NATO Hybrid Partnerships & Networked Security

29 NOVEMBER 2025

Eleonora Crespi



Beyond the Alliance: How NATO is Reinventing Cooperation through Hybrid Partnerships and Networked Security

1. Introduction: From Alliance to Network

The shifting security landscape of the past few years – from the war in Ukraine to rising tensions in the Indo-Pacific – has pushed NATO to rethink the limits of its traditional, treaty-bound structure. The 1949-conceived Alliance now operates in a world where threats are no longer confined by

geography or formal alliances: cyberattacks, disinformation campaigns, and maritime disputes transcend borders with ease, revealing the inadequacy of rigid institutional boundaries in an era of fluid, interconnected security. This evolving pattern reflects the recognition that today's security challenges are transnational and cannot be contained within fixed geographic or institutional borders. In this context, NATO's expanding network of partnerships represents more than pragmatic adaptation: it is a testing ground for a hybrid model of cooperation that blends the credibility of a formal alliance with the flexibility of ad hoc coalitions.

Increasingly, the Alliance engages with non-member partners such as Australia, Japan, South Korea, and Colombia – the so-called Indo-Pacific Four (IP4) – integrating them into operations, exercises, and policy coordination without extending full and formal membership.

Through its Partners Across the Globe framework, NATO has institutionalised this outreach, enabling cooperation with distant partners on missions, training, and strategic dialogue while avoiding the political and legal complexities of enlargement. The partnership with Australia is emblematic: Canberra has contributed to NATO-led operations in Afghanistan and maritime security missions, demonstrating how collaboration can deepen even outside the boundaries of formal accession.

Examining this shift reveals how NATO is positioning itself for an era of fluid, interconnected threats while raising crucial questions about legitimacy, decision-making, and strategic coherence.

2. Beyond Article 5: Redefining Cooperation

2.1. The Limits of the Traditional Model

For most of its history, NATO's strength and power lay in its simplicity: the mutual defence clause – Article 5 – which offered certainty, deterrence, and trust. Yet this clarity came with rigidity, in this way confining the Alliance both geographically to the North Atlantic area and institutionally to its signatories.

In the 21st century, however, that framework has grown increasingly inadequate, as security has become globalised, multidimensional and, mostly, unpredictable: for instance, cyberattacks can cripple a member's infrastructure without crossing borders; while disinformation campaigns can target societies from thousands of kilometres away. NATO's original mechanisms were clearly never designed for such diffuse and hybrid threats, forcing the Alliance to adapt beyond its conventional architecture.

2.2. Partners Across the Globe: From Defence to Resilience

In response, NATO has established the Partners Across the Globe framework – a mechanism allowing cooperation with non-member countries based on one common ground: shared security and strategic concerns.

Through Individual Partnership and Cooperation Programmes (IPCPs), the Alliance engages partners in training, joint missions and technology exchanges without extending formal membership and, indirectly, the deriving obligations.

Australia's participation exemplifies this approach, as Canberra's involvement in NATO-led operations in Afghanistan and in maritime security initiatives apparently illustrates how collaboration can evolve outside the boundaries of accession. These partnerships highlight mainly a conceptual transition: from collective defence to collective resilience. This means NATO is no longer only guarding borders; it is indeed strengthening systems, capabilities, and norms. The Alliance is becoming not a gatekeeper of security, but more a convener of capacities and a hub that connects rather than confines.

3. The Indo-Pacific Connection

The so-called Indo-Pacific Four (Japan, South Korea, Australia, and New Zealand) represent NATO's most dynamic set of external partnerships. Although geographically distant, these states share NATO's democratic values and its concerns about strategic instability, particularly regarding China's growing assertiveness and North Korea's accelerating militarisation.

As the Indo-Pacific gradually becomes the world's geopolitical and geoeconomic epicentre, both states and regional organisations have begun to pivot toward it: for NATO and its members, engagement in the region reflects a combination of strategic, economic, and normative drivers – from U.S. pressure and alliance coordination to market opportunities and shared security concerns. This pivot has intensified cooperation between European and Indo-Pacific actors under Washington's broader leadership, though recent transatlantic tensions, particularly over burden-sharing and the war in Ukraine, are testing this alignment.

