems incident and identification protocol, distinct from but coordinated with the AI human-control measures discussed in Section 4.1, is the governance response most directly indicated by this gap.

Hypersonic Delivery Systems

A. Technological Development: Hypersonic weapons, systems capable of sustained maneuvering flight at Mach 5 or above, combine speed that curtails warning time with maneuverability that complicates existing missile-defense architectures. The Congressional Research Service's background report on hypersonic weapons documents continued Chinese and U.S. development of hypersonic glide vehicles and boost-glide systems, including systems fielded by China's PLA Rocket Force in both conventional and dual-capable configurations (Congressional Research Service [CRS], 2024). The DoD's 2025 assessment documents continued PLA Rocket Force integration of these systems (DoD, 2025), and the United States continues to field and develop its own hypersonic strike programs across the Army and Navy (CRS, 2024).

B. Strategic Stability Mechanism: Hypersonic systems compress warning time potentially to well under the roughly thirty minutes associated with traditional ballistic missile trajectories, bearing on crisis stability, while their existence in both conventional and nuclear-capable configurations without reliable external differentiation bears on deterrence stability (Speier et al., 2017).

C. Risk Pathway: The Congressional Budget Office's assessment of U.S. and Chinese hypersonic weapons notes that several hypersonic configurations are not reliably distinguishable from nuclear-capable variants by an adversary's sensors at the moment of launch (Congressional Budget Office [CBO], 2023). In a compressed-timeline crisis, a hypersonic strike intended by the launching side as conventional could be assessed by the receiving side's nuclear planners as the initial phase of a broader attack, creating pressure toward preemptive action before conventional intent could be communicated (Acton, 2018a; Talmadge, 2017).

D. U.S.–China Interaction: Both sides' hypersonic programs are described in official and institutional sources primarily in terms of restoring or maintaining conventional deterrent capability relative to the other's air and missile defenses (DoD, 2025; CBO, 2023). Each side's hypersonic investment, whatever its declared conventional purpose, is likely read by the other as evidence of an evolving strike capability requiring its own compensatory response, an action-reaction dynamic characteristic of arms-race instability rather than evidence of unilateral escalatory intent by either side.

Online ISSN: 3006-8886
Print ISSN: 3006-8878

E. Governance Gap: No U.S.–China arrangement exists for pre-launch notification of hypersonic tests or for communicating intended target category during a crisis, notwithstanding the missile-related notification issues surveyed in the CRS background report (CRS, 2024).

F. Policy Implication. A notification-based confidence-building measure and a dedicated incidents-communication channel are the governance responses most directly indicated by this gap.

Conventional-Nuclear Entanglement

A. Technological Development: Conventional-nuclear entanglement refers to conditions in which conventional operations threaten nuclear command-and-control infrastructure, or in which nuclear and conventional delivery systems are co-deployed such that they cannot be reliably discriminated (Acton, 2018a, 2018b). The DoD's 2025 assessment identifies China's DF-26 intermediate-range ballistic missile as deployed in both nuclear and conventional-armed configurations within the same PLA Rocket Force units, without reliable means for external observers to distinguish the two at the time of a targeting decision (DoD, 2025).

B. Strategic Stability Mechanism: Entanglement bears on all three SST dimensions: it degrades crisis stability by creating first-strike-relevant ambiguity, contributes to arms-race instability through reciprocal deployments, and threatens deterrence stability insofar as conventional strikes against co-deployed systems risk destroying nuclear assets or severing command authority (Acton, 2018a).

C. Risk Pathway: Acton (2018b) describes how a conventional strike against dual-capable missile batteries during a regional conflict, a militarily rational targeting choice from a purely conventional standpoint, could inadvertently destroy nuclear warheads or degrade nuclear command links, generating an assessment on the targeted side that a disarming first strike was underway. This risk runs in both directions: comparable discrimination problems would arise for Chinese action against any U.S. or allied system capable of both conventional and nuclear-configured munitions.

D. U.S.–China Interaction: Entangled dual-capable systems are, on both sides, presented domestically as restoring conventional deterrent capability rather than as nuclear signaling (DoD, 2025). This dynamic is consistent with security-dilemma analysis, in which each side's rational security-seeking behavior such as expanding forces to address its own perceived vulnerabilities, intensifies the other's threat perceptions regardless of either side's actual intentions (Jervis, 1989).

E. Governance Gap: No bilateral understanding exists distinguishing nuclear from conventional variants of dual-capable systems for crisis-communication purposes, and no agreed protocol exists for communicating the conventional intent of actions that the other side's sensors might assess as nuclear-relevant (Acton, 2018b, 2020).

F. Policy Implication: Geographic or functional "exclusion" understandings around nuclear command facilities, combined with an incidents-communication channel capable of conveying conventional intent in real time, are the governance responses most directly indicated.

