Council for Security Cooperation in the Asia Pacific

Regional Security Outlook

2026

Integrated Technologies, Fragmented Governance:

Emerging Escalation Risks in Northeast Asia

Umi Ariga, Research Fellow, Japan Institute of International Affairs

If a missile launch were detected over the Korean Peninsula today, the warning would likely move from ground- and space-based sensors through automated processing and multi-sensor fusion, across data links and networked command-and-control systems, before reaching a human decision-maker—each layer speeding detection and dissemination while also expanding the vulnerable attack surface (Saltini et al. 2025). Across Northeast Asia's flashpoints, AI, cyber capabilities, space-based systems, and prospective quantum advances are becoming embedded within shared data networks and decision-support architectures.

This article argues that the strategic significance of these developments lies less in their individual capabilities than in their interaction effects: the way these technologies connect to create new, compounded risks. As military systems become more digitally integrated, they compress decision timelines, heighten uncertainty about data integrity, and multiply pathways for cross-domain escalation. This means that a localized incident in one area, such as a cyber intrusion or interference with a satellite, can now much more easily spill over and trigger a wider military response across the air, sea, or land domains. These dynamics do not undermine deterrence in Northeast Asia's overlapping nuclear and conventional deterrence relationships, but they intensify structural stressors in a region already marked by frequent missile testing, contested air and maritime operations, and persistent high readiness.

While bilateral and trilateral defence- and security-co-operation mechanisms have expanded in recent years, governance of these mechanisms remains largely siloed by domain and unevenly distributed across the region. Managing the risks of emerging technologies therefore requires governance mechanisms that are as integrated as the technologies themselves.

Soyuz TMA-16 launches from the Baikonur Cosmodrome in Kazakhstan, 2009. Photo by NASA via Unsplash

“Emerging defence technologies in Northeast Asia are not advancing along parallel tracks. The region’s most consequential capabilities increasingly depend on shared data, networks, and space-enabled connectivity, creating interlocking chains in which disruption in one domain could cascade into others.”

Cross-Domain Integration of Emerging Technologies in Northeast Asia

Emerging defence technologies in Northeast Asia are not advancing along parallel tracks. The region's most consequential capabilities increasingly depend on shared data, networks, and space-enabled connectivity, creating interlocking chains where disruption in one domain could cascade into others. Northeast Asia is uniquely sensitive to these dynamics because of its geography and the high density of advanced military assets in close proximity. In geographically compressed theatres such as the Taiwan Strait and the Korean Peninsula, missile flight times are measured in minutes, significantly reducing warning and decision timelines. In such environments, advances in hypersonic weapons and AI-enabled targeting further accelerate the pace of operations, such that even marginal increases in speed can disproportionately affect the tactical balance by reinforcing first-mover advantages. Furthermore, the region is characterized by persistent high readiness and frequent missile testing, creating an environment where automated alerts or data disruptions are more likely to be interpreted as precursors to an actual strike.

The most mature illustration of AI-enabled, multi-sensor fusion remains the United States' Project Maven, established explicitly to "turn the enormous volume of data" from Intelligence, Surveillance, and Reconnaissance (ISR) into actionable intelligence by integrating big data and machine learning into processing, exploitation, and dissemination workflows (Deputy Secretary of Defense 2017). Maven's model (algorithmic assistance applied to imagery and sensor flows) has become the reference point for how AI can accelerate target recognition and analysis at scale (Kuzuoka 2024; Pfaff and Hickey 2025).

In Northeast Asia, publicly documented integration often points to networked kill-chain connectivity (data links enabling target identification and strike execution) and warning-chain connectivity (links transmitting early-warning data to defenders), especially via satellite communications. Japan's upgraded Type 12 surface-to-ship missile program, for instance, highlights how long-range strikes increasingly rely on space-enabled data links: its "Up to Date Command" function is designed to receive target updates via satellite communications mid-flight, enabling strikes against moving targets at extended distances (Inaba 2022). Japan's investment in dedicated defence communications satellites (e.g., Kirameki) similarly reflects how command connectivity and data sharing are being expanded through space infrastructure (Kim 2025).

This connectivity also expands vulnerabilities. Sensors, satellites, data links, and command networks have all become potential points of disruption. Cyber operations aimed at networks or space-based infrastructure can corrupt or delay the information that targeting and early warning depend upon, often in ambiguous ways. The strategic problem is therefore not simply the existence of offensive cyber tools, but their ability to exploit the interdependence of data-dependent command structures. When decision-making relies on a continuous information flow, interference with that flow can generate uncertainty across the entire system.