Within this evolving environment, NATO's Indo-Pacific partnerships embody both opportunity and constraint, as the IP4 are all formal U.S. allies, but their priorities and capacities vary:

Recent years have thus seen a surge in concrete and diversified collaboration, as:

These are not isolated initiatives but components of what analysts describe as a networked security architecture (Wilkins, 2023): a web of like-minded partners connected by shared values and interoperable systems rather than by binding treaties. Through this network, NATO extends its influence without extending its borders, bridging the Euro-Atlantic and Indo-Pacific theatres.

At the same time, the geopolitical balance underpinning these partnerships remains fragile, and this can apparently be witnessed in the 2° Trump administration, which is less aligned with traditional U.S. foreign policy pillars, raising uncertainty about Washington's role in coordinating transat-

lantic and Indo-Pacific security. This, combined with Europe's growing awareness of the region's strategic and economic significance, is gradually prompting European actors to adopt a more active Indo-Pacific posture. For NATO, this dual dynamic could evolve into a new form of "triangular cooperation", (Patalano & Locatelli, 2025) in which European, Indo-Pacific, and North American partners seek to maintain stability amid a more fragmented international order.

Ultimately, NATO's engagement in the Indo-Pacific is not about enlargement or projection of power, but about relevance: it represents an attempt to shape the evolving global security architecture by linking democracies across regions, ensuring that the Alliance remains not only a Euro-Atlantic actor, but a global connector.

4. Cyber Cooperation as a Laboratory for Hybrid Models

4.1. The Digital Domain: A Common Ground

Among all emerging domains, cyberspace best illustrates NATO's hybrid model in practice: digital threats are inherently transnational and challenge the very idea of territorial defence. Indeed, they demand rapid coordination, information exchange, and innovation – qualities that rigid alliance structures struggle to sustain.

4.2. The Tallinn Case Study

The Cooperative Cyber Defence Centre of Excellence (CCDCOE) in Tallinn epitomises NATO's transformation from a territorial alliance to a networked security actor. The idea for such a centre predates Estonia's NATO membership: as early as 2003, Tallinn proposed the creation of a cyber defence hub to address emerging digital vulnerabilities. The 2006 Riga Summit had already listed cyberattacks among the "asymmetric threats" to collective security and called for long-term programs to strengthen information systems protection.

A year later, in 2007, Estonia suffered a series of unprecedented cyberattacks that paralysed its government, banking and media infrastructure: these events marked a turning point for NATO, revealing that digital networks had become the new frontline of collective defence. In the wake of these attacks, the Alliance, with strong support from then–Secretary General Jaap de Hoop Scheffer, approved a comprehensive NATO Policy on Cyber Defence in January 2008, followed by the official decision at the Bucharest Summit to establish a capability «to assist allied nations, upon request, to counter a cyberattack.» (Staff Writers, SpaceWar, 2008).

As General James Mattis stated shortly before its creation (Brussels, 14 May 2008):

«The need for a cyber-defence centre to be opened today is compelling.

It will help NATO defy and successfully counter the threats in this area.»

Established in Tallinn later that year, the CCDCOE has since evolved into NATO's premier hub for cyber research, training, and joint exercises. It is one of 21 accredited Centres of Excellence (COEs) operating under NATO's Allied Command Transformation, funded through a mix of national and multinational contributions: its founding members (Estonia, Germany, Italy, Latvia, Lithuania, Slovakia, and Spain) were soon joined by over twenty additional nations, including France, the United Kingdom, the United States, and several non-NATO countries. The centre's open membership policy has enabled the participation of partners such as Austria, Finland, Ireland, and, more recently, South Korea (2022) and Japan (2022), making it a genuinely transatlantic and transregional platform.

The CCDCOE's mission extends well beyond training. It serves as a hub for interoperability within NATO's Network Enabled Capability (NNEC) environment, advancing doctrine development, operational testing, and legal analysis in the field of cyber defence. Its activities include (Tarien, 2018):

Within this framework, partners contribute analysts, technical expertise, and funding to collective projects that range from threat intelligence and capacity-building to the exploration of the legal and ethical dimensions of digital conflict. The 2022 admission of Ukraine as a contributing participant – only months after Russia's invasion – underscored the centre's growing role as a bridge between NATO and its wider strategic ecosystem.