Online ISSN: 3006-8886
Print ISSN: 3006-8878

Cyber Operations and Nuclear Command-and-Control

A. Technological Development: CISA's Volt Typhoon advisory documents persistent access by China-linked state-sponsored actors within U.S. critical infrastructure systems, including power distribution, water treatment, and communications networks, which CISA assesses as pre-positioning oriented toward disrupting military logistics and civilian support infrastructure in a potential future contingency (CISA, 2024). China's 2025 white paper on arms control, disarmament, and nonproliferation identifies the protection of critical information infrastructure as a national-security priority in its own terms (SCIO, 2025). The DoD's 2023 Cyber Strategy Summary identifies critical-infrastructure defense and resilience as a core U.S. cyber priority (DoD, 2023), and the United States conducts offensive cyber operations as an established element of its own military doctrine, although comparably detailed open-source documentation of specific U.S. operations against Chinese infrastructure is not publicly available to the same extent.

B. Strategic Stability Mechanism: Where cyber operations have plausible effects on infrastructure adjacent to nuclear command, control, and communications (C3) systems, they bear directly on deterrence stability, since the perceived vulnerability of NC2 systems can create incentives toward early or more dispersed nuclear postures on the affected side (Acton, 2020).

C. Risk Pathway: Levite et al. (2021), in a joint U.S.–Chinese expert assessment of cyber-nuclear C3 stability, identify the absence of any bilateral governance framework for cyber operations against NC2-adjacent infrastructure as a significant unmanaged risk: a domain in which both sides possess offensive capability, neither has articulated clear red lines, and miscalculation could plausibly intersect with nuclear-relevant systems regardless of which side's operations are involved in a given incident.

D. U.S.–China Interaction: Chinese officials have not publicly acknowledged the Volt Typhoon operations as described in U.S. assessments, and the United States has not published a comparably detailed account of its own offensive cyber posture toward Chinese infrastructure. This asymmetry in public documentation should be read as a limitation of available open-source evidence rather than as evidence that only one side conducts such operations; both governments maintain substantial offensive cyber capabilities as a matter of declared doctrine and both identify critical-infrastructure protection as a national-security priority in their own terms (DoD, 2023; SCIO, 2025).

E. Governance Gap: The 2015 U.S.–China cyber agreement explicitly excluded military cyber operations and established no NC2-protection framework, and no successor arrangement has since been concluded (White House, 2015; CISA, 2024; Levite et al., 2021).

F. Policy Implication: A mutual, reciprocal non-interference understanding specific to NC2-adjacent infrastructure, with an associated notification mechanism for inadvertent effects, is the governance response most directly indicated.

Space and Counter-Space Capabilities

A. Technological Development: CSIS's Space Threat Assessment 2024 documents Chinese co-orbital satellite inspection capabilities, directed-energy dazzling of optical satellites, and ground-based anti-satellite capability at low-earth-orbit altitudes, alongside continued U.S. and allied

Online ISSN: 3006-8886
Print ISSN: 3006-8878

counter-space development (Harrison et al., 2024). The Secure World Foundation's open-source assessment of global counter-space capabilities corroborates the broad contours of this multi-domain buildup (Secure World Foundation, 2024). The DoD's Defense Space Strategy Summary identifies resilient space architecture and space-domain awareness as priority U.S. investment areas for sustaining the early-warning and command functions central to U.S. nuclear posture (DoD, 2020). China's arms-control position paper on outer space reiterates its long-standing support for negotiating an international instrument to prevent an arms race in space (Ministry of Foreign Affairs of the People's Republic of China [MFA PRC], 2022).

B. Strategic Stability Mechanism: Degradation of early-warning satellites bears on crisis stability; it could generate an assessment on the affected side that a nuclear attack is imminent, triggering heightened alert or launch-on-warning postures that neither side may have intended to provoke.

C. Risk Pathway: If either side's early-warning satellites were degraded or destroyed during the opening phase of a conventional conflict, whether deliberately, for conventional military purposes, or inadvertently the affected side could reasonably interpret this as preparation for a nuclear first strike, given the role such satellites play in that side's own nuclear early-warning architecture (Harrison et al., 2024).

D. U.S.–China Interaction: China's declaratory support for a prevention-of-an-arms-race-in-outer-space instrument sits alongside continued Chinese counter-space capability development documented by independent observers (Harrison et al., 2024; Secure World Foundation, 2024), a gap between declaratory and observed posture that is not unique to China, the United States has likewise continued to develop its own space and counter-space capabilities while not offering China a reciprocal bilateral transparency arrangement (DoD, 2020). Both patterns are consistent with the general finding, developed further in Section 6, that declaratory positions on restraint have generally outpaced the bilateral instruments that would make restraint verifiable.

E. Governance Gap: The 1967 Outer Space Treaty establishes general principles for the peaceful use of outer space but does not address incident notification, identification, or de-confliction procedures for the counter-space capabilities documented above (United Nations Office for Outer Space Affairs, 1967), and no bilateral U.S.–China mechanism fills this specific gap.

F. Policy Implication: A dedicated space-incidents notification channel, paralleling the hypersonic and cyber measures discussed above, is the governance response most directly indicated.

