POLICY BRIEF NO. 130/2026-2027

CALIBRATING THE "ONE THEATRE" CONCEPT: A BLUEPRINT FOR CONSENT-BASED SECURITY COOPERATION AND TECHNOLOGICAL AUTONOMY

SOOJEONG CHOI

She is Berlin-based Senior Policy Analyst and Ph.D. (Candidate) at the University of Hamburg, specialising in international maritime law, submarine cable cyber infrastructure, and Indo-Pacific security. A former Senior Researcher at Korea Maritime Institute (KMI, 2000–2012), she has held research fellowships at NATO Defense College (Rome), NATO MARSEC COE (Istanbul), and NATO CCDCOE (Tallinn). Her forthcoming works on Indo-Pacific Strategy will be published with Palgrave Macmillan. She is an Institutional Partner at IADN, India. She can be reached at: soojeongchoi1209@gmail.com

As minilateral security architectures rapidly redefine the Indo-Pacific, a major structural challenge emerges for middle powers striving to preserve their strategic autonomy within allied frameworks. This paper examines the evolution of the U.S.-Japan "One Theatre Concept" (OCEAN Framework) and the centralised, AI-driven "SAMURAI Initiative," outlining a blueprint for calibrating regional integration with sovereign data protection. By analysing the data-sovereignty disputes surrounding Paragraph 3 of the 2026 NATO Ankara Summit Declaration and the recent legislative push by the U.S. Senate for real-time intelligence integration, the study highlights the cyber vulnerabilities—particularly via lateral movement from advanced state-sponsored hacker groups like North Korea's Lazarus—inherent in vertical, centralised military clouds. To foster resilient, long-term alliance cohesion without compromising national technological parameters, this paper introduces a horizontal calibration strategy tailored for India, South Korea, and NATO combining Zero-Knowledge Proofs (ZKP) and Tactical Edge Computing.

Advocating for an architecture built on consent-based security cooperation, the brief proposes decentralised "Sovereignty Filters" combining Zero-Knowledge Proofs (ZKP) and Tactical Edge Computing. This framework ensures that New Delhi and Seoul can actively contribute to high-velocity allied interoperability while leveraging NATO-established data sovereignty norms. Specifically, the consent-based, metadata-only principles embedded in NATO STANAG (Standardisation Agreement) 4586– to safeguard foundational technological sovereignty and foster a balanced, multi-layered regional security geometry.

*This **framework** ensures **that New Delhi and Seoul** can actively contribute to high-velocity allied **interoperability** while leveraging **NATO-established data sovereignty norms***

INTRODUCTION: THE ANKARA WARNING AND THE NEW INDO-PACIFIC REALISM

In July 2026, the NATO Summit in Ankara exposed a profound, largely underreported structural friction regarding data sovereignty among transatlantic allies. [i]The United States officially unveiled its $40 billion "Drone Edge" initiative, demanding that allies feed their front-line raw sensor data in real-time into a centralised theatre cloud modelled after the Pentagon's Joint Warfighting Cloud Capability (JWCC) architecture. As reflected in the Ankara Summit Declaration and the EPC's annotated reading,[ii] the European response led by France, Germany, and Türkiye was resolutely defensive. Recognising that centralised data networks lead to a catastrophic Single Point of Failure (SPOF) and the loss of independent

command, European powers drew an unyielding line. They refused to surrender raw sensor data, instead mandating a decentralised, compartmentalised standard (STANAG 4586) that limits exchanges strictly to refined operational outputs (metadata) via a newly formed Counter-Drone Marketplace.

A structurally analogous dynamic is now emerging in the Indo-Pacific, where the absence of a binding multilateral treaty framework comparable to NATO renders middle powers considerably more exposed to unilateral data centralisation pressures.[iii] Against the backdrop of Washington's transactional "America First" foreign policy and its managed retreat from primary peninsular defence burdens, the U.S. is aggressively flattening regional political nuances to force middle powers into centralised data architectures.[iv]

The "Ankara Warning" serves as an essential lesson for New Delhi and Seoul. Military alliances inherently generate multi-layered interdependencies spanning collective deterrence, diplomatic signalling, and economic co-production. These benefits are neither negligible nor illusory.

