Chinese Perspectives on Arms Control and Strategic Stability in Emerging Technologies

Tianjiao Jiang

Associate Professor of the Development Institute, Fudan University

China's strategic community remains concerned about the cross-domain entanglement of emerging technologies, believing that this situation creates new national and international security risks. On November 27, 2025, China released a white paper titled "China's Arms Control, Disarmament and Non-proliferation in the New Era," which for the first time dedicated a chapter to outlining its international security governance propositions in emerging fields such as outer space, cyberspace, and artificial intelligence[1]. This demonstrates that China will adopt a more proactive stance on arms control issues related to emerging technologies. However, the white paper also points out that the continuous improvement of missile defense technology and the rapid development of military applications in emerging fields such as outer space, cyberspace, and artificial intelligence are changing the traditional strategic offensive and defensive landscape and bringing new shocks to global strategic stability. In Beijing's view, it is not the emerging technologies themselves, but rather the unilateralism of specific countries that exacerbate security threats.

On the Issue of Space Entanglement

Space systems are crucial for strategic deterrence, enhancing command, control, communications, and intelligence. Space technology also maintains strategic stability by increasing transparency.

However, the imbalance of space power and the disorder of rules also bring instability. In the white paper, China explicitly raises four objections to the weaponization of space. One of the biggest concerns is the rapid development of mega-constellations like Starlink. These commercial satellite constellations blur the lines between military and civilian use, and lack clear international rules to constrain them. In times of crisis, Starlink could be rapidly militarized, providing communications and intelligence capabilities, thereby altering the military balance. Numerous examples have emerged in the previous Ukraine war and the protests in Iran last year. Therefore, the white paper explicitly opposes "the use of commercial satellites to intervene in armed conflicts in other countries and to interfere in the internal affairs

of other countries." More importantly, Elon Musk could decide to provide Starlink services to Ukraine or cease related services based on personal preferences or corporate interests, and such decisions would have serious geopolitical consequences. This poses a fundamental challenge to digital sovereignty.

Starlink enhances the resilience of the US space system through its distributed architecture, but it could make China's space assets vulnerable. Starlink plans to launch 40,000 satellites, while China currently has fewer than 1,000 in orbit. China's space station has been repeatedly approached by Starlink without its true intentions being known. Even just by collision, Starlink could potentially destroy a large portion of China's space assets. This is further compounded by the Trump administration's Golden Dome project. Starlink could be equipped with interceptors or possess non-kinetic attack capabilities such as lasers, microwaves, and electronic jamming. Non-kinetic attacks are particularly dangerous due to their reversible effects and the difficulty in attribution, and could be used as "probing attacks" during crises, increasing the risk of miscalculation and escalation of conflict.

On the Issue of Cyber Entanglement

As early as 2021, the Shanghai Institute for International Studies and the Carnegie Endowment for International Peace jointly released a report entitled "China-U.S. Cyber-Nuclear C3 Stability[2]." The Chinese strategic community believes that cyberattacks bring challenges in attribution and uncertainty, leading to miscalculations and escalation of conflict during crises. Therefore, the US-China Track II dialogue called for attention to the risks of cyber and nuclear entanglement, but ultimately failed to further implement confidence-building measures. With the rapid development of Starlink, satellite internet has now integrated space and cyberspace. This has increasingly blurred the boundaries between space security and cybersecurity. Nuclear command and control systems could be compromised due to cyberattacks on satellites or ground stations.

Furthermore, mutual trust between China and the US in the field of cybersecurity is very low, with frequent accusations of cyberattacks against each other. A recent example is when the US accused China of launching the so-called Volt Typhoon, in October 2025, China's Ministry of State Security stated that it possessed evidence of long-term NSA attacks on the China National Time Service Center since 2022, thus posing a significant negative impact on strategic stability. Meanwhile, China's strategic community has long expressed concern about persistent

engagement and hunt-forward cyber operations by the US, believing these actions could be used to thwart China's missile launches.

On the Entanglement Problem Brought about by AI

Adding AI to discussions of space, cyberspace, and nuclear entanglement complicates matters further. For example, a recent Anthropic report shows that traditional cybersecurity architectures are completely inadequate to handle cyberattacks by AI agents[3]. In fact, we don't really understand what kind of disruptive impact AI agents will bring.