Comparative Strategic Stability Assessment

The technology-specific analysis in Section 4 shows that risks are not uniform in nature and severity across the domains. Conventional-nuclear entanglement and the cyber–NC2 interface involve the widest spectrum of SST dimensions and have the most direct link to unintended nuclear escalation, as they operate on infrastructure and systems most closely linked to nuclear employment decisions. The most critical time constraints for crisis decisions are found in hypersonic systems and AI-driven decision-making. Arms-race stability is the most heavily affected by autonomous and unmanned systems, and the action-reaction dynamics they create ripple through the more intense risks listed above, but do not themselves pose an acute risk. Space and counter-space capabilities produce a relatively focused but intense threat to early-warning systems. This

Online ISSN: 3006-8886
Print ISSN: 3006-8878

ordering is not intended to imply that any one technology or actor is more "responsible" for instability than any other, but rather that the risk pathway to nuclear command authority and the time available for decision-making are closer to the technology in question.

Table 1: Comparative Strategic Stability Assessment

Technology	Key Risk	SST Dimension	Governance Gap	Policy Priority
Artificial Intelligence	Timeline compression; false-warning pathways	Crisis Stability	No verifiable bilateral human-control standard for nuclear-adjacent use	High
Autonomous / Unmanned Systems	Mass proliferation; ambiguous incidents; reciprocal buildup	Arms-Race Stability	No incident-notification or identification protocol	Moderate-High
Hypersonic Weapons	Warning-time elimination; dual-use launch ambiguity	Crisis + Deterrence Stability	No pre-launch notification or target-category communication	High
Conventional–Nuclear Entanglement	C2 ambiguity; inadvertent disarming assessment	All Three Dimensions	No discrimination or exclusion-zone understanding	Highest
Cyber vs. NC2	NC2-adjacent degradation; unintended posture escalation	Crisis + Deterrence Stability	No NC2 non-interference understanding	Highest
Space / Counter-Space	Early-warning denial; inadvertent posture elevation	Crisis Stability	No incidents-notification mechanism	Moderate-High

Source: Author's Own

Note. NC2 = Nuclear Command and Control; SST = Strategic Stability Theory. Policy priority reflects the proximity of each technology's risk pathway to nuclear command authority and available decision time, based on the analysis in Section 4, and does not represent a numerical or independently validated ranking.

Governance Architecture and Policy Problem

Nuclear Arms-Control and Strategic Stability Gap

The United States has no bilateral nuclear arms-control or strategic-stability dialogue with China comparable to its treaty relationship with Russia, even as the DoD's annual assessments document a substantial and continuing expansion of China's nuclear forces (DoD, 2025). This gap reflects the reluctance of both governments, for differing reasons rooted in their differing force postures and strategic doctrines, to accept the transparency obligations that a formal arms-control relationship would require, rather than the unwillingness of one side alone (Krepon, 2021).

Online ISSN: 3006-8886
Print ISSN: 3006-8878

Cyber Governance Gap

As discussed in Section 4.5, the 2015 U.S.–China cyber agreement excluded military operations and did not establish an NC2-protection framework, and no successor arrangement has since been concluded (White House, 2015; Levite et al., 2021).

Crisis Communication Gap

Existing U.S.–China military-to-military communication channels address conventional incidents generally but have no agreed protocol for communicating the intent of actions that the receiving side's sensors might assess as nuclear-relevant, precisely the ambiguity that hypersonic and entangled conventional-nuclear systems generate (Acton, 2018b, 2020). The broader history of U.S.–China and U.S.–Soviet/Russian arms control shows that such channels are themselves vulnerable to political suspension during periods of tension, precisely when they may be most needed (Krepon, 2021).

Autonomous Weapons and Unmanned-Systems Governance Gap

The CCW process convened to address lethal autonomous weapons systems has not produced a binding agreement, notwithstanding continued multilateral engagement on the issue (United Nations, 2025b), even though both governments own declaratory statements on human control are broadly convergent (United Nations, 2018, 2025a). A related and narrower gap concerns the physical proliferation of unmanned platforms documented in Section 4.2, neither the CCW process nor any bilateral channel currently provides incident-notification or identification procedures for unmanned systems operating in contested Indo-Pacific waters or airspace, notwithstanding the scale at which both governments describe fielding such systems.

Space Governance Gap

No bilateral U.S.–China mechanism exists for notification of incidents affecting early-warning or communications satellites, and the 1967 Outer Space Treaty's general principles do not address this specific gap (United Nations Office for Outer Space Affairs, 1967). China's declaratory support for an international instrument preventing an arms race in outer space has not translated into a bilateral notification arrangement with the United States, and the United States has not proposed one either, leaving this a genuine two-sided gap rather than a one-sided refusal (DoD, 2020; MFA PRC, 2022).

The Stability Infrastructure Gap

Taken together, these governance deficits constitute what this article characterizes as a stability infrastructure gap; a growing divergence between the pace of military-technological change and the institutional capacity on both sides to manage its most consequential effects. This inadequacy does not appear to be primarily a function of technical complexity; nuclear arms-control frameworks were developed and sustained during a period of comparable or greater technical novelty (Krepon, 2021). It instead appears to reflect the reluctance of both governments to accept the degree of transparency that effective governance mechanisms would require of programs each treats as a source of competitive advantage, a reluctance for which each side bears responsibility to a degree that available evidence does not allow this analysis to apportion precisely between them.

Online ISSN: 3006-8886
Print ISSN: 3006-8878

The resulting policy problem may be stated as follows, the pace and cross-domain effects of emerging military technologies are advancing faster than the bilateral and multilateral institutions designed to manage strategic instability between the United States and China. This problem is institutional rather than attributable to either government's unilateral conduct, and it is the problem the policy analysis in Sections 7 through 10 is designed to address.

