By Centre for
Diplomacy and
Innovation

January 2026

NATO-INDIA RELATIONS

Advancing Joint Actions Through Complementarity and Dialogue

NATO-INDIA RELATIONS

Advancing Joint Actions Through Complementarity and Dialogue

Giulia Casot
Junior Researcher
Mondo Internazionale APS

Ishan Sinha
Research Associate
The Geostrata

Anshika Malik
Research Associate
The Geostrata

Nandita Lata
Research Associate
The Geostrata

Chiara Merlin
Deputy Director
Mondo Internazionale APS

Rosa Santa Serravalle
Senior Researcher
Mondo Internazionale APS

Dia Atal
Junior Researcher
The Geostrata

Sharon Giacomelli
Junior Researcher
Mondo Internazionale APS

Francesco Oppia
Editor-in-Chief
Mondo Internazionale APS

Valeria Picciolo
Editor-in-Chief
Mondo Internazionale APS

Contents

01-02
Prologue

03-11
Strategic Autonomy and Defence

12-19
Cooperation in Space Warfare

20-31
The Indo-Pacific Dimension of
NATO'S Counter-Terrorism Strategy

32-39
Securing Cyberspace Across Borders

40
Concluding Remarks

41-45
References

To download the full report,
visit: thegeostrata.com

PROLOGUE

Despite India not being a NATO ally, the shared values of freedom, democracy, sovereignty, human rights widened the scope of NATO-India cooperation.

NATO-India relations have evolved significantly into a global defence and political importance. In an ever-evolving global trend marked by realignment and cataclysmic effects of globalisation, the participatory framework of partnerships with non-member states from different geographical regions shape the democratic and security interests of nations beyond the transatlantic community. The relations between NATO and India goes back to the events of '9/11', shaping the dialogue for countering the non-traditional security threats. On the sidelines of the India-NATO dialogue in 2009, in New Delhi, the former Deputy Head of the NATO Secretary General's Policy Planning Unit, Michael Ruhle, stated that the incident shaped the alliance's views in effectively dealing with new security threats in the globalising world.[1]

Despite India not being a NATO ally, the shared values of freedom, democracy, sovereignty, human rights widened the scope of NATO-India cooperation.[2] With India's major strides in missile technology, space capabilities, along with growing capabilities on satellite surveillance, the scope for fostering effective cooperation with international security organisations like NATO becomes vital in preserving the regional and global security interests. NATO's expertise in facilitating the latest innovation in advanced technology, interoperability skills can benefit India in expanding its defence capabilities to counter asymmetric regional and global threats. Additionally, India can aid NATO member countries and allies to expand its defence capabilities and technological advancements through cost-effective approach.

Similar positions of common security threats also surfaced in March 2025 during the inaugural NATO-India Youth Conference, organised by The Geostrata, in collaboration with the NATO Public Policy Division, Embassy of the Netherlands, and the Konrad-Adenauer-Stiftung (KAS).[3] This report intends to explore areas where India and NATO-member countries can collaborate to expand its capacity, advance technological relations and cooperation to ensure regional and global security threats in the face of aggravating global threats.

Strategic Autonomy and Defence

India's Roadmap in Indigenous Defence Development

India became a nuclear power in 1974 and evolved its policy towards the U.S. and the Soviet Union.

Introduction:

The non-aligned approach adopted by the Indian authorities during the Cold War continues to drive current choices of national impact. Seventy years since the contestations between the U.S. and the Soviet Union, nuclear weapon systems continued to shape their spheres of international and regional influence. India became a nuclear power in 1974India tested its nuclear capabilities in 1974 and became a full-fledged nuclear power in 1998 and evolved its policy towards the U.S. and the Soviet Union.[4] The pariah condition the latter is put under by Western countries since the start of its aggression against Ukraine in February 2022, brought India closer to the U.S. and NATO. Therefore, this article intends to understand India's quest for indigenously developing military equipments and highlight its roadmap as the net exporter of advanced technologies.

Strategic Autonomy and India’s Shifting Geopolitical Alignments

American administrations welcomed the shift since the 2000s under the Bush presidency, showing bipartisan support towards defence and security cooperation. During Trump’s first presidency, India was attributed the unique status of ‘Major Defence Partner’ in June 2016 and was cited in the U.S. Indo-Pacific Strategy of 2019 among the pivotal American allies in the region.[5] It was then labelled as one of ‘our closest friends’ by the then U.S. President Biden in 2021. With the rising tensions with China in the Indo-Pacific region, India reinforced its position as a maritime power in the border and naval clashes, calling for reinforced, reliable alliances. These declarations hint at the will for stronger ties between the two powers to accelerate the integration and modernisation of defence industries. It resulted in fostering co-production of fighter jet engines and armoured vehicles; however, scholars question whether this alone is sufficient to ensure reliable U.S.–India relations, particularly in light of the Trump administration’s emphasis on encouraging partners to take greater responsibility for their own defence, alongside India’s enduring pursuit of strategic autonomy.

Missile Diplomacy and the Pursuit of Indigenous Capability

This cautious approach is apparent in the realm of missile diplomacy, namely, the use of missile production, supply, and technology sharing as a diplomatic instrument. On the one hand, the United States' primary strategic focus remains countering China; beyond this, its attention may gradually shift toward strengthening defence capabilities in other regions and partnerships. Trump's recent threat to increase tariffs on Indian goods imports if the country continues buying Russian oil represents a warning in this regard. On the other hand, India keeps emphasizing realistic diplomacy and national interest advancements through multiple engagements in missile production and sales, with respect to the 'Make in India' policy. The consequent Indian leapfrog in defence and security-related investments reinforced risk-taking policy, nationalist sentiment (Bharat-first), and deference to 'Vishwaguru' tenets or "the greater the risk, the greater the return."

In practical terms, those investments led the Indian research body to develop the Akash surface-to-air missile system, whose manufacturing[6]technical aspects are from the competence of Bharat Dynamics Ltd (BARA.NS). The national company cooperates with the Defence Research and Development Organisation (DRDO) and foreign Original Equipment Manufacturers (OEMs), supplying missiles and equipment to the Indian Armed Forces, including product life cycle support and refurbishment. It also exports selected defence equipment and joins strategic alliances with public and private sector companies, particularly appreciative of the Akash missile system capacity of travelling at supersonic s[7]peeds, engaging with up to 64 targets reaching 18,000 meters of altitude, and detonating 60 kilograms of explosives in proximity of the target, while resisting jamming.