> “The strategic problem is therefore not simply the existence of offensive cyber tools, but their ability to exploit the interdependence of data-dependent command structures.”

China’s evolving concept of “intelligentized warfare” reflects this same tension between integration and vulnerability. It is described as coordinated operations across land, sea, air, space, electromagnetic, cyber, and cognitive domains, underpinned by networked information systems and data fusion (Takagi 2022; Yamaguchi et al. 2023, 46). While such integration promises greater coordination and speed, it also deepens reliance on uninterrupted data flows and digital connectivity. As in the US and Japanese cases, Chinese operational effectiveness is also increasingly tied to system-wide interdependence. Taken together, Northeast Asia’s technological acceleration has generated cross-domain dependence on data integrity and connectivity, acting as a multiplier for military effectiveness but also as a source of systemic fragility.

Finally, quantum computing represents a longer-term but potentially structural disruptor of this networked system. Modern military integration depends on encryption securing satellite communications, missile data links, command networks, and early-warning transmissions. Advances in quantum computing could, in principle, undermine widely used public-key cryptographic systems that protect these channels (Chochrek 2025; Riaz and Waseem 2026). While large-scale, relevant quantum computers do not yet exist, states must assume that encrypted communications intercepted today could be decrypted in the future. In a region where strategic stability relies heavily on secure command-and-control and early-warning systems, even the simple prospect of quantum-enabled decryption introduces long-term uncertainty, in particular into Nuclear Command, Control, and Communication (NC3) integrity (Ajaykumar 2025).

Implications for Regional Stability in Northeast Asia

Technological acceleration does not automatically translate into operational transformation. Despite experimentation with AI-enabled systems, a gap remains between demonstrated capability and battlefield reality. That said, crisis stability (the degree to which states can manage escalating tensions without triggering pre-emptive action) depends as much on perceived trajectories

> “Technological acceleration does not automatically translate into operational transformation. Despite experimentation with AI-enabled systems, a gap remains between demonstrated capability and battlefield reality.”

as on fully realized systems. In Northeast Asia—a region marked by frequent missile testing, near-miss air and maritime encounters, and persistent high readiness—incremental shifts in speed and connectivity can have disproportionate effects.

First, digitally networked systems compress decision timelines (Boulanin et al. 2020, 113–14). As the US defence planning around the “sense, make sense, act” concept underscores, modern command-and-control increasingly hinges on accelerating the flow from sensing to decision across domains (US Department of Defense 2022). AI-assisted processing can accelerate this cycle, flagging anomalies and elevating alerts in seconds. In flashpoints such as the Korean Peninsula or the Taiwan Strait, this temporal compression reduces deliberation space (Saalman 2019, 104; Johnson 2024). When ambiguous signals are framed as urgent threats, decision-makers may feel pressure to act before verification is complete. Precautionary moves taken under time pressure may escalate a crisis, even if no actor initially intended to do so.

Second, the growing dependence on interconnected data flows heightens concerns about both integrity and attribution (Levite et al. 2021). Cyber interference, whether through GPS spoofing, satellite-uplink disruption, or network intrusion, does not need to destroy systems to destabilize them; it need only introduce doubt. In tightly networked architectures, anomalous signals may stem from a technical malfunction, an environmental interference, or deliberate manipulation. The difficulty lies not only in detecting corrupted data, but in determining the intent behind the disruption. If commanders cannot distinguish a system error from a hostile intrusion, confidence in early-warning and command networks erodes. In nuclear-armed environments, where rapid assessment underpins deterrence credibility, even temporary uncertainty can distort risk perceptions and incentivize precautionary responses (Raju and Wan 2024).

Finally, the growing interconnection between domains increases the risk that a problem in one area quickly spreads to others. This dynamic is not entirely new (Acton 2018). However, as more military functions depend on shared data networks, satellite connectivity, and AI-assisted processing, the number of potential spillover points expands (Arie 2024). A cyber intrusion into a satellite ground station can disrupt missile-warning data. Interference with space-based navigation can affect conventional air or naval operations. A limited conventional clash, in turn, may prompt cyber retaliation against

A UN staff member at work in the General Assembly Hall on the first day of the debate of the General Assembly's seventy-ninth session, September 24, 2024. Photo by Loey Felipe via UN Photo

command networks or electronic interference with space assets. As military systems become more tightly linked through shared data and communications, it becomes harder to contain incidents within a single domain.