Policy Options Analysis

This section identifies three categories of policy option responsive to the governance gaps identified in Section 6, prior to their systematic evaluation in Section 8.

Option One: Bilateral Technology Incidents Protocol

Objective: To establish a dedicated communication channel for incidents involving emerging military technologies that existing military-to-military mechanisms do not adequately address.

Mechanism: A Bilateral Technology Incidents Protocol (BTIP) would combine a hypersonic-incidents channel (real-time notification of hypersonic launches, including intended target category), a cyber–NC2 non-interference understanding with associated notification procedures, a space-incidents notification mechanism, and an unmanned-systems incident and identification channel addressing the risk pathway identified in Section 4.2. It would be framed explicitly as safety infrastructure rather than as an instrument of diplomatic leverage, in an effort to insulate it from the kind of political suspension that has affected other bilateral channels during periods of tension (Krepon, 2021).

Advantages: None of its components requires disclosure of classified capability parameters; each establishes a behavioral commitment or communication procedure rather than a technology-transparency obligation, which lowers the political cost of participation for both sides.

Limitations: A framing as "safety infrastructure" does not guarantee insulation from political pressure during an actual crisis, when the channel would be most needed and political incentives to suspend cooperative arrangements may be highest. Verification of compliance with the non-interference and notification components would rely substantially on good-faith reporting.

Political Feasibility: Moderate. Both governments have precedent for maintaining incident-communication channels even amid broader tension, though neither has yet agreed to a technology-specific instrument of this kind.

Implementation Challenges: Requires sustained diplomatic negotiation to define notification thresholds and communication procedures, and institutional commitment to keep the channel operating independent of the broader political relationship.

Likely Responses: U.S. officials have generally supported expanded crisis-communication mechanisms in principle, though implementation would require interagency coordination on notification thresholds that do not reveal sensitive capability information. Chinese officials have historically been cautious about mechanisms perceived as constraining operational flexibility or as a one-sided transparency obligation; framing the BTIP as reciprocal and safety-oriented, rather than as an arms-control instrument, is intended to address this concern, though its acceptance cannot be assumed.

Online ISSN: 3006-8886
Print ISSN: 3006-8878

Option Two: Domain-Specific Confidence-Building Measures

Objective: To reduce structural sources of instability identified in Section 4 through targeted, verifiable confidence-building measures (CBMs) in each domain.

Mechanism: Measures include: pre-launch notification of hypersonic test flights, of the kind surveyed in existing missile-notification literature (CRS, 2024); a joint declaration on human-control standards for lethal autonomous systems in nuclear-adjacent scenarios, building on the convergent declaratory positions documented in Section 4.1 (United Nations, 2018, 2025a); and mutually recognized NC2 exclusion understandings that constrain targeting of facilities each side identifies, without disclosing exact locations or capabilities, as nuclear-command-adjacent.

Advantages: These measures are narrower and more technically bounded than a comprehensive arms-control treaty, and hypersonic pre-launch notification in particular has direct precedent in existing missile-notification frameworks, reducing the novelty of the political commitment required.

Limitations: CBMs of this kind address specific risk pathways but do not resolve the broader strategic competition driving the underlying technological investment; they are risk-reduction measures rather than a substitute for a comprehensive stability architecture.

Political Feasibility: Moderate to High for hypersonic notification, given precedent; Moderate for the human-control declaration and NC2 exclusion understandings, which would require each side to identify constraints on its own operational planning.

Implementation Challenges: Defining verification-light notification protocols that do not reveal classified capability parameters; identifying and mutually recognizing NC2 exclusion zones without requiring disclosure of exact facility locations or capabilities.

Likely Responses: Both governments have generally supported narrowly bounded, reciprocal CBMs in other domains historically, suggesting these measures are more readily achievable than broader binding constraints, though their nuclear-adjacent character introduces sensitivities not present in purely conventional notification arrangements.

Option Three: Multilateral and Track-1.5 Governance

Objective: To develop norms and confidence-building measures through channels less constrained by the current political limits on formal bilateral U.S.–China arms-control negotiation.

Mechanism: This option includes reinvigorating the CCW Group of Governmental Experts process on lethal autonomous weapons with a narrower, U.S.–China co-sponsored mandate focused specifically on nuclear-adjacent applications (United Nations, 2025b); establishing Track-1.5 dialogues involving former officials and academic specialists on AI military applications, hypersonic notification, and the cyber-nuclear interface, of the kind that has already produced joint U.S.–Chinese expert assessment in the cyber-nuclear domain (Levite et al., 2021); and engaging regional institutions and states including Japan, Australia, India, and ASEAN members in advancing normative frameworks for emerging-technology governance.