Expanding Defence Partnerships Through Multi-Stakeholder Engagement

Reflecting growing international confidence in India's indigenous air defence capabilities, in early 2025, Armenia and the Philippines paid more than USD 200 million to purchase the Akash system.[8] For India, both deals prove it is gaining international trust as a 'global teacher' and reliable partner, making defence accessible to smaller nations looking for affordable security to foster worldwide increased collaboration and stability. Within the frame of a five-year defence structure and strategy renovation, the Philippines already bought USD 375 million worth mid-range BrahMos supersonic cruise missile in 2022, a significant milestone for the Indian authorities that already exported this military technology to Israel in 2017, compliant to the national multipartner strategy.[9] India is implementing the 'Make in India' initiative launched by Prime Minister Modi in 2014 to boost multinational and national companies' production in the Middle Eastern country through the government company, Bharat Electronics Ltd (BEL). For this reason, the Israel Aerospace Industries (IAI) received a USD 630 million worth of contract to supply long-range surface-to-air missile (LRSAM) defence systems for the Indian Navy.[10]

Technology Transfer, Industrial Ambitions, and the Limits of Self-Reliance

The 'Make in India' policy was proposed in 2020 under the label 'Self-Reliant India' to support Indian manufacturers by creating 'good force multipliers' and turning the country into a global supply chain hub, among others. In the defence sector, Indian authorities translated this goal into a USD 277 million-worth contract signed between the Ministry of Defence and BEL to enhance the indigenous production of Electronic Warfare Suites and other arms gear for the Indian Air Force.[11] The Indian government reinvests revenues from arms and ammunition exports in research and development in defence and security, fueling a virtuous cycle tailored to boost the nation's technological development and innovation.

In this regard, the country is also taking advantage of the reinforced relationship with the U.S., which opens technology sharing and strategic know-how. This cooperation benefits the Americans as well, ensuring that the Indian ally aligns the technological expertise of other pivotal actors for the defence of the U.S. interests in the Indo-Pacific countries, such as Australia and Japan, in the Quadrilateral Security Dialogue. Most notably, the American administration aims at countering the Chinese quest for regional and global leadership and believes that an economically strong India, featured by improved skills and a developed labour market through national exports in high-value industries such as defence, can successfully help to hinder the rise of China.

The increased focus on national independence in defence and security is also not sufficient to ensure India will win anytime soon in the race for indigenous freedom. Its defence equipment export totalled USD 2.40 billion in the fiscal year ending in March 2024, surging up to 150% since 2020, but this share cannot be compared to arms and ammunition exports to Australia, South Korea, and China.[12] Further, the country remains the main recipient of arms exported by France, Russia, and Israel, ranking second place on global importers after Ukraine. A main driver behind this dynamic can be identified in the rising tensions with both China and Pakistan, further marred by China's rising arms export to the Pakistani government, up to 81% in 2020-2024 from 74% in 2015-2019.[13]

Defining Narratives Beyond Borders

For the Indian Aerospace and Defence Sector to ever be able to shape global narratives in military technology innovation, it needs to stand on three prerequisites – quality, reliability, and accessibility. By striving to achieve international standards of quality set in stone by the global standards set by NATO STANAGs, United States' MIL-STD, and the European Defence Agency's guidelines, Indian products can become dominant entrants in a market where defence capabilities need to excel consistently. Establishing a rapport defined by reliability of production, durability of products, and after-sales support is critical to forge a place in international arms markets. Indian producers, especially the DPSU's that are otherwise known for bureaucratic delays and operational inefficiency, must work on building a brand of trust and excellence. It was not until very recently, in the HAL-Safran deal for LEAP engine co-development, that ToT was accompanied by transfer of critical IP and source codes.

International collaborations will continue to yield limited results as far as bolstering indigenous production through ToT is concerned, unless full access to source codes, IP, and design autonomy becomes the norm. Moving from the licensing model of collaboration to models of co-development, similar to the India-France partnership, is crucial for a country striving to create global ripples. Military technologies are becoming increasingly oriented towards the use of low-cost, tech-intensive solutions to destroy high-cost strategic assets and military capabilities. India, with its academically-oriented workforce in the defence sector, must co-create doctrines, bring academic, governing, and producing stakeholders on the same temporal and strategic plane, and incorporate technologies that are not simply disruptive by their very nature but also enable the development of such technologies.

From Global Insights to Local Strategy- Incorporating Best Practices

The United States, during the First and Second World Wars, had a well-oiled machine for defence production called the Military Industrial Complex. In fact, as far back as in 1996, the U.S. Department of Defence signed a contract for the initial concept development of the Joint Strike Fighter with Lockheed Martin and Boeing. Each was awarded USD 750 million for design and development, while prohibiting the companies from using internal sources of financing for the adoption of low-cost manufacturing and assembly techniques. In 2001, Lockheed Martin's X-35 beat the Boeing X-32, thereby bagging the eventual contract.[14] This system was rooted entirely in state funding for R&D, low-cost production techniques, and metrics that awarded capability and competence. Chinese defence production runs along the Military-Civil Fusion. The strategy, while being an embodiment of the very scale of integration that India currently lacks, is rooted in the concept of dual-use technologies. While civilian innovations in AI, quantum computing, and biotechnology are being rapidly integrated into defence use, the PLA remains the foreman of disruptive capabilities.

Beijing institutionalised the very idea of aligning state policy, industry mandates, and academic depth by placing the MCF Development Commission under the direct ambit of the Central Military Commission. Not only does this demolish isolationist approaches to defence production, it enables the civilian tech companies of the likes of Huawei, CETC, and AVIC to function as extensions of the defence ecosystems. Only two out of the triad of quality, cost-effectiveness, and convoluted regulations can co-exist in our Public-Private Partnership model.