*The "**Ankara Warning**" serves as an essential lesson for **New Delhi** and **Seoul***

However, in the age of AI-driven warfare, the locus of strategic power has fundamentally shifted: the actor who controls the data pipeline controls the algorithmic decision cycle and, therefore, the operational tempo of the alliance itself. When a middle power is structurally compelled to feed its raw front-line sensor data into a foreign-operated centralised cloud without legal safeguards or reciprocal data governance rights, it surrenders the very cognitive infrastructure upon which independent command decisions rest. In this specific and increasingly prevalent configuration, military alliance

without data protection is not merely a technical inconvenience; it functions, in operational practice, as a structural mechanism of progressive strategic dependency. When the algorithmic models that process allied sensor data are owned, trained, and updated exclusively by a single partner's defence contractors, the dependent actor's operational judgements are increasingly shaped by analytical outputs it neither controls nor fully audits—a condition that progressively narrows the effective range of its autonomous strategic calculation.

THE ANKARA DECLARATION: TRANSATLANTIC DATA LOCALITY FRICTION

The strategic friction at the July 2026 Summit was crystallised during the negotiating process of the official Ankara Summit Declaration.[v] Behind closed doors, the formulation of Paragraph 3 became a geopolitical and technological battleground.[vi] The original operational concept, heavily driven by Washington's $40 billion "Drone Edge" initiative, pushed for an uncompromisingly centralised, unidirectional data architecture to power what the Pentagon envisioned as a "unified allied cloud repository."

However, delegations from Paris and Berlin launched an unyielding diplomatic counter-offensive. They successfully mandated that any framework governing the newly announced *"interoperable transatlantic warfighting cloud and adopting powerful AI models"* must strictly respect digital sovereignty and data locality as unalterable parameters of allied multi-domain integration.[vii]

French and German defence officials recognised that surrendering raw sensor data directly to an overseas centralised repository under great-power algorithmic hegemony undermines national strategic command, rendering independent sovereign defence assets functionally obsolete.[viii] By compelling a decentralised architectural consensus, the European allies established a vital regulatory precedent: allied interoperability does not mandate technical assimilation.[ix] This structural clash serves as a direct warning to the Indo-Pacific, where similar vertical integration pressures are being applied without the mitigating institutional buffer of a balanced multi-domain treaty network.[x]

French *and* ***German defence officials*** *recognised that* ***surrendering raw sensor data directly*** *to an* ***overseas centralised repository*** *under* ***great-power algorithmic hegemony undermines*** *national strategic command, rendering* ***independent sovereign defence assets*** *functionally obsolete*

DECONSTRUCTING THE ONE THEATRE CONCEPT AND THE PRESSURE OF THE INSTITUTIONALISED SUBJUGATION

The push toward vertical intelligence fusion in the Indo-Pacific has moved beyond mere strategic preference; it is rapidly becoming institutionalised. In June 2026, the U.S. Senate Intelligence Committee advanced Section 691 of the FY2027 Intelligence Authorisation Act, which legally mandates that the Director of National Intelligence (DNI) significantly deepen real-time intelligence integration with key regional partners, explicitly naming South Korea, Japan, Australia, and the Philippines. [xi]This legislative pressure aims to operationally consolidate the East China Sea, the South China Sea, the Taiwan Strait, and the Korean Peninsula into a single unified theatre zone—Tokyo's "*One Theatre Concept*" operationalised under the acronym OCEAN.[xii] To control this massive unified theatre, the U.S. and Japan have

launched the SAMURAI Initiative—an AI-driven platform powered by centralised big-tech cloud architectures such as Palantir and Anduril. The strategic objective is the *de facto* gatekeeping capacity over interoperability standards of regional "*AI algorithmic hegemony*" through the absorption of independent tactical data from regional partners.[xiii]

The illusion of this unified geometry was shattered in April 2026, when Philippine Secretary of National Defence Gilberto Teodoro Jr. explicitly declared that the Korean Peninsula must be excluded from its operational discussions of the OCEAN framework.[xiv] Manila's pragmatic decoupling reaffirmed a foundational principle of alliance theory: sovereign actors prioritise national interest calculations even within formalised security frameworks.[xv]

Manila's calculated exclusion of the Korean Peninsula from OCEAN discussions reveals a structural logic that transcends the specific geography of the South China Sea. The Philippines, despite being a treaty ally of the United States, demonstrated that even within a formalised bilateral security architecture, a sovereign actor retains both the political will and the institutional capacity to draw operational red lines when national interests diverge from alliance-wide frameworks.