Online ISSN: 3006-8886
Print ISSN: 3006-8878

Advantages: Multilateral and Track-1.5 channels can develop practical measures on shorter timelines than formal diplomatic processes and build the technical understanding and personal relationships that formal crisis-communication channels depend on when actually used (Krepon, 2021; Levite et al., 2021). Regional institutions such as ASEAN, whose Outlook on the Indo-Pacific emphasizes dialogue over bloc confrontation, may provide a normative framework within which technology-specific CBM proposals can be advanced without triggering the more zero-sum dynamics that have constrained bilateral engagement (Association of Southeast Asian Nations [ASEAN], 2019); NATO's own regional foresight analysis of the Indo-Pacific similarly underscores the value of broader like-minded engagement in shaping the normative environment around emerging military technologies, even where NATO itself is not a direct party to U.S.–China bilateral measures (NATO Allied Command Transformation, 2022).

Limitations: Track-1.5 dialogues and multilateral processes generally lack binding authority and cannot substitute for direct bilateral commitments on the highest-priority risks identified in Section 5, particularly conventional-nuclear entanglement and cyber–NC2 interference. Regional states' interests in this agenda are shaped by their own security concerns and institutional roles rather than automatic alignment with either Washington or Beijing, and their capacity to influence bilateral U.S.–China dynamics directly should not be overstated.

Political Feasibility: High, relative to the other two options, precisely because these channels do not require formal bilateral commitments that either government's domestic politics might not currently sustain.

Implementation Challenges: Translating Track-1.5 or multilateral consensus into measures that affect actual bilateral military behavior; sustaining momentum in the absence of formal governmental endorsement.

Comparative Policy Evaluation

Table 2: Policy Options Evaluation Matrix

Policy Option	Effectiveness	Political Feasibility	Urgency	Implementation Difficulty	Escalation Sensitivity
Bilateral Technology Incidents Protocol	High	Moderate	High	Moderate	Low
Domain-Specific Confidence-Building Measures	Moderate–High	Moderate	High	Moderate–High	Low–Moderate
Multilateral / Track-1.5 Governance	Moderate	High	Moderate	Low–Moderate	Low

Source: Author's Own

The evaluation indicates a characteristic policy trade-off: The Bilateral Technology Incidents Protocol offers the highest expected effectiveness against the most severe risks identified in Section 5, but its political feasibility is only moderate, reflecting the historical difficulty of sustain-

Online ISSN: 3006-8886
Print ISSN: 3006-8878

ing bilateral crisis-communication mechanisms amid broader political tension. Domain-specific CBMs are similarly effective but vary in implementation difficulty depending on the domain, with hypersonic notification the most tractable and NC2 exclusion understandings the most demanding. Multilateral and Track-1.5 governance offers the highest political feasibility and lowest escalation sensitivity but correspondingly lower direct effectiveness against the highest-priority risks, since it operates through non-binding or indirect channels.

This trade-off between effectiveness and feasibility does not indicate that the most effective option should automatically be preferred in isolation. A policy framework that pursues the BTIP alone, without the complementary legitimacy and technical groundwork that Track-1.5 and multilateral engagement can provide, risks political fragility; conversely, a framework that relies solely on multilateral and Track-1.5 channels is unlikely to generate the direct bilateral commitments needed to address the highest-priority risks identified in Section 5. The recommended framework in Section 9 therefore treats the three options as complementary and sequenced rather than as mutually exclusive alternatives.

Recommended Policy Framework

Based on the evaluation in Section 8, this article recommends a three-part policy framework combining the options identified in Section 7, sequenced to address the most urgent risks first while building the political and technical foundation for measures that are currently less feasible.

Bilateral Technology Incidents Protocol

The framework's first and most urgent component is the establishment of the BTIP described in Section 7.1, comprising a hypersonic-incidents channel, a cyber–NC2 non-interference mechanism, and a space-incidents notification mechanism. This component targets the highest-priority risks identified in Table 1, conventional-nuclear entanglement and cyber effects on NC2 infrastructure and is prioritized despite its moderate feasibility because the urgency of these risks, per Section 8, outweighs the implementation cost.

Domain-Specific Confidence-Building Measures

The framework's second component comprises the CBMs described in Section 7.2; hypersonic test pre-notification, a joint declaration on human-control standards for nuclear-adjacent autonomous systems, and NC2 exclusion understandings. These measures are pursued in parallel with the BTIP, as they address overlapping but analytically distinct risk pathways, the BTIP provides real-time incident communication, while the CBMs reduce the structural frequency of the incidents that communication is needed to manage.

Multilateral and Track-1.5 Governance

The framework's third component pursues the multilateral and Track-1.5 measures described in Section 7.3, including a narrower CCW Group of Governmental Experts mandate on nuclear-adjacent autonomous weapons applications (United Nations, 2025b) and Track-1.5 dialogues on AI, hypersonic, and the cyber-nuclear interface. Regional states including Japan, Australia, India, and ASEAN members, are engaged not as automatic supporters of either Washington's or Beijing's position, but according to their own institutional interests and regional security concerns.

Online ISSN: 3006-8886
Print ISSN: 3006-8878

ASEAN's Outlook on the Indo-Pacific, which emphasizes dialogue over bloc confrontation, is identified as a potentially useful venue for advancing CBM proposals without triggering the more zero-sum dynamics that have constrained direct bilateral engagement (ASEAN, 2019). This component provides the political groundwork and technical expertise that can, over time, improve the feasibility of the more direct bilateral measures in 9.1 and 9.2.