The Tallinn model demonstrates how effective security cooperation can emerge through functional integration rather than institutional accession. By anchoring collaboration in shared expertise and joint simulations, NATO has transformed the cyber domain into a laboratory for hybrid diplomacy – a setting where traditional boundaries between member and partner fade in favour of operational interdependence. In this space, solidarity is not declared through treaties, but demonstrated through practice: by testing, training, and trusting together.

5. Strategic Challenges and Political Dilemmas

5.1. The Question of Authority

NATO's hybrid partnerships, while innovative, raise profound questions about authority and legitimacy: non-member partners increasingly contribute troops, funding, and expertise, yet remain excluded from collective decision-making. This asymmetry can generate perceptions of "second-tier" participation (Fasola, 2024), weakening the sense of shared ownership on which alliances depend.

As highlighted in several NATO's statements (AC24 Compendium, 2024), one of the key strategic challenges lies in defining "appropriate influence"

for partners that participate in missions without the political rights of membership, denoting that this imbalance risks producing a gap between operational contribution and institutional voice. For NATO, maintaining inclusivity without eroding its decision-making autonomy thus remains a delicate balancing act – one that tests the very grammar of collective security in an era of networked cooperation.

5.2. Accountability and Oversight

Democratic accountability represents another sensitive frontier, as NATO's legitimacy rests not only on its capabilities but also on its identity as a community of democracies. Yet, the warning is that expanding defence cooperation without proper oversight "may weaken rather than strengthen security" (Grandi, 2025), especially when democratic standards among partners differ.

When operations involve both member and non-member states, the chain of accountability becomes blurred: who bears political responsibility if a joint cyber operation fails, escalates, or breaches international law? These ambiguities risk undermining NATO's normative credibility, deriving from the idea that it not only protects democracy but also practises it through transparent decision-making and civilian control. To address this, analysts recommend reinforcing parliamentary scrutiny mechanisms and harmonising reporting standards across the partnership frameworks, ensuring that hybrid cooperation does not evolve into democratic exceptionalism.

5.3. Strategic Coherence

Expanding partnerships also complicates NATO's strategic coherence: the proliferation of frameworks – from the Partners Across the Globe initiative to enhanced bilateral ties – has created overlaps and inefficiencies that can dilute strategic priorities. Each partnership adds flexibility but also complexity, particularly when partners pursue their own regional agendas or maintain parallel commitments with other institutions. This can be identified as one of NATO's major dilemmas: the risk that "quantity substitutes for quality" in partnership management (Fasola, 2024). Without a unified assessment mechanism or clear prioritisation, the Alliance risks turning its cooperative network into a patchwork of uncoordinated engagements.

At the same time, external perception matters, as closer coordination with Indo-Pacific partners has already drawn criticism from Beijing and Moscow, which frame NATO's outreach as an attempt to "globalise containment" (MOFA China, 2022-2024) While this misrepresents the Alliance's intent, it illustrates the geopolitical sensitivity of hybrid cooperation and the need for NATO to communicate its strategy consistently, avoiding the impression of strategic drift.

5.4. Balancing Openness and Integrity

We can understand that, ultimately, NATO's challenge lies in reconciling openness with integrity: the Alliance must evolve from "crisis-driven adaptation to structure-driven resilience" (Fasola, 2024). This requires institutionalising cooperation in a way that preserves cohesion, clarifies commitments, and maintains public trust. Too much rigidity risks irrelevance in a fast-moving strategic environment; too much openness risks fragmentation and incoherence. The future of NATO's credibility will depend on its ability to strike this equilibrium, ensuring that hybrid partnerships strengthen rather than dilute the Alliance's collective identity and strategic purpose.

6. Conclusion: A New Grammar of Cooperation

NATO's hybrid partnerships reflect more than pragmatic adjustment; they embody a deeper transformation in how international cooperation is conceived. The Alliance is evolving from a closed club of treaty-bound members into a flexible network of shared capabilities and trust.

By blending the structure of formal alliances with the adaptability of ad hoc coalitions, NATO is sketching the contours of a new diplomatic order. Its emerging model suggests that in a world of diffuse threats, collective security must be defined not by geography, but by connection.

This is not the end of the Alliance model: it is through its reinvention. NATO's partnerships with non-member states show how old institutions can learn the language of a networked world, where cooperation depends less on belonging and more on contribution. If this experiment succeeds, it could redefine not only NATO's future, but the very grammar of global diplomacy.