The strategic conditions facing India are distinct in their geographic and doctrinal character—New Delhi's primary security calculus is anchored in the integrity of its continental borders along the Line of Actual Control and the assertion of autonomous maritime power projection across the Indian Ocean Region, neither of which maps neatly onto the East Asia-centric OCEAN geometry.

Yet the underlying structural dynamic is analogous in one critical respect: in both cases, a middle power operating within a U.S.-led security architecture faces the structural incentive to accept centralised data integration as the price of alliance credibility, regardless of whether that

integration aligns with its own primary threat calculus. It is this specific mechanism—the conflation of interoperability with data subordination—that Teodoro's decoupling exposes as negotiable, not inevitable

THE SHADOW OF LAZARUS: CYBER VULNERABILITIES OF CENTRALISED INTEGRATION

Centralised, real-time data synchronisation architectures inherently establish a massive, high-value Single Point of Failure. The actor most aggressively positioned to exploit this digital target is North Korea's Lazarus Group.[xvi] Within the trilateral Eurasian strategic alignment colloquially termed CRINK (China, Russia, Iran, and North Korea),[xvii] Pyongyang has transformed its military into a sophisticated hybrid actor by absorbing real-time battlefield lessons from the Russia-Ukraine War.[xviii] In exchange for troop deployments, Russia has transferred advanced military-grade electronic warfare, radar, and cyber capabilities to North Korea.[xix]

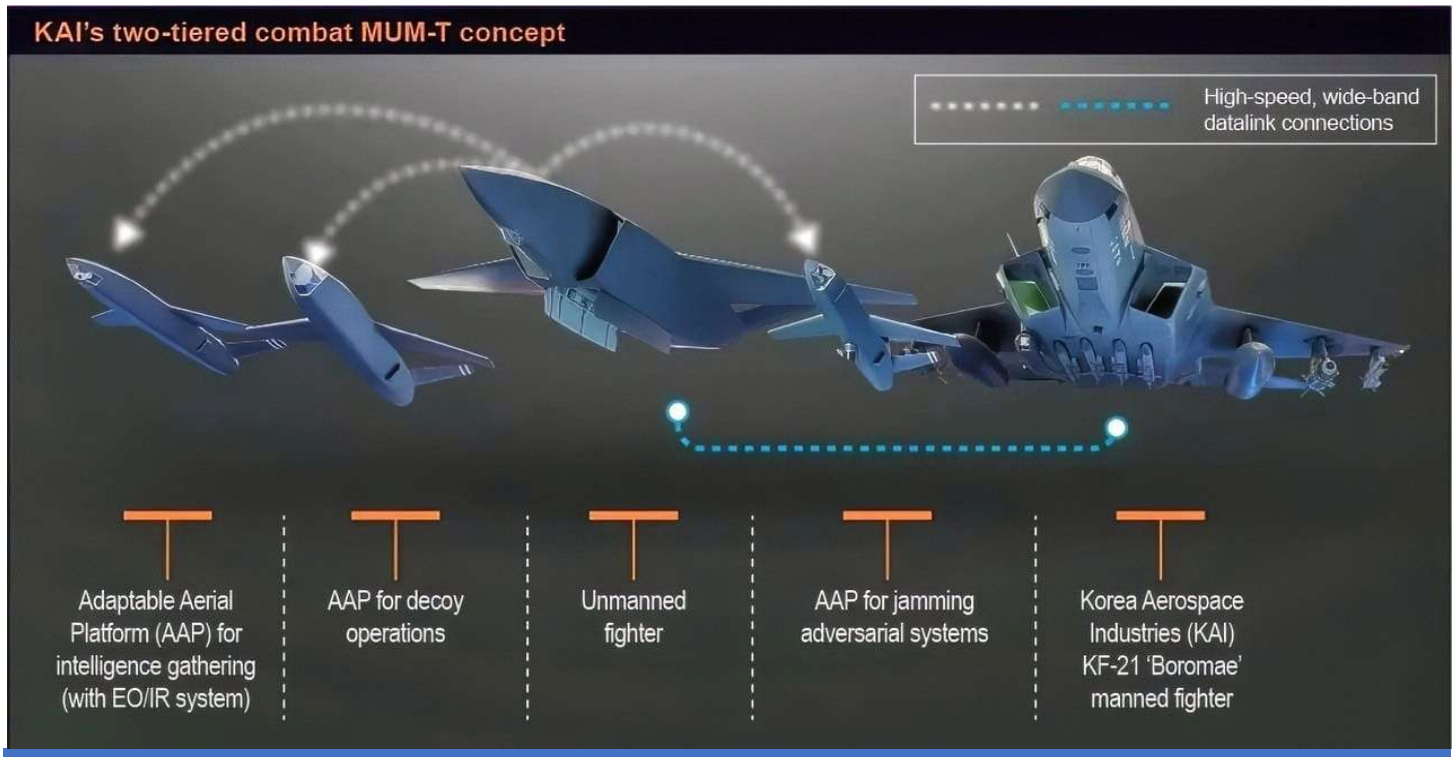
The weakest link in the SAMURAI Initiative is the deeply entrenched bureaucratic rigidity and delayed patch management characterising Japan's Self-Defense Forces (JSDF) networks.[xx] Under a unified cloud, if South Korea, India, or other regional partners link their proprietary tactical networks directly for the sake of "interoperability," they open a fatal backdoor for lateral movement.