Conclusion

Indian authorities have shown willingness and capacity to adapt to changing international contexts while maintaining protection and fulfillment of national interests as guiding lights. In defence and security, this resulted in a closer cooperation with the US, reinforcing a wider regional defensive alliance through solid ties in military industrial production, in contrast to the common Chinese enemy. However, resorting to US expertise is insufficient to satisfy India's quest for independent security. In fact, the rising Asian power keeps pursuing it by exporting indigenously produced arms and missile systems and settling Indian defence companies abroad, without reconsidering the motley of checks and balances, regulatory obstructions, and operational inconsistencies. Instead, this is pivotal to eventually adopt a well-defined model for defence production, also inspired by different successful national examples, to revamp the Indian position of net-importer and raise the global defence landscape as the net exporter.

Cooperation in Space Warfare

NATO–India Strategic Convergence in the Fifth Domain

For India, an aspiring global power with one of the fastest-growing space agencies, the militarisation of space is a tangible security concern instead of a distant distraction.

Introduction:

Space cooperation is the need of the decade. It has evolved into a frontier of strategic rivalry and has witnessed an evolution in the character of warfare. The reliance of militaries and economies on satellites for navigation and intelligence has made space a vital pillar of defence. As a result, space deterrence and preparing for its potential weaponisation have become central to debates on security around the world. For India, an aspiring global power with one of the fastest-growing space agencies, the militarisation of space is a tangible security concern instead of a distant distraction. Meanwhile, NATO, traditionally oriented toward terrestrial and maritime security, has now recognised space as its fifth operational domain. As both these actors navigate a rapidly shifting environment marked by both China and Russia's technological assertiveness, the idea of cooperation in space has gained significant resonance. This chapter will explore NATO-India collaboration in the realm of space security, examining shared interests, areas of convergence, analysing both India and NATO's evolving policy, and the possible areas of cooperation.

The Militarisation of Outer Space

Outer space is rapidly emerging as a critical and highly complex domain of modern warfare, with analysts warning about the growing militarisation of the 'edge of space'.[15] The increasing militarisation of space is also evidenced by the successful testing of Anti-Satellite (ASAT) weapons by major powers, including the United States, Russia, China, and India, which generate long-lasting orbital debris and heighten strategic instability. Yet, most counter-space operations today rely on non-kinetic, easily executed, and difficult-to-attribute means: the latter include laser systems that blind optical sensors, jamming devices that disrupt critical communication links, and spoofing techniques that feed false navigation data.[16]

The increasing militarisation of space is also evidenced by the successful testing of Anti-Satellite (ASAT) weapons by major powers, including the United States, Russia, China, and India, which generate long-lasting orbital debris and heighten strategic instability. Yet, most counter-space operations today rely on non-kinetic, easily executed, and difficult-to-attribute means: the latter include laser systems that blind optical sensors, jamming devices that disrupt critical communication links, and spoofing techniques that feed false navigation data.[17]

Cyber operations targeting satellites' software and data infrastructures further amplify vulnerabilities, as they are challenging to detect and attribute. Given these conditions, the unique environment of space grants a strategic advantage to offensive actions, while current defence mechanisms, which are designed for terrestrial threats, remain severely limited.

NATO's Approach to Space Warfare

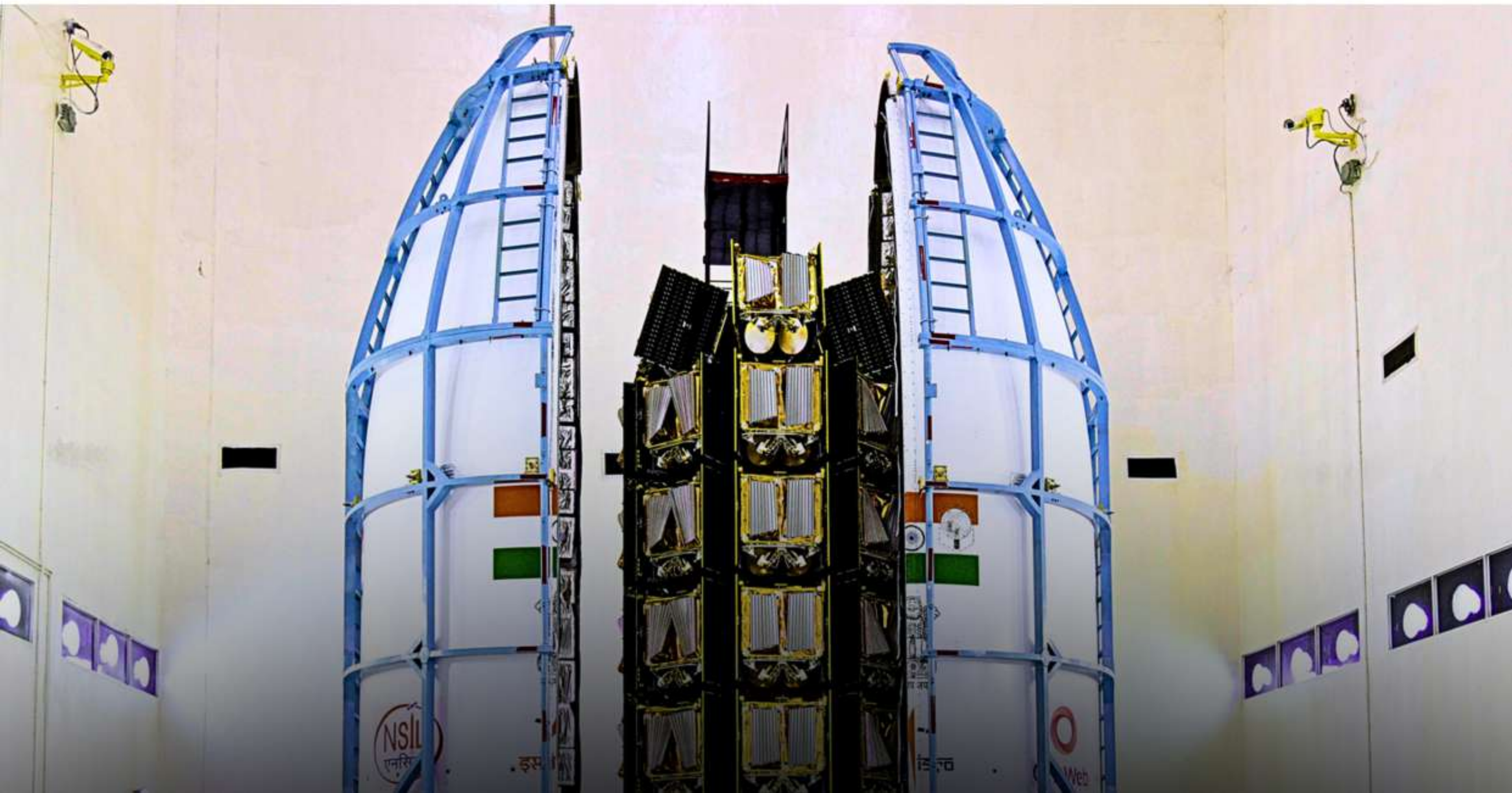
NATO formally defined its strategic approach in 2019 with the adoption of the Overarching Space Policy, consequently declaring space as the fifth operational domain alongside air, land, maritime, and cyberspace. Space capabilities are fundamental to the alliance's deterrence and defence posture as they support essential functions such as Positioning, Navigation, and Timing (PNT), secure satellite communications, and missile early-warning systems. Policy explicitly states that the organisation does not intend to become an independent space actor or develop its own space assets. Instead, it depends on the voluntary contributions of space resources and capabilities provided by its member states. To centralise coordination and enhance information sharing, the NATO Space Operations Centre (NSpOC) was established in Ramstein, Germany, which serves as a vital hub for operational intelligence coordination. Crucially, deterrence continues to play a key role: allies agreed at the 2021 Brussels Summit that attacks in or from space pose a clear security challenge, and thus could be as detrimental to modern societies as a conventional attack. Such actions might potentially lead to the invocation of Article 5, although this decision requires a precise, case-by-case approval by the North Atlantic Council.