Taken together, emerging technologies in Northeast Asia do not fundamentally overturn deterrence, but they intensify three enduring stressors of crisis stability: speed, uncertainty, and cross-domain entanglement. The strategic problem is therefore less about the existence of new tools than about how their interaction compresses time, complicates judgment, and widens escalation pathways. Managing these interaction effects is the central stability challenge facing the region.

Existing Frameworks and Co-operation Mechanisms in Northeast Asia

Over the past several years, a dense set of bilateral and minilateral initiatives have been developed regarding emerging technologies, particularly within the US–Japan–South Korea trilateral framework. At the global level, normative discussions on military AI and cybersecurity continue at the United Nations, including the UN General Assembly's resolution on AI in the military domain (United Nations General Assembly 2024). While these efforts provide important principles, they remain largely declaratory and do not offer regionally tailored operational mechanisms for managing escalation or coordinating restraint in a crisis.

Regionally, the most significant development has been the institutionalization of US–Japan–South Korea co-operation. In December 2023, the three governments fully activated a real-time North Korean missile-warning data-sharing mechanism and adopted a multi-year trilateral

exercise plan (US Department of Defense 2023). Their annual trilateral exercise, Freedom Edge, further aims to deepen interoperability across maritime-, air-, and missile-defence domains (US Indo-Pacific Command Public Affairs 2025). In parallel, director-level US–Japan–South Korea dialogues on space security now address threats, national strategies, and responsible behaviour in orbit (Ministry of Foreign Affairs of Japan 2023).

Bilateral co-operation within Northeast Asia has also expanded. In 2025, South Korea and Japan agreed to pursue co-operation in emerging defence technologies, including AI, unmanned systems, and space—a commitment that was again reinforced in 2026 under the new Japanese leadership (Lee 2025; Indo-Pacific Defense Forum 2026). Seoul has deepened defence-industrial collaboration with the United States, including joint work between Hanwha Aerospace and General Atomics Aeronautical Systems on unmanned aircraft systems (Hanwha 2025). Both Japan and South Korea are also diversifying partnerships beyond the United States: Japan's participation in the Global Combat Air Programme with the United Kingdom and Italy institutionalizes advanced defence-technology collaboration, while both South Korea and Japan are key players in NATO's Indo-Pacific Four (IP4) flagship projects on cyber defence, emerging technologies, and supply-chain security.

China's approach to emerging technologies has emphasized self-sufficiency and civil–military integration, with comparatively limited transparency regarding how cross-domain escalation risks would be managed in crisis (Gokireddy and Jash 2024). Taiwan, facing acute threat, has prioritized asymmetric resilience and rapid technological adaptation. However, because it is not part of US alliance frameworks in the region, it lacks formalized multilateral mechanisms through which emerging-technology risks can be jointly addressed (Panella 2025). The result is a fragmented regional landscape in which technological integration advances more rapidly than shared crisis-management frameworks.

Taken together, these developments demonstrate a growing capacity for co-operation that nevertheless lacks alignment with the evolving risks facing the region. Existing initiatives remain largely organized by domain—missile defence, space security, cyber coordination, or industrial development—while the escalation dynamics described earlier cut across them. Northeast Asia therefore exhibits a governance gap: technological integration is advancing at the cross-domain level, but institutional responses remain compartmentalized.

Toward Cross-Domain Guardrails in Northeast Asia

As emerging technologies simultaneously impact decision-making speed, heighten uncertainty, and increase the chances of cross-domain spillover, the challenge of managing the region's stability becomes institutional rather than purely technological. In this context, Northeast Asia needs practical guardrails designed to prevent ambiguous disruptions from escalating.

The first priority is continuity, considering that the political momentum behind US–Japan–South Korea co-operation is vulnerable to leadership turnover and shifting strategic priorities (Kanodia 2025). As a result, the most durable guardrails should be built below the level of summit diplomacy. Regular technical and operational dialogue among mid-level defence and intelligence officials can sustain co-operation even when political relations fluctuate. The recent institutionalization of recurring director-level meetings, working groups, and trilateral-secretariat support provides an administrative foundation that could be leveraged for emerging-technology risk reduction.

Second, Northeast Asian actors should complement existing domain-specific co-operation with cross-domain risk framing. Existing mechanisms already cover missile warning, cyber coordination, and space dialogue, but they largely treat these issues separately. A modest but meaningful step would be to introduce a shared agenda focused on interaction risks: data integrity in warning systems, ambiguous cyber/space interference, and decision-time compression. The objective would not necessarily be to standardize capabilities or disclose sensitive operational details, but to develop shared understandings of how uncertain events are interpreted and managed in crisis.