Implementation Framework

Table 3: Implementation Framework for Recommended Policy Measures

Policy Recommendation	Primary Actors	Mechanism	Time Horizon	Major Constraint
Hypersonic incidents channel	DoD; PLA Rocket Force; existing military-to-military channels	Direct military-to-military communication channel	Short-term	Political willingness to institutionalize outside crisis periods
Cyber–NC2 non-interference understanding	National Security Council; CISA; PLA cyber command elements	Reciprocal declaratory commitment with notification procedure	Short- to medium-term	Verification relies on good-faith reporting; attribution disputes
Space-incidents notification mechanism	U.S. Space Command; PLA Strategic Support Force successor elements	Bilateral notification channel modeled on existing space-safety practice	Medium-term	Absence of existing bilateral space-security dialogue to build on
Hypersonic pre-launch test notification	DoD; PLARF; State Department; Chinese Ministry of Foreign Affairs	Notification protocol modeled on existing missile-test arrangements	Short-term	Requires precedent-setting first agreement in a historically opaque domain
Human-control declaration for nuclear-adjacent autonomous systems	White House; Central Military Commission; UN CCW GGE on LAWS	Joint political declaration, potentially UN-endorsed	Medium-term	Verification of internal command-and-control practices is inherently limited
NC2 exclusion understandings	DoD; PLA Rocket Force; Track-1.5 technical experts	Geographic/functional designation with reciprocal targeting restraint	Medium- to long-term	Requires indirect disclosure of facility sensitivity without revealing exact locations
Track-1.5 dialogues (AI, hypersonics, cyber-nuclear interface)	Academic and former-official participants from both countries; CSIS, Carnegie, and comparable Chinese institutions	Recurring unofficial dialogue series	Short-term (can begin immediately)	Translating dialogue outcomes into binding government commitments
Regional and multilateral engagement	Japan; Australia; India; ASEAN	Multilateral forums and regional working groups	Short- to medium-term	Limited direct leverage over bi-

Online ISSN: 3006-8886
Print ISSN: 3006-8878

(Quad, ASEAN, UN CCW GGE)	Secretariat; UN	lateral U.S.–China commitments

Source: Author's Own

Discussion

The preceding analysis indicates, first, that emerging military technologies challenge classical strategic stability theory not merely by adding new capabilities to existing arsenals, but by compressing the temporal and perceptual conditions, decision time, signal clarity, and confidence in relative capability on which each of SST's three classical dimensions depends. Second, the compounding technological uncertainty described in Section 3.3 interacts with crisis, arms-race, and deterrence stability rather than operating as a separate fourth category: uncertainty about relative capability itself contributes to first-strike incentives (crisis stability), compensatory investment (arms-race stability), and doubts about second-strike survivability (deterrence stability), a dynamic Levite et al. (2021) document concretely for the cyber-nuclear C3 relationship specifically.

Third, the governance analysis in Section 6 indicates that existing bilateral and multilateral mechanisms have not kept pace with these technological developments primarily because of the reluctance of both governments to accept transparency and notification obligations regarding programs each treats as a source of competitive advantage, rather than because of the technical infeasibility of governance itself nuclear arms-control frameworks were sustained during a period of comparable technical novelty (Krepon, 2021). Fourth, this suggests that policy responses should focus on reducing the probability of inadvertent or unintended escalation rather than on eliminating the underlying strategic competition between the two powers, which the evidence available to this analysis does not indicate either government is prepared to abandon, and which lies outside the scope of feasible near-term policy. Fifth, because the risks analyzed throughout this article arise substantially from reciprocal, security-seeking behavior and action-reaction dynamics rather than from the unilateral conduct of either state, measures that are reciprocal and mutually acceptable rather than measures requiring asymmetric concessions from one side alone are correspondingly more realistic and more likely to be sustained through periods of broader political tension.

Finally, the deliberate exclusion of quantum computing and semiconductor competition from Section 4, discussed in Sections 1.6 and 2.5, should be read as a scope decision rather than a judgment that these issues are unimportant. Both bear on the technologies analyzed here computing capacity underwrites AI and autonomy, which is why the 2025 U.S. export-control actions are noted briefly in Section 4.1, and cryptographically relevant quantum computing would, if achieved, bear on the survivability of second-strike forces but the publicly available evidence does not yet support the same kind of documented, source-grounded risk-pathway analysis applied to the six domains in Section 4. Analysts and policymakers should treat these as issues warranting continued monitoring rather than immediate governance action, a judgment consistent with, rather than contradictory to, this article's broader emphasis on evidentiary discipline.

These findings reinforce the article's central contribution; connecting the technology-specific empirical analysis of Section 4, the theoretical framework of Section 3, and the systematically

Online ISSN: 3006-8886
Print ISSN: 3006-8878

evaluated policy options of Sections 7 and 8 into a single analytical chain that moves from technological development to strategic-stability risk to governance gap to evaluated policy response.

Key Findings

1. Compressed decision time is the common thread. AI-enabled decision-support systems and hypersonic delivery systems both reduce the time available for human assessment and decision-making during a crisis. This compression of decision time constitutes a key mechanism through which these technologies can contribute to degraded **crisis stability** across the technologies examined.