Furthermore, NATO aims to boost resilience and interoperability: for instance, defence ministers endorsed the NATO Commercial Space Strategy in February 2025 to better leverage commercial solutions across all phases of conflict. Additionally, the alliance Persistent Surveillance from Space (APSS) programme, representing the largest multinational investment in space capabilities in NATO's history, since it leverages over USD 1 billion in contributions from 17 allies, is aimed at significantly enhancing space-based surveillance and intelligence. Ultimately, all NATO activities in this field are carried out in full compliance with international law, as reflected in the alliance's strong opposition to the weaponisation of space.

India's Position on Space Militarisation

India's trajectory in space militarisation reflects both technological ambition and strategy. Historically, the Indian Space Research Organisation (ISRO) has been framed within developmental priorities such as communication and scientific exploration.[18] Growing regional issues and the increasing reliance of India's armed forces on satellite-based systems gradually pushed the country toward a more defence-oriented space posture, and an 'aatmanirbhar' (self-reliant) space program. A significant turning point for ISRO came in March 2019, when India successfully conducted its first anti-satellite (ASAT) test under its 'Mission Shakti.'

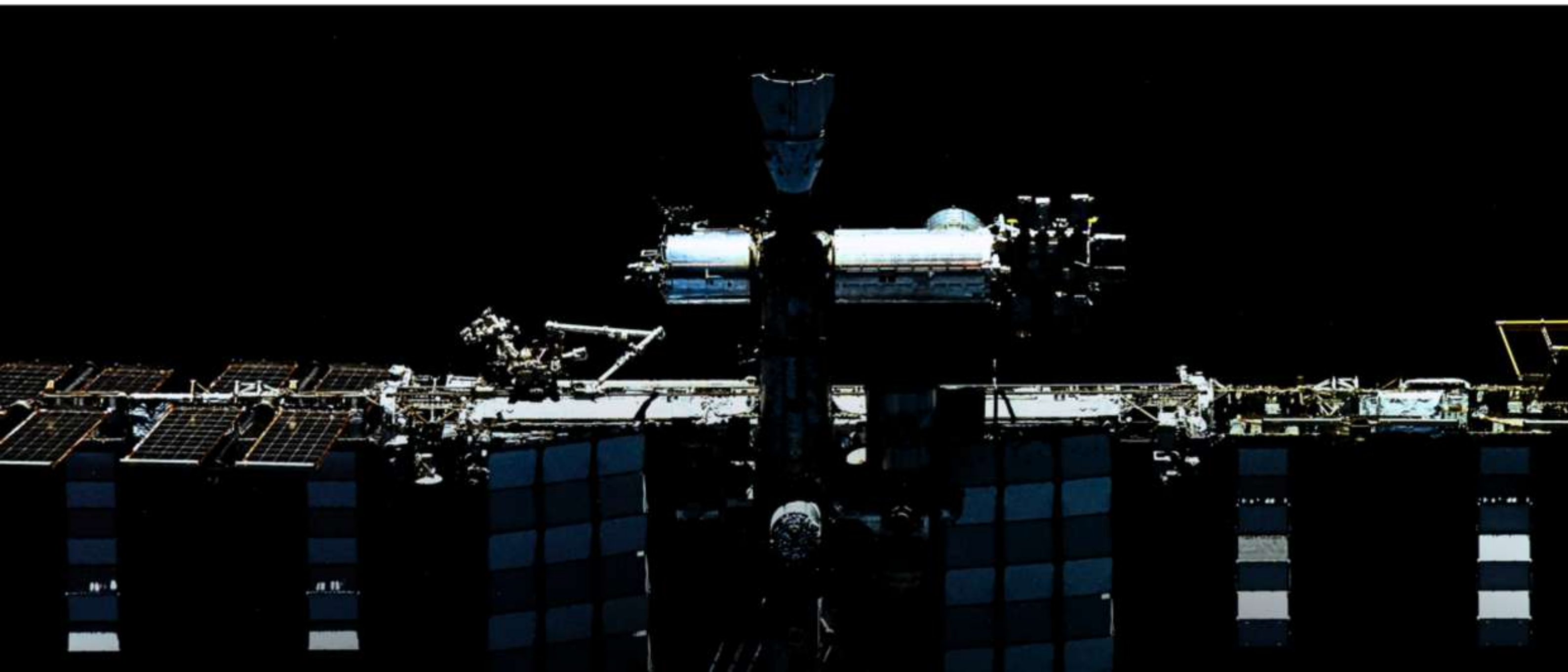
India joined a select group of countries, alongside the United States, Russia, and China, by destroying a live satellite in low-earth orbit, proving its capability of offensive counter-space operations. This test proved New Delhi's determination to secure deterrence in this new strategic frontier. Institutionally, India has also created the Defence Space Agency, which is currently working on a military space doctrine, consolidating military space capabilities. Additionally, India puts forward its 'aatmanirbharta' (self-reliance) via its indigenous navigation system, NAVIC, and increasing investment in dual-use satellite constellations, highlighting the integration of space assets into national defence. Furthermore, New Delhi continues to call for a resilient global framework, emphasising cooperation and prevention of space weaponisation. Thus, it positions India precisely in potential partnerships with organisations such as NATO, where credibility rests on adherence to international norms and regulations.