Third, the region should prioritize risk-reduction routines rather than ambitious new treaties. This can include agreed practices for consultation during disruptive cyber/space incidents affecting strategic systems, and regular scenario-based discussions among relevant stakeholders. Exercises already underway can also be used as governance laboratories: their value is not only interoperability but rehearsing how actors communicate and deconflict under stress.

Finally, partnership diversification can reinforce risk-reduction guardrails by broadening exposure to trusted practices and benchmarks for responsible emerging-technology use. Both South Korea and Japan are widening their defence partnerships beyond the core alliance framework, helping to socialize shared expectations about responsible behaviour in contested domains.

Taken together, these steps treat cross-domain guardrails as a *governance layer* that can be incrementally strengthened through institutional continuity, shared risk framing, and routine co-operation, even in cases of imperfect political alignment.

> “As emerging technologies simultaneously impact decision-making speed, heighten uncertainty, and increase the chances of cross-domain spillover, the challenge of managing the region’s stability becomes institutional rather than purely technological.”

REFERENCES

Acton, James M. 2018. "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. https://doi.org/10.1162/isec_a_00320.

Ajaykumar, Shravishtha. 2025. "Redefining Nuclear Command and Control: A Look at Quantum Communication and AI." *Observer Research Foundation,* August 26. https://www.orfonline.org/expert-speak/redefining-nuclear-command-and-control-a-look-at-quantum-communication-and-ai.

Arie, Koichi. 2024. "New Domains and Nuclear Weapons Systems: The Implications for Nuclear Deterrence and Arms Control." In *New Horizons of the Nuclear Age,* edited by Ichimasa Sukeyuki. National Institute for Defense Studies.

Boulanin, Vincent, Lora Saalman, Petr Topychkanov, Fei Su, and Moa Peldán Carlsson. 2020. *Artificial Intelligence, Strategic Stability and Nuclear Risk.* Stockholm International Peace Research Institute. https://www.sipri.org/sites/default/files/2020-06/artificial_intelligence_strategic_stability_and_nuclear_risk.pdf.

Chochrek, Jamison. 2025. "How Quantum Computing Will Change the Status Quo of Cyber Security." *Proceedings of the European Conference on Cyber Warfare and Security* 24 (1). https://doi.org/10.34190/eccws.24.1.3595.

Deputy Secretary of Defense. 2017. "Memorandum: Establishment of an Algorithmic Warfare Cross-Functional Team (Project Maven)." US Department of Defense, April 26. https://dodcio.defense.gov/Portals/0/Documents/Project%20Maven%20DSD%20Memo%2020170425.pdf.

Gokireddy, Hima Bindu, and Amrita Jash. 2024. "China's Shift from CMI to MCF: Military Modernization and the Defense Industry at the Core." *Issues & Studies* 60 (3). https://doi.org/10.1142/S1013251124500127.

Hanwha. 2025. "Hanwha Aerospace Signs Contract with GA-ASI for UAS Co-Development." Press release, October 16. https://www.hanwha.com/newsroom/news/press-releases/hanwha-aerospace-signs-contract-with-ga-asi-for-uas-co-development.do.

Inaba, Yoshihiro. 2022. "Here Is Our First Look at Japan's Type 12 SSM (Upgraded)." *Naval News,* August 17. https://www.navalnews.com/naval-news/2022/08/here-is-our-first-look-at-japans-type-12-ssm-upgraded/.

Indo-Pacific Defense Forum. 2026. "Japan, ROK Advance Defense Collaboration, Plan Naval Exercise." February 22. https://ipdefenseforum.com/2026/02/japan-rok-advance-defense-collaboration-plan-naval-exercise/.

Johnson, James. 2024. "Revisiting the 'Stability–Instability Paradox' in AI-Enabled Warfare: A Modern-Day Promethean Tragedy Under the Nuclear Shadow?" *Review of International Studies:* 1–19. https://doi.org/10.1017/S0260210524000767.

Kanodia, Kanishkh. 2025. *Securing the Future of US–Japan–South Korea Cooperation: How to Strengthen the Trilateral Partnership and Maintain Stability in the Indo-Pacific.* Chatham House.

Kim, Felix. 2025. "Japan Boosts Defense Satellite Investments to Strengthen Space Resilience, Communications." *Indo-Pacific Defense Forum,* February 26. https://ipdefenseforum.com/2025/02/japan-boosts-defense-satellite-investments-to-strengthen-space-resilience-communications/.

Kuzuoka, Shigeki. 2024. "Projects Using Artificial Intelligence – Project Maven – Automatic Target Detection from Unmanned Aerial Reconnaissance Imagery." Global Institute of Emerging Security Technology, September 22. https://www.giest.or.jp/en/contents/briefs/2872/.