2. Conventional–nuclear entanglement and cyber effects on nuclear command, control, and communications (NC3) pose the highest risks. These two domains interact with all three dimensions of Strategic Stability Theory and affect infrastructure and decision-making processes closely connected to nuclear forces and employment decisions. They therefore emerge as the most urgent risk areas identified in Table 1.

3. Autonomous systems primarily intensify arms-race dynamics rather than generating acute crisis risks. Their relatively low cost, scalability, and rapid fielding potential can encourage reciprocal military buildup by both sides. Their destabilizing consequences therefore tend to materialize indirectly through other, more acute risk pathways.

4. Instability is reciprocal rather than one-sided. Across the technologies examined, the evidence is consistent with a security-dilemma dynamic in which investments perceived by one side as defensive or precautionary may be interpreted by the other as threatening, prompting compensatory responses. The resulting instability is therefore better understood as an interactive process than as the product of unilateral escalation by either government.

5. The governance gap is primarily institutional rather than technical. Existing bilateral and multilateral mechanisms have not adequately kept pace with emerging military technologies. The principal constraints appear to include limited political willingness to accept the transparency, information-sharing, and mutual restraint required for more effective governance, rather than the absence of technically feasible governance mechanisms.

6. A sequenced and complementary policy response is more realistic than any single measure. The evaluation in Section 8 indicates that no single policy option performs strongly across both effectiveness and feasibility criteria. The framework proposed in Section 9 therefore combines a bilateral incidents protocol, domain-specific confidence-building measures (CBMs), and multilateral and Track-1.5 engagement. This combination is intended to address the identified risks through complementary mechanisms rather than relying on a single instrument.

Conclusion

This article has undertaken a qualitative, problem-oriented policy analysis of the effects of emerging military technologies on U.S.–China strategic stability in the Indo-Pacific. The central finding is that these technologies such as artificial intelligence-enabled systems, autonomous and unmanned platforms, hypersonic delivery vehicles, entangled conventional-nuclear systems, cyber capabilities with potential effects on NC2 infrastructure, and counter-space systems gener-

Online ISSN: 3006-8886
Print ISSN: 3006-8878

ate strategic-stability risk primarily through four interacting mechanisms: compression of crisis-decision timelines, deepening of conventional-nuclear entanglement, increased vulnerability of nuclear command-and-control infrastructure, and pervasive technological uncertainty, each of which the existing governance architecture has not adequately adapted to manage.

The principal governance gap identified, a widening divergence between the pace of technological change and the institutional capacity of both bilateral and multilateral mechanisms to manage its consequences, constitutes the policy problem this article addresses. In response, the article identified and systematically evaluated three categories of policy option a Bilateral Technology Incidents Protocol, domain-specific confidence-building measures, and multilateral/Track-1.5 governance engagement, against explicit criteria of effectiveness, feasibility, urgency, implementation difficulty, and escalation sensitivity, and recommended a sequenced, complementary combination of the three, specified through the implementation framework in Section 10.

Theoretically, the article applies Strategic Stability Theory to a multi-domain contemporary technological environment, and it shows that compounding technological uncertainty is a pattern that reinforces, not detracts from, the three classical dimensions of SST, and that this analytical chain is consistently applied from technology to stability mechanism to SST dimension to governance gap to policy response. Analytically, it extends this approach to both U.S. and Chinese capabilities and doctrine, viewing instability as largely a result of mutual security-seeking actions and reaction rather than as a result of the unilateral actions of either state. In policy terms, it goes beyond a diagnosis of risk to a set of recommendations that are systematically evaluated and implementable, deliberately limited to the technologies for which the evidence is available, and supported throughout by an independently verified reference base, not assumed.

The analysis is limited by the factors outlined in Section 2.5, such as the fact that it is based on publicly available information, that technology is changing rapidly and that strategic perceptions are not directly observed. In this context, the main policy conclusion of the article is that it is important to maintain, rather than eliminate, the strategic competition between the United States and China, but to reduce the likelihood of unintended or unmanaged escalation from technology-driven competition, it is necessary to invest in the institutions involved in the technologies discussed here, in a sustained and reciprocal manner.

Reference

1. Acton, J. M. (2018a). Escalation through entanglement: How the vulnerability of command-and-control systems raises the risks of an inadvertent nuclear war. *International Security, 43*(1), 56–99.
2. Acton, J. M. (2018b, October 29). *Inadvertent escalation and the entanglement of nuclear command-and-control capabilities*. Belfer Center for Science and International Affairs.
3. Acton, J. M. (2020). Cyber warfare and inadvertent escalation. *Daedalus, 149*(2), 133–149. https://doi.org/10.1162/daed_a_01794
4. Association of Southeast Asian Nations. (2019). *ASEAN outlook on the Indo-Pacific*. ASEAN Secretariat.
5. Bardach, E., & Patashnik, E. M. (2020). *A practical guide for policy analysis: The eightfold path to more effective problem solving* (6th ed.). CQ Press.