Strategic Rationale for NATO-India Cooperation & Areas of Cooperation

The cornerstone of space cooperation between India and NATO is the mutual objective of maintaining the stability of the rules-based international order in a context characterised by growing instability, both in the Indo-Pacific region and in the Euro-Atlantic area. Indeed, it is evident that NATO has a growing interest in the Indo-Pacific region, as outlined in the alliance's latest Strategic Concept of 2022, which describes China as a revisionist actor. From a strategic perspective, as articulated by NATO leaders, China is demonstrating a willingness to effect modifications to the prevailing rules-based international order, encompassing the domains of space, cyber, and maritime activities. This strategic intent is underpinned by China's objective of enhancing its international standing and achieving its geopolitical aims. The deepening of the strategic partnership between China and the Russian Federation is indicative of this phenomenon. Furthermore, the mutual attempts of both states to subvert the rules-based international order have been identified as a threat to our shared values and interests. From the NATO and India's perspective, therefore, deepening mutual cooperation responds to a logic of strategic balance, aimed at containing – at least partially– the destabilising dynamics produced by the Sino-Russian axis. [19]

In the last decade, New Delhi has gradually increased its space capabilities for military purposes, as evidenced by the anti-satellite test of 2019. As part of this test, a ballistic missile defence interceptor was used to strike and destroy an Indian satellite in a flight that lasted just over half a minute. This development was largely triggered by China's precedent ASAT test in 2007, which prompted India to reaffirm its deterrence capabilities, in part as a reflection of persistent land tensions with Beijing along the Himalayan borders.[20]



Moreover, from the Indian standpoint, there would be considerable benefit in collaborating on space situational awareness capabilities with NATO and its member states. Indeed, this would enable India to more effectively counter Chinese actions in space, thereby enhancing Indian deterrence and intelligence capacities. In turn, NATO would benefit from expanded monitoring capabilities in the Indo-Pacific region, a region where its strategic outreach remains limited.

Challenges and Future Outlook

Despite increasing cooperation, significant challenges still exist. The first being the geopolitical implications, India occupies a crucial position in South Asia, a region which is historically marked by a fragile balance of power. China could see India's cooperation with NATO as a strategic threat and as a move to contain its rise, which might lead to escalating tensions in the Indo-Pacific and outer space domains. Still, NATO-India cooperation in space warfare remains strong, can pursue collaboration with mutual trust building and recognition of each side's limitations. Conversely, despite the potential for significant mutual benefits from enhanced space cooperation between NATO and India, several factors limit the scope of this partnership. India's commitment to closer collaboration could, to some degree, affect its traditional research for strategic autonomy. Nonetheless, this does not preclude the creation of a flexible, institutionalised cooperative framework. India has already shown its willingness to participate in such arrangements, as evidenced by its engagement in the Quad.[21] Indeed, the establishment of this framework would enable both India and NATO to achieve their strategic objectives in countering Chinese and Russian assertiveness in the space domain, while respecting India's search for strategic autonomy. Simultaneously, this action would lay the foundations for a more structured, long-term partnership in the future.

Conclusion

Everything considered, space cooperation between NATO and India is contemplated as the need of the decade, as space has evolved into a highly complex battleground and a frontier of strategic rivalry. Consequently, both entities recognise space as the fifth operational domain, vital for defence and economies. Moreover, the foundation of this partnership rests on the mutual goal of maintaining the stability of the rules-based international order, specifically to counter the destabilising dynamics produced by the Sino-Russian axis. Therefore, India, having demonstrated its deterrence capability (via the 2019 ASAT test), stands to gain improved Space Situational Awareness (SSA). In return, NATO benefits from expanded monitoring capabilities in the Indo-Pacific region. Nevertheless, significant challenges persist, including geopolitical concerns (China potentially viewing it as containment) and India's commitment to strategic autonomy (Aatmanirbharta). Thus, the future requires establishing a flexible, institutionalised cooperative framework. Ultimately, this structure will enable both partners to achieve their strategic objectives regarding assertiveness while respecting New Delhi's search for autonomy.

The Indo-Pacific Dimension of NATO's Counter-Terrorism Strategy

NATO-India Joint Efforts in Addressing Terrorism

Counterterrorism has become a central pillar of NATO's strategy since the Alliance invoked Article 5 in response to the '9/11' attacks.

Introduction:

The concept of terrorism is intrinsically linked to perceptions of identity-based injustice and the strategic use of fear as a tool to influence or destabilise societies. In contemporary times, it has evolved into a phenomenon dispersed, decentralised, and multifaceted. Terrorism in India is vast and scattered, from the far north to sub/central India, and to the Northeast, comprising forms such as Islamist extremism, secessionist & separationist violence, and left-wing extremist activities. Focal points include primarily cross-border terrorism in Jammu & Kashmir in the north (regularly emanating from Pakistan-backed organisations), anti-establishment insurgency in the Northeast, and radical left-wing extremism in Central and nearby coastal India.

Lashkar-e-Taiba and Jaish-e-Muhammad (National Crime Investigation Bureau 2012) form the core of Islamist Extremism in India, with the primary objectives of merging Kashmir into Pakistan through any means possible and turning India into an Islamic state.[22] India has also seen Khalistani Separatist forces in Punjab (Western/Northwestern India) demanding a new Sikh state, going back to the 1980s, and experiencing a rapid increase in the last decade. Counterterrorism has become a central pillar of NATO's strategy since the Alliance invoked Article 5 in response to the '9/11' attacks. NATO's evolving gudelines emphasise prevention, resilience, and cooperation with global partners.