Lee, Minji. 2025. "Defense Chiefs of S. Korea, Japan Agree to Explore Cooperation on Advanced Technologies." *Yonhap News Agency,* September 8. https://en.yna.co.kr/view/AEN20250908001452315.

Levite, Ariel E., Lyu Jinghua, George Perkovich, et al. 2021. *China-U.S. Cyber-Nuclear C3 Stability.* Carnegie Endowment for International Peace. http://carnegieendowment.org/research/2021/04/china-us-cyber-nuclear-c3-stability.

Ministry of Foreign Affairs of Japan. 2023. "Japan-U.S.-ROK Trilateral Dialogue on Space Security (Director-Level Meeting)." November 8. https://www.mofa.go.jp/fp/msp/page1e_000802.html.

Panella, Chris. 2025. "Taiwan Needs to Flood the Battlefield with Cheap, Mobile, and Survivable Weapons to Counter China, Former Senior Military Officer Says." *Business Insider,* December 23. https://www.businessinsider.com/taiwan-needs-lots-low-cost-weapons-china-war-former-official-2025-12.

Pfaff, C. Anthony, and Christopher John Hickey. 2025. *Integrating Artificial Intelligence and Machine Learning Technologies into Common Operating Picture and Course of Action Development.* United States Army War College Press. https://press.armywarcollege.edu/monographs/980.

Raju, Nivedita, and Wilfred Wan. 2024. *Escalation Risks at the Space–Nuclear Nexus.* SIPRI Research Policy Paper. Stockholm International Peace Research Institute. https://www.sipri.org/sites/default/files/2024-02/2402_rpp_space-nuclear_nexus.pdf.

Riaz, Saad, and Sibra Waseem. 2026. "Quantum Technologies: Transforming Battlefield Surveillance and Targeting." *Comparative Strategy,* February: 1–21. doi:10.1080/01495933.2026.2624401.

Saalman, Lora. 2019. "The Impact of Artificial Intelligence on Nuclear Asymmetry and Signalling in East Asia." In *The Impact of Artificial Intelligence on Strategic Stability and Nuclear Risk, Volume II: East Asian Perspectives,* edited by Lora Saalman. Stockholm International Peace Research Institute.

Saltini, Alice, Sylvia Mishra, and Philip Reiner. 2025. *Nuclear Command, Control & Communications (NC3): A Primer on Strategic Warning, Decision Support, and Adaptive Targeting Subsystems.* The Institute for Security and Technology. https://securityandtechnology.org/wp-content/uploads/2025/07/NC3-Primer-on-Strategic-Warning-Decision-Support-and-Adaptive-Targeting-Subsystems.pdf.

Takagi, Koichiro. 2022. "New Tech, New Concepts: China's Plans for AI and Cognitive Warfare." *War on the Rocks,* April 13. https://warontherocks.com/2022/04/new-tech-new-concepts-chinas-plans-for-ai-and-cognitive-warfare/.

United Nations General Assembly. 2024. Resolution 79/239: *General and Complete Disarmament.* A/RES/79/239. December 24.

US Department of Defense. 2022. *Summary of the Joint All-Domain Command & Control (JADC2) Strategy.* March. https://media.defense.gov/2022/Mar/17/2002958406/-1/-1/1/SUMMARY-OF-THE-JOINT-ALL-DOMAIN-COMMAND-AND-CONTROL-STRATEGY.PDF.

US Department of Defense. 2023. "United States-Japan-Republic of Korea Trilateral Ministerial Joint Press Statement." Press release, December 19. https://www.war.gov/News/Releases/Release/Article/3621235/united-states-japan-republic-of-korea-trilateral-ministerial-joint-press-statem/.

US Indo-Pacific Command Public Affairs. 2025. "Freedom Edge 2025: Building Trilateral Trust Across the Indo-Pacific." Press release, September 19. https://www.navy.mil/Press-Office/News-Stories/display-news/Article/4308744/freedom-edge-2025-building-trilateral-trust-across-the-indo-pacific/.

Yamaguchi, Shinji, Masaaki Yatsuzuka, and Rira Momma. 2023. *NIDS China Security Report 2023: China's Quest for Control of the Cognitive Domain and Gray Zone Situations.* National Institute for Defense Studies. https://www.nids.mod.go.jp/publication/chinareport/pdf/china_report_EN_web_2023_A01_revised.pdf.

2026

Council for Security Cooperation in the Asia Pacific