Under the SAMURAI Initiative's proposed unified cloud model, participating partners are required to establish persistent, real-time data pipelines between their national tactical networks and the shared theatre cloud. South Korea's KF-21 mission computer telemetry—including flight envelope data, radar signature profiles, and potentially source code segments transmitted during over-the-air software update cycles—would, by design, traverse network segments topologically adjacent to JSDF-managed nodes. In network security terms, this adjacency eliminates the air gap that currently protects proprietary combat system code from external exposure. If JSDF-managed nodes within that shared environment are compromised, the absence of cryptographic segmentation between national network partitions means that an adversary with persistent access could conduct lateral reconnaissance across the shared fabric toward adjacent national segments—up to and including South Korea's KF-21 source code repositories and real-time telemetry of Indian maritime patrol assets.

*The weakest link in the **SAMURAI Initiative** is the deeply entrenched **bureaucratic rigidity** and delayed patch management characterising **Japan's Self-Defense Forces (JSDF)** networks*

The cascading implications of such a breach extend beyond the immediate loss of proprietary code. Once an adversary gains persistent access to the encryption matrices governing autonomous platform communications—whether UAV swarms, naval patrol drones, or AI-assisted targeting systems—the theoretical attack surface expands significantly. Security researchers studying the 2024 Incheon Airport incident[xxi] and the broader pattern of Lazarus Group intrusions have documented a consistent escalation pathway: initial network penetration, credential harvesting, and gradual lateral expansion toward high-value command-and-control nodes. In a worst-case scenario, and under the specific condition that encryption key management is centralised within the compromised cloud environment, a sophisticated state actor could potentially manipulate the command authentication layer of networked autonomous assets—effectively converting allied defence infrastructure into a vector for disruption against its own operators. This is not a prediction, but a structural risk that the proposed centralised architecture does not adequately mitigate.

*Once an adversary gains persistent access to the **encryption matrices** governing **autonomous platform** communications—whether **UAV swarms**, naval patrol drones, or **AI-assisted targeting systems**—the theoretical attack surface expands significantly*



TECHNICAL BLUEPRINT: "SOVEREIGNTY FILTERS" FOR DECENTRALISED GATEWAYS

Modern Tactical Edge Computing has fundamentally altered the calculus of battlefield data processing. Local combat nodes—whether an Indian Navy destroyer or a South Korean KF-21 fighter—can now execute heavy AI inference and sensor fusion computations directly at the point of engagement, without transmitting raw sensor data to a centralised overseas hub.