NATO's Counter-Terrorism Strategy

NATO is an alliance focused on political and military security. Among all the international organisations against the terrorist threat following the '9/11' attacks, NATO is considered one of the most active and experienced actors in combating terrorism.[23] The Defence Against Terrorism Programme of Work (DAT POW), launched in 2004, focuses on developing rapid, field-ready capabilities to counter asymmetric threats such as IEDs, drones, and attacks on critical infrastructure, combining technology, training, and doctrine. NATO has also undertaken major counterterrorism operations—ranging from Eagle Assist and Active Endeavour to Afghanistan—while building expertise in intelligence-sharing, counterinsurgency, and emerging technologies.

The 2010 Strategic Concept marked a turning point by recognising terrorism as a direct threat to NATO citizens and global stability, framing it within a strategy rooted in international law, human rights, and the principles of awareness, capabilities, and partnerships. Despite these advances, NATO–EU cooperation on counterterrorism remains limited by political and legal barriers, even if operational coordination exists on the ground. Most recently, the 2024 Washington Summit reaffirmed terrorism as a central security concern and updated NATO's guidelines to meet contemporary threats.

This outlook resonates with India's own counterterrorism efforts, particularly against cross-border terrorism in Jammu and Kashmir and insurgency in other regions, highlighting a convergence in NATO and India's recognition of terrorism as a transnational challenge requiring enhanced readiness and global cooperation. The Indo-Pacific is important for NATO, given that developments in that region can directly affect Euro-Atlantic security.[24] Any construct of an 'Asian' or 'Indo-Pacific' NATO would derive from a cohesive, committed, and structured compliance to alliance mechanisms.[25]

India's Counter Terrorism Strategy

India's strategy to combat terror has evolved from a lack of the same to a framework comprising multiple agencies that work to eliminate what is now considered a national security threat. The post-independence period saw trans-territorial terrorism as less of a concern contra regional insurgencies and secessionist movements. The 26/11 terror attacks across Mumbai are marked as a turning point in India's national security doctrine, bringing out significant gaps in prevention and bolstering counter-measures.[26] Today, the domestic and the foreign are interlinked in India's stride to eliminate terrorist forces from the country, and international partnerships and joint strategy remain crucial to national integrity. The Left-Wing Extremism (LWE) Division in the Ministry of Home Affairs was operationalised in 2006 to track such activities across the country, primarily in 9 affected states at different levels (Chattisgarh, Jharkhand, Odisha, West Bengal, Andhra Pradesh, Telangana, Maharashtra, Madhya Pradesh, and Kerala).[27]

It also propagates capacity-building initiatives and allocates funds for prevention measures to the CAPF (Central Armed Police Force) deployments and respective state governments.

A shift can be observed from countering militancy through disparate measures to adopting a concrete framework supported by designated response teams. The phenomenon has been largely centralised, enabling better coordination amongst various agencies under the same political leadership. Agencies include the National Investigation Agency (law enforcement related to counter terrorism measures), and Intelligence Bureau (internal security and counterintelligence), and the Research & Analysis Wing (foreign intelligence). India's means and methods of combating the previously mentioned vast terror landscape have multiplied over the years, becoming increasingly outward-looking and involving Joint Working Groups on Counterterrorism (JWG-CT) with multiple global partners such as the U.S., Egypt, Uzbekistan, and many NATO member states, including Italy, France, and Germany.

Further, dialogues and partnerships with multilateral and regional organisations enable inputs from mass-scale expertise and common deliberation on methodologies, examples being the India-EU JWG-CT and the BIMSTEC's (Bay of Bengal Initiative for Multi-Sectoral Technical and Economic Cooperation) JWG-CTTC.[28]This highlights the urgent need for a JWG-CT between India and NATO could be an unprecedented scale of collaboration and achievement upon establishing frameworks for undertaking joint operations and measures.

European Regional Challenges

The strategic cooperation between the European Union and NATO represents a cornerstone of security and stability in the Euro-Atlantic area. This partnership is essential not only for the protection of civilians but also for safeguarding borders, critical interests, and territorial integrity.

Built upon shared values, EU-NATO cooperation seeks to promote and preserve peace, freedom, and prosperity on both a national and international level. Among the key challenges confronting this partnership, terrorism continues to represent a pressing and persistent threat.[29] Since Russia's full-scale invasion of Ukraine, cooperation has intensified, highlighting the importance of collective defence and resilience. Nevertheless, political obstacles remain significant. Longstanding disputes, such as those involving Cyprus and Türkiye, continue to hinder intelligence sharing, joint planning, and operational interoperability.

Furthermore, the EU remains reliant on NATO, particularly on U.S. capabilities, for its military and operational effectiveness, underscoring the persistent asymmetry between the two organisations. The outcome of the 2024 U.S. elections has further underscored the uncertainty of transatlantic security, with American leadership continuing to play a decisive role in shaping the future of NATO-EU relations. At the same time, this dynamic has accelerated calls for strengthening the EU's strategic autonomy. Keychallenges ahead include meeting higher defence spending targets, ensuring alliance cohesion, countering Russian threats, particularly in European airspace, and advancing Europe's defence capabilities.[30]

South Asian Regional Challenges

The South Asian subcontinent serves as a prime example for an extremely volatile theatre of militancy and revolt. Collapsed democracies in a state of ruin and dictatorships/military rule reign in the region, with India being one of the rare few defying the status quo. Regional stability becomes difficult to achieve, with all but one of India's immediate South Asian neighbours experiencing military rule, an ousted government, or a failed national security practice in the recent past. Illegal and disguised safe havens for terrorists have become an obstacle for multilateral cooperation, sourcing from the fact that the region serves as the birthplace of many of the largest and most violent terrorist outfits in history. It is often direct kinetic action that temporarily resolves a part of the issue, the most recent example being Operation Sindoor (May 2025), which saw India strike terrorist camps inside Pakistan in response to the Pahalgam terrorist attack the previous month.[31]

Drawing from this, state-sponsored terrorism becomes a challenge in multilateral cooperation. SAARC (South Asian Association for Regional Cooperation) has steadily declined in dialogue and effectiveness over the years, in essence due to the India-Pakistan rift overcross-border terrorism standing in the way of all other spheres of cooperation. India remains firm and adamant on the resolution of this issue before collaboration can be sought elsewhere.