Online ISSN: 3006-8886
Print ISSN: 3006-8878

6. Basit, A., Bano, S., & Mahar, I. A. (2025). Nuclear stability or strategic crises? A contextual analysis of the India–Pakistan conflict of May 2025. *Social Prism, 2(4), 121–135.* https://doi.org/10.69671/socialprism.2.4.2025.109
7. Bureau of Industry and Security. (2025a, January 15). *Commerce strengthens restrictions on advanced computing semiconductors to enhance foundry due diligence and prevent diversion to PRC*. U.S. Department of Commerce.
8. Bureau of Industry and Security. (2025b, May 13). *Industry guidance to prevent diversion of advanced computing integrated circuits*. U.S. Department of Commerce.
9. Congressional Budget Office. (2023, January 31). *U.S. hypersonic weapons and alternatives*. U.S. Congress.
10. Congressional Research Service. (2025). *Hypersonic weapons: Background and issues for Congress* (CRS Report R45811). U.S. Congress.
11. Cybersecurity and Infrastructure Security Agency. (2024, February 7). *PRC state-sponsored actors compromise and maintain persistent access to U.S. critical infrastructure* (AA24-038A). U.S. Department of Homeland Security.
12. Department of Defense. (2020). *Defense space strategy summary*. Office of the Secretary of Defense.
13. Department of Defense. (2023). *2023 cyber strategy summary*. Office of the Secretary of Defense.
14. Department of Defense. (2024a, May 6). *Deputy Secretary of Defense Hicks announces first tranche of Replicator capabilities focused on all domain attritable autonomous systems*. U.S. Department of Defense.
15. Department of Defense. (2024b, September 30). *Replicator 2: Direction and execution* [Memorandum]. Office of the Secretary of Defense.
16. Department of Defense. (2024c, November 13). *Deputy Secretary of Defense Kathleen Hicks announces additional Replicator all-domain attritable autonomous capabilities*. U.S. Department of Defense.
17. Department of Defense. (2024d, December 18). *Military and security developments involving the People's Republic of China 2024*. Office of the Secretary of Defense.
18. Department of Defense. (2025, December 23). *Military and security developments involving the People's Republic of China 2025*. Office of the Secretary of Defense.
19. Geist, E., & Lohn, A. J. (2018). *How might artificial intelligence affect the risk of nuclear war?* RAND Corporation.
20. Horowitz, M. C. (2019). When speed kills: Lethal autonomous weapon systems, deterrence and stability. *Journal of Strategic Studies, 42*(6), 764–788.
21. Jervis, R. (1989). *The meaning of the nuclear revolution: Statecraft and the prospect of Armageddon*. Cornell University Press.
22. Krepon, M. (2021). *Winning and losing the nuclear peace: The rise, demise, and revival of arms control*. Stanford University Press.
23. Paparo, S. J. (2025, April 9). *Statement of Admiral Samuel J. Paparo, Commander, U.S. Indo-Pacific Command: U.S. Indo-Pacific Command posture*. U.S. House of Representatives Committee on Armed Services.
24. Perkovich, G., Levite, A. E., Lyu, J., Lu, C., Li, B., Yang, F., & Xu, M. (2021, April 8). *China-U.S. cyber-nuclear C3 stability*. Carnegie Endowment for International Peace.
25. Schelling, T. C. (1966). *Arms and influence*. Yale University Press.

Online ISSN: 3006-8886
Print ISSN: 3006-8878

26. Secure World Foundation. (2024). *Global counterspace capabilities: An open-source assessment*. Secure World Foundation.
27. Swope, C., Bingen, K. A., Young, M., & LaFave, K. (2025, April 25). *Space threat assessment 2025*. Center for Strategic and International Studies.
28. Speier, R. H., Nacouzi, G., Lee, C., & Moore, R. M. (2017). *Hypersonic missile nonproliferation: Hindering the spread of a new class of weapons*. RAND Corporation.
29. State Council Information Office of the People's Republic of China. (2019). *China's national defense in the new era*.
30. State Council Information Office of the People's Republic of China. (2025, November 27). *China's arms control, disarmament, and nonproliferation in the new era*.
31. State Council of the People's Republic of China. (2017, July 20). *New generation artificial intelligence development plan*.
32. State Council of the People's Republic of China. (2026a, March 5). *China to nurture emerging and future industries*.
33. State Council of the People's Republic of China. (2026b, March 13). *Report on the work of the government*.
34. Talmadge, C. (2017). Would China go nuclear? Assessing the risk of Chinese nuclear escalation in a conventional war with the United States. *International Security*, *41*(4), 50–92.
35. United Nations. (2018). *Position paper submitted by China: Regulating the military applications of artificial intelligence* (CCW/GGE.1/MISC.1). Convention on Certain Conventional Weapons.
36. United Nations. (2025a). *Artificial intelligence in the military domain and its implications for international peace and security* (A/80/78). United Nations General Assembly.
37. United Nations. (2025b). *Group of Governmental Experts on emerging technologies in the area of lethal autonomous weapons systems*. Convention on Certain Conventional Weapons.
38. United Nations Office for Outer Space Affairs. (1967). *Treaty on principles governing the activities of states in the exploration and use of outer space, including the moon and other celestial bodies*.
39. Weimer, D. L., & Vining, A. R. (2017). *Policy analysis: Concepts and practice* (6th ed.). Routledge.
40. White House. (2015, September 25). *Fact sheet: President Xi Jinping's state visit to the United States*. Obama White House Archives.
41. White House. (2025, July 23). *Winning the AI race: America's AI action plan*. The White House.