To justify demands for data centralisation, great-power planners consistently rely on the technical doctrine of the "Data Transmission Gap," arguing that a hyper-velocity modern battlefield cannot tolerate decentralised storage latency. This argument, while historically grounded in the latency constraints of legacy wide-area network architectures, has been progressively invalidated by the exponential maturation of Tactical Edge Computing. The U.S. Defense Advanced Research Projects Agency (DARPA)'s Distributed Battle Management programme and the NATO Edge Computing Reference Architecture (ECRA) have both demonstrated

that modern edge inference chips—such as NVIDIA's Jetson AGX Orin series deployed in forward-deployed naval platforms—are capable of executing complex AI-driven sensor fusion and targeting computations with sub-100 millisecond latency at the node level, without requiring round-trip data transmission to a centralised cloud.[xxii]

***South Korean KF-21** fighter—can **now execute heavy AI inference** and **sensor fusion** computations*

Furthermore, the operational performance of Ukraine's Delta battlefield management system—which employs a distributed, partially disconnected architecture—has empirically demonstrated that decentralised data processing does not materially degrade tactical decision speed under contested electromagnetic conditions.[xxiii] The Data Transmission Gap doctrine therefore reflects an outdated technical assumption, one that serves the institutional interests of centralised cloud vendors rather than the operational realities of the modern edge-enabled battlefield.

The meaningful expansion of sovereign cryptographic capacity for middle powers lies in the architecture of "Sovereignty Filters", which fuse "Tactical Edge Computing" with military-grade "Zero-Knowledge Proofs" (ZKP).[xxiv] ZKP allows an actor to generate a cryptographically verifiable proof of the validity and integrity of an information dataset without exposing any of the underlying raw data—subject to the computational overhead constraints that ongoing advances in hardware acceleration are progressively reducing.[xxv] Crucially, recent field deployments demonstrate that under

modern military-grade edge computing hardware, the computational overhead associated with generating these cryptographic proofs is sufficiently mitigated, reducing processing latency to sub-milliseconds and ensuring that ZKP integration preserves hyper-velocity allied interoperability without introducing operational delays.

Under this decentralised gateway architecture, India and South Korea must actively align with NATO to implement a standard where raw sensor signatures, radar logs, and proprietary AI algorithms are sealed securely behind their respective national firewalls. The ZKP engine on the edge node processes the raw data locally and generates an instantaneous, mathematically unforgeable proof. The Sovereignty Filter then transmits only the refined operational metadata, such as the finalised target coordinates, into the multinational cloud. This technical framework is designed to facilitate high-velocity allied interoperability while mitigating lateral cyber movement and safeguarding sovereign combat data from systemic extraction by foreign big-tech platforms.

*Under this **decentralised gateway architecture**, India and **South Korea** must actively align with **NATO** to implement a standard where raw sensor signatures, radar logs, and proprietary **AI algorithms** are sealed securely behind their respective national firewalls*

THE TRIPARTITE CORE AND NEW DELHI'S "DUAL-TRACK" QUAD STRATEGY

The implementation of this decentralised data architecture cannot rely solely on cryptographic engineering; it requires a robust, calculated alignment of geopolitical and industrial strategies. India's overarching national defence directive, *Atmanirbhar Bharat*, dictates absolute self-reliance in military technology to break free from foreign strategic dependencies. However, true self-reliance in the 21st century requires asserting normative power over the software and standards that govern the modern digital battlefield. As theorised by Snyder[xxvi] and empirically manifested in recent legislative mandates, regional powers must enforce strict "strategic conditions" onto defence integration schemes to preserve their sovereign independence.

***India** should remain an enthusiastic and highly proactive participant in the Quad's **Critical and Emerging Technologies (CET)** Working Group*

To operationalise this without causing a diplomatic rupture with Washington, New Delhi must implement a calculated, "Dual-Track" Strategy directly within the architecture of the Quadrilateral Security Dialogue (Quad). Under Track One, India should remain an enthusiastic and highly proactive participant in the Quad's Critical and Emerging Technologies (CET) Working Group, engaging fully in non-military tech supply chain diversification, telecommunications resilience, and semiconductor collaboration.