Present Challenges in NATO-India Collaboration

India promoted multilateral counter-terrorism in the G-20, the UN, the Quad 2.0, ASEAN Regional Forum. However, it remains cautious about joining an 'Asian' or 'Indo-Pacific NATO' due to strategic concerns over China's rising power,regional security gaps, and the potential erosion of its strategic autonomy. Historically, India viewed NATO with aloofness, favouring non-alignment and closer ties with the Soviet Union, while maintaining bilateral security relations with key NATO members. NATO's Strategic Concept portrays India ambiguously—as a peaceful democracy but also as linked to regional instability with Pakistan.[32]

While peacekeeping emerges as a promising area for NATO–India collaboration, India's robust counterterrorism capabilities and zero-tolerance approach—strengthened through partnerships with the U.S. and multilateral forums—position it as a potential, yet largely untapped, NATO partner. Challenges remain, where an 'Asian NATO' is widely seen as U.S.-driven and aimed at countering China, echoing Cold War dynamics. Past failures of Asian security alliances, India's non-alignment tradition, and economic interdependence with China complicate deeper engagement. U.S. dual-track policy—supporting India while maintaining Pakistan's MNNA status—further undermines credibility and complicates NATO–India cooperation.

NATO-India Potential Synergy in Counter-Terrorism

NATO and India share core values of democracy and freedom, both of which are essential to fostering stability and security in the Indo-Pacific region. As the world's largest democracy and a rapidly expanding economy, India has consolidated its statusas a global power, making it an increasingly significant partner for NATO. Strengthening cooperation between the allianceand India would not only contribute to reshaping the security framework of the Indo-Pacific but would also reinforce thebroader international order. For NATO, deepening dialogue with India represents an opportunity to enrich its existing network of partnerships and extend its strategic presence beyond the Euro-Atlantic.[33] Counterterrorism stands out as one of the mostpromising areas for synergy.

Both NATO and India have direct stakes in Afghanistan's stability and are committed to ensuring maritime and land security. India's prior cooperation with the European Union, covering law enforcement, border management, transport, and aviation security, provides valuable experience that could be translated into a closer partnership with NATO. Possible synergies between India and NATO could emerge through a dual-track approach that combines thematic cooperation and structured consultation, offering a balanced framework for deepening engagement without formal alliance commitments. On the one hand, cooperation on specific thematic areas such as cybersecurity could provide a pragmatic entry point.

Recent escalations, including the May 2025 India–Pakistan conflict, underscore India's firm stance against terrorism while exposing key political and strategic gaps in NATO–India cooperation. The first gap concerns strategic divergence over China: NATO's U.S.-led Indo-Pacific approach contrasts with India's pursuit of strategic autonomy. This can be narrowed through joint threat assessments focused on counterterrorism and maritime security. The second gap involves political credibility, as India remains wary of U.S. dual policies—particularly Pakistan's MNNA status—highlighting the need for regular consultations and transparent partnership frameworks. The third gap lies in operational interoperability, which could be strengthened through joint training, peacekeeping cooperation, and crisis response exercises. Overall, NATO–India collaboration faces strategic, political, and historical obstacles that make alignment delicate and conditional on regional dynamics.

After NATO's experience in responding to the 2007 cyberattacks, the Alliance has developed substantial expertise in resilience-building, crisis response, and digital defence coordination. Partnering with India in this domain would allow for mutual learning, joint capacity building, and the development of best practices to counter increasingly sophisticated cyber threats. Such collaboration would strengthen NATO's technological resilience while advancing India's own security priorities in an era of growing cyber vulnerabilities and hybrid warfare. On the other hand, the establishment of NATO as a platform for structured security consultations would create a valuable channel for strategic dialogue and policy alignment. This framework could expand NATO's security perspective to incorporate an Indo-Pacific dimension, offering the Alliance a broader understanding of regional dynamics while enabling India to engage more closely with Euro-Atlantic partners on global security concerns. Regular consultations could also facilitate the exchange of intelligence, enhance situational awareness, and support coordinated responses to transnational challenges. Together, these two complementary avenues would foster a more coherent and multidimensional partnership, enhance joint counterterrorism capacities, and reinforce both NATO's and India's role as responsible global security providers committed to maintaining stability across regions.

Conclusion

NATO's growing focus on the Indo-Pacific is driven by shared security threats, particularly Russia's war in Ukraine and China's alignment with Moscow. The 2022 Strategic Concept labelled China a systemic challenge, prompting deeper engagement with the Indo-Pacific Four (Japan, South Korea, Australia, New Zealand), who have joined recent NATO summits. Key priorities include strengthening defence industries, securing supply chains, and advancing cooperation on cybersecurity, technology, and counter-disinformation.

Furthermore, America's counter-terrorism cooperation with India will be especially important for U.S. interests. New Delhi is Washington's most capable defence and intelligence partner in South Asia, particularly after the collapse of the Afghan military. This can be vitalised by India as an opportunity to initiate engagement with NATO in the subcontinent and further expand with time. The NATO-India partnership brings unmatched scale and cohesiveness that could benefit joint counterterrorism initiatives, especially given India's warm and cordial relations with multiple NATO member states.