Chinese strategic circles believe that AI is a double-edged sword for strategic stability. On the one hand, AI technology can improve NC3's reaction speed, enhance situational awareness, and increase system resilience. On the other hand, AI brings the challenges of information overload and time pressure during crises. Cyberattacks and disinformation can make it difficult for decision-makers to distinguish truth from falsehood. AI-driven data analysis systems can help process massive amounts of information, but they can also become targets for data poisoning and reward hacking, leading to misunderstandings and escalations.

The rapid development of AI technology itself, along with issues such as algorithmic black boxes, alignment issues, synthetic data problems, and the scheming, self-replication, and agent drift of frontier models, could all potentially trigger inadvertent or deliberate escalations of conflict. According to a recent study published by King's College London, advanced AI models tended to choose the use of nuclear weapons in 95% of simulated geopolitical crises[4]. This has raised widespread concerns about the future role of AI in military decision-making.

Several Track II dialogues between China and the US, and between China and Europe, are actively discussing these scenarios and exploring how to further deepen and broaden the commitment made by the top leaders of China and the US to keep nuclear weapons under human control. All parties should also jointly explore what constitutes meaningful human control, whether a negative list can be developed to avoid attacking each other's strategic AI systems, how to establish crisis management mechanisms and clarify handling principles and procedures for emergencies involving unmanned equipment and space assets, how to establish new hotlines to address crises and escalations caused by emerging technologies, how to reduce misperceptions regarding each other's emerging technology development and military application, and how to adopt insurance measures such as nuclear fail-safe. While these

measures are far from credible and verifiable, doing nothing will only exacerbate the security dilemma and strategic instability.

Broader Recommendations for Future Research

First, research on how artificial intelligence technology further complicates the entanglement of space, cyberspace, and nuclear systems remains insufficient, particularly regarding the analysis of technical details. The academic community still has limited understanding of the extent to which AI has been applied militarily in various countries. However, this is crucial for understanding what constitutes meaningful human control and is a challenging task.

Second, research on the involvement of non-state actors, especially technology companies, in geopolitics is needed. For example, how do commercial satellite constellations alter the balance of communication capabilities during crises? How do cybersecurity vulnerabilities in the private sector propagate to nuclear facilities? What kind of domestic regulatory and international legal innovations are needed to regulate and govern these emerging actors?

Finally, how does the Global South view these challenges and what role will it play in maintaining global strategic stability? How will competition among major powers in emerging technologies affect the development and security environment of these countries? How can we bridge the digital divide while avoiding the security risks posed by the proliferation of emerging technologies? These researches will contribute to enriching global dialogue and building a more equitable and inclusive governance system.

Notes

[1] Ministry of Foreign Affairs, People's Republic of China "China releases white paper on arms control in new era," November 27, 2025, https://www.fmprc.gov.cn/mfa_eng/xw/wjbxw/202511/t20251127_11761653.html[2] George Perkovich et al. "China-U.S. Cyber-Nuclear C3 Stability," Carnegie Endowment for International Peace, April 8, 2021, https://carnegieendowment.org/research/2021/04/china-us-cyber-nuclear-c3-stability.

[3] Anthropic, "Disrupting the first reported AI-orchestrated cyber espionage campaign," November 13, 2025, https://www.anthropic.com/news/disrupting-AI-espionage.

[4] Kenneth Payne "King's study finds AI chose nuclear signalling in 95% of simulated crises," King's College London 27 February 2026, https://www.kcl.ac.uk/news/artificial-intelligence-

under-nuclear-pressure-first-large-scale-kingsstudy-reveals-how-ai-models-reason-and-escalate-under-crisis

About the Author

Tianjiao Jiang is associate professor at Development Institute of Fudan University. He also serves as deputy director of Center for BRICS Studies and research fellow of Center for Global AI Innovative Governance at Fudan. His research focuses on emerging technologies, international security and BRICS cooperation. He has published 4 books and more than 40 academic papers in the World Economics and Politics, Foreign Affairs Review, journal of International Security Studies, Copenhagen Journal of Asian Studies, etc. Dr. Jiang is member of China Arms Control and Disarmament Association, ACONA fellow of Davis Center for Russian and Eurasian Studies at Harvard University (2021-2022), and visiting scholar at Paul Tsai China Center of Yale Law School (2026). He is frequently interviewed by media outlets such as the New York Times, the South China Morning Post, and Le Monde, and has participated as an expert in P5 Young Professional Network and several Track II dialogues on Sino-US strategic stability.