However, under Track Two—which governs active multi-domain operational data exchange—New Delhi must enforce an unyielding defensive boundary. India must flatly refuse to feed its frontline data into the centralised U.S.-Japan SAMURAI platform. Instead, New Delhi should legally and technically mandate the Sovereignty Filter framework as the non-negotiable standard for all Quad maritime and aerial surveillance synchronisation.

To anchor this strategy, India must widen its geopolitical leverage by forging a NATO-India-South Korea tripartite defence supply chain. This tripartite matrix operates on an equal, peer-to-peer, consent-based model, replacing the current hub-and-spoke dependency with a sovereignty-preserving security architecture:

- **India's Emerging Software Capacity (Bangalore)**: India's candidacy for ZKP cryptographic protocol development rests on a demonstrable technical foundation. Bangalore's defence-tech ecosystem—anchored by DRDO's Centre for Artificial Intelligence and Robotics (CAIR)[xxvii], the

Indian Institute of Science (IISc), and iDEX-affiliated deep-tech startups[xxviii]—has demonstrated expanding capabilities in secure communications and cybersecurity protocols. The Government of India's 2023 National Quantum Mission[xxix] further prioritises post-quantum cryptography and quantum key distribution, with significant dual-use defence implications. Provided that institutional coordination between DRDO, the private sector, and allied standards bodies is formalised through the tripartite framework, India's defence-tech clusters are strategically positioned to anchor the cryptographic software layer of the proposed Sovereignty Filter architecture.

- **South Korea's Advanced Hardware Manufacturing (Sacheon)**: Anchored by its defence manufacturing hub in Sacheon—home to Korea Aerospace Industries (KAI) and Hanwha Systems—South Korea contributes advanced hardware capabilities including the KF-21 Boramae platform, tactical edge computing modules, and precision munitions systems to the tripartite network, while preserving autonomous command over its primary security theatre on the Korean Peninsula.

- **NATO's Continental Autonomy and Standards (Brussels)**: European NATO members, facing production attrition, gain access to South Korea's robust production lines and India's secure software.[xxx] In return, Brussels shares the consent-based, metadata-only principles of the STANAG 4586 protocol, granting India and South Korea the normative leverage to demand a decentralised data framework from the United States.[xxxi]

CONCLUSION: CONSENT-BASED SECURITY COOPERATION VS. DIGITAL SUBJUGATION

The structural warning echoed across contemporary intelligence and defence debates is an existential reality for the future of middle powers: those who yield to centralised data structures under the guise of allied efficiency create structural incentives to trade their national sovereignty for digital vassalage.[xxxii] India, South Korea, and European NATO nations stand at an identical historical crossroads. Their path to survival lies neither in total geopolitical isolation nor in submissive assimilation as mere subsystems of a foreign hegemon.

The geopolitical pressures documented in this analysis—from the Ankara Declaration's data locality precedent to Teodoro's operational decoupling—suggest that consent-based security cooperation is not merely a normative aspiration but an emerging operational necessity for middle powers seeking durable alliance participation on sovereign terms. By deploying military-grade Zero-Knowledge Proofs and Tactical Edge Computing as the technical foundation of a standardised, tripartite supply chain network, New Delhi, Seoul, and Brussels can demonstrate to the international community that robust allied operational cohesion does not require the sacrifice of national data borders.[xxxiii] Each jurisdiction must consistently assert its independent voice, its defence infrastructure, and its technological parameters. By establishing decentralised gateways governed strictly by mutual consent, this tripartite coalition offers a replicable model—demonstrating that robust allied security cohesion is achievable not through structural subordination to a single centralised architecture, but through the deliberate construction of a consent-based, decentralised framework in which sovereign nations participate as equal and autonomous partners.

[1] NATO, 'The Ankara Summit Declaration', *NATO Official Texts*, 8 July 2026, https://nato.int, accessed 29 July 2026.

[3] European Policy Centre (EPC), 'Annotated 2026 NATO Summit Declaration: Reading Between the Lines', *EPC World Programme*, 9 July 2026, https://epc.eu, accessed 29 July 2026.