Lastly, NATO's reinvention reminds us that true strength emerges not from rigid walls, but from flexible bonds that adapt as the world shifts beneath them. In such a networked age as the one we're living in, contribution matters more than belonging; security is a web of collaboration, spun by those willing to act beyond the lines that divide them.

References

Abbondanza G., NATO-Europe-US Cooperation in the Indo-Pacific: Challenging Times Ahead, Istituto Affari Internazionali (Mar. 14, 2025) https://www.iai.it/en/pubblicazioni/c05/nato-europe-us-cooperation-indo-pacific-challenging-times-ahead

CCDCOE, About us, CCDCOE official website https://ccdcoe.org/about-us

Chinese Ministry of Foreign Affairs, MOFA, Foreign Ministry Spokesperson Wang Wenbin's Regular Press Conference on May 12, 2023, May 2023

Fasola N., Reforming and Enhancing Partnerships to Strengthen NATO's Strategic Posture, Parameters 54, n. 4, 2024

Grandi F., Expanding Defence Spending without proper accountability could weaken rather than strengthen security Civicus Lens, 2025

Grgic G., How NATO and its Indo-Pacific partners can work together in an era of strategic competition, Atlantic Council (Aug. 7, 2024) https://www.atlanticcouncil.org/blogs/new-atlanticist/how-nato-and-its-indo-pacific-partners-can-work-together-in-an- era-of-strategic-competition/

Hooker R. D., Hybrid Warfare and NATO, NATO Defence College Foundation

Iskandarov K. & Gawliczek P., NATO's New Force Model and Partner Engagement in an Evolving Security Landscape, Journal of Scientific Papers Social development & Security (Apr. 15,2025) https://www.researchgate.net/profile/Khayal-Iskandarov/publication/391523041_NATO%27s_New_Force_Model_and_Partner_Engagement_in_an_Evolving_Security_Landscape_Nova_model_sil_NATO_ta_vzaemodia_partneriv_u_umovah_minlivogo_bezpekovogo_landsaftu/links/681b861cdf0e3f544f5296ec/NATOs-New-Force-Model-and-Partner-Engagement-in-an-Evolving-Security-Landscape-Nova-model-sil-NATO-ta-vzaemodia-partneriv-u-umovah-minlivogo-bezpekovogolandsaftu.pdf?origin=publication_detail&_tp=eyJjb250ZXh0Ijp7ImZpcnN0UGFnZSI6InB1YmxpY2F0aW9uIiwicGFnZSI6InB1YmxpY2F0aW9uRG93bmxvYWQiLCJwcmV2aW91c1BhZ2UiOiJwdWJsaWNhdGlvbiJ9fQ

NATO, Multinational capability cooperation (Jul. 30, 2025) https://www.nato.int/cps/en/natohq/topics_163289.htm

NATO, Relations with Partners in the Indo-Pacific Region (Oct. 24, 2024) https://www.nato.int/cps/el/natohq/topics_183254.htm

NATO, Statement between NATO Secretary General and the four Indo-Pacific partners, NATO Summit in The Hague (Jun. 25,2025)

Pugliese G, "How to Facilitate NATO-IP4 Defense Industrial Cooperation: The Case of Italy and Japan", in Liselotte Odgaard (ed.), Moving the NATO-IP4 Partnership from Dialogue to Cooperation Maritime Security and Next- Generation Technologies, Washington, Hudson Institute (Mar. 2025)

Staff Writers, NATO launches cyber defence centre in Estonia, SpaceWar (May 2008)

Patalano A. & Locatelli A., NATO-Europe-US Cooperation in the Indo-Pacific. Challenging Times ahead, IAI Papers 2025, Mar. 2025

R. Inoue, Why the security of Asia and Europe are inseparable, The Japan Times (October 2024)

Tarien T., NATO CCDCOE – Expertise and cooperation make our cyber space safer, e-Estonia (Oct. 2018) https://e-estonia.com/nato-ccdcoe-expertise-cyber-space-safer/

Wilkins T., "A Hub-and-Spokes 'Plus' Model of US Alliances in the Indo-Pacific: Towards a New 'Networked' Design", in Elena Atanassova-Cornelis Yoichiro Sato and Tom Sauer (eds), Alliances in Asia and Europe. The Evolving Indo-Pacific Strategic Context and Inter-Regional Alignments, London, Routledge (2023)

DOI 10.69790/epis-rep-ird-1/20379