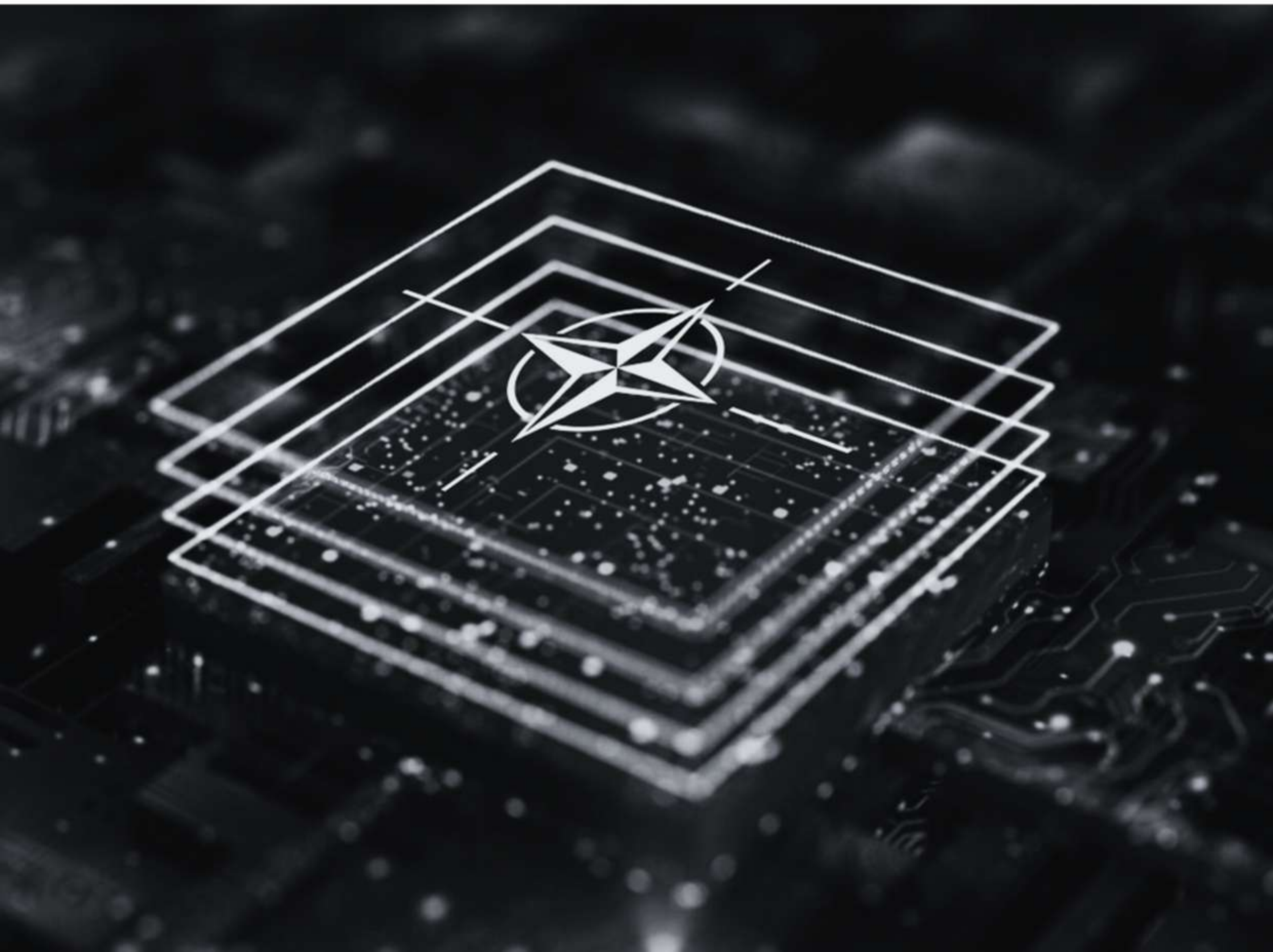
Securing Cyberspace Across Borders

Navigating Strategic Gaps and Responses

Introduction

NATO member states face evolving threats such as disinformation or even AI-powered attacks.

India and the NATO member states' digital growth story has been remarkable over the last few years. As India expands its digital infrastructure, cyber vulnerabilities also increase. Rising cyber threats have led India to prioritise cybersecurity as part of its broader national security framework. Even the NATO member states face evolving threats such as disinformation or even AI-powered attacks. This article aims to navigate the layers of challenges that India and the NATO countries face and analyse the future trajectory of the responses to tackle them in the domain of cybersecurity.



The Threat of Cyberattack: Failed Defence?

In the current global security environment, cyber attacks and threats are more frequent, more complex, and severe, going from critical infrastructure sabotages to hybrid disinformation campaigns, placing cyberspace at the forefront of international competition. This field is constantly evolving, blending military and civilian targets, and operating without clear geographical boundaries. In recent years, cyber attacks have become more and more sophisticated and disruptive. In fact, they can not only create severe problems for different kinds of systems, but can also destroy physical assets. The speed of technological innovation, especially in areas like artificial intelligence and quantum computing, means that offensive capabilities can grow fast and that any defence system may be constantly at risk of obsolescence. Cybersecurity is seen differently by the two actors. In fact, for NATO, cyber defence is crucial for its collective defence, while in terms of India's perspective, it is a matter of national economic sovereignty and data integrity in developing its digital economy.

Giving more details, the increasing potential of cyber attacks poses a series of questions for the alliance. NATO, for the first time, formally stated that a cyber attack could potentially trigger Article 5 in 2014 during the Wales Summit, and this concept was reaffirmed at the Warsaw and Brussels Summits in 2016 and 2021.[34] At the 2021 Summit, the 32 allies endorsed a Comprehensive Cyber Defence Policy, which commits all the States to deter, defend, and counter the full spectrum of cyber threats with the use of political, diplomatic, and military tools. Yet it is not clear how to respond to this type of threat, since one important subject is to avoid escalation. Therefore, responding with conventional force is highly risky, but at the same time, a weak response could signal to the attacker a lack of resolve and unity. Moreover, given that NATO is an alliance and lacks a common cyber defence system, its cybersecurity efforts lie at the member-state level.[35]

This means that there are some problems related to asymmetric capabilities among them. In addition, even though there are already existing mechanisms that facilitate the sharing of information, establishing real-time and trusted information sharing of threat intelligence among all the member states is a huge logistical and political hurdle. Some obstacles to Cyber Threat Intelligence (CTI) sharing are incompatible platforms, jurisdictional constraints, and conflicting strategic cultures.

In the case of India, its digital transformation has increased the frequency of cyberattacks on individuals, businesses, or even the state. The primary challenge is the lack of cybersecurity awareness among individuals and institutions. This lack of digital literacy impacts responses of society, such as falling prey to cyber fraud or even financial scams. This dearth is also observed in cybersecurity professionals, limiting expertise in this field. Furthermore, India needs to effectively implement its regulations and laws concerning cyberattacks. Outdated legislations and the absence of strict regulations leads to limited accountability and responsibility by authorities. The complex cybersecurity structure of India gets further complicated due to the advent of emerging technologies, including artificial intelligence and 5G networks. More efficiency and productivity need more data transfers and a web of IoT (Internet of Things), broadening the cyberattack landscape and triggering vulnerabilities.

For instance, Generative AI has made cyber phishing or malpractices easier