[4] B. Glosserman, 'Peak minilateralism: The rise of lattice-like security networks in the Indo-Pacific', *Pacific Forum PacNet*, No. 34, 2024.
[5] S. Shaukat, 'America's Managed Retreat: How the 2025 U.S. National Security Strategy Shifts the Burden to Allies', *Global Security Review*, 10 February 2026, https://globalsecurityreview.com, accessed 29 July 2026.
[6] NATO, *supra* note 1.
[7] EPC, *supra* note 3.

[8] NATO, *supra* note 1.
[9] EPC, *supra* note 3.

[10] NATO, *supra* note 1.
[11] Glosserman, *supra* note 4.

[12] US Senate Select Committee on Intelligence, *Intelligence Authorisation Act for Fiscal Year 2027*, S. 4615, 119th Cong., Sec. 691, June 2026.

[xii] M. Sato, 'Japan broadened "one-Theatre" concept to U.S. for Indo-Pacific', *The Asahi Shimbun*, 15 April 2025.
[xiii] Glosserman, *supra* note 4.

[xiv] G. C. Teodoro, Jr., 'Operationalising the Comprehensive Archipelagic Defence Concept', *Armed Forces of the Philippines Public Affairs*, 29 May 2026.
[xv] G. H. Snyder, 'The security dilemma in alliance politics', *World Politics*, vol. 36, no. 4, 1984, pp. 461–495.
[xvi] S. J. Yoon, 'North Korean non-kinetic attacks: A problem for Incheon Airport', *38 North*, 8 November 2024, https://38north.org, accessed 29 July 2026.

[xvii] B. Lin et al., 'CRINK security ties: Growing co-operation, anchored by China and Russia', *Center for Strategic and International Studies (CSIS)*, 30 September 2025, https://csis.org, accessed 29 July 2026.

[xviii] *Ibid.*
[xix] J. S. Bermudez and J. Jun, 'North Korean Strategic UAV Activity at Panghyon Airbase', *Beyond Parallel, Center for Strategic and International Studies (CSIS)*, 1 April 2025, https://csis.org, accessed 29 July 2026.
[xx] Yoon, *supra* note 17.; Bermudez and Jun, *supra* note 19.

[xxi] Yoon, *supra* note 17.
[xxii] DARPA, 'Distributed Battle Management Programme', *Defence Advanced Research Projects Agency*, 2024, https://drdo.gov.in, accessed 29 July 2026.

[xxiii] J. Watling and N. Reynolds, 'Meatgrinder: Russian tactics in the second year of its invasion of Ukraine', *Royal United Services Institute (RUSI)*, 2024, https://rusi.org, accessed 29 July 2026.

[xxiv] DARPA, *supra* note 23.; NATO NIFC, 'NATO Edge Computing Reference Architecture (ECRA)', *NATO Information and Communications Agency*, 2025, https://nato.int, accessed 29 July 2026.

[xxv] DARPA, *supra* note 23.
[xxvi] Snyder, *supra* note 16.
[xxvii] DRDO, 'Centre for Artificial Intelligence and Robotics (CAIR)', *Defence Research and Development Organisation*, 2024, https://drdo.gov.in, accessed 29 July 2026.

[xxviii] Ministry of Defence, Government of India, *iDEX Annual Report*, Defence Innovation Organisation, 2023, https://idex.gov.in, accessed 29 July 2026.

[xxix] CCEA, 'Cabinet approves National Quantum Mission', *Press Information Bureau, Government of India*, 19 April 2023, https://pib.gov.in, accessed 29 July 2026.

[xxx] M. F. Cancian and C. H. Park, 'The 2026 national defense strategy by the numbers: Radical changes, moderate changes, and some continuities', *Center for Strategic and International Studies (CSIS)*, 27 January 2026, https://csis.org, accessed 29 July 2026.

[xxxi] NATO, *supra* note 1.

[xxxii] NATO, *supra* note 1.; Yoon, *supra* note 17.

[xxxiii] NATO, *supra* note 1.; Watling and Reynolds, *supra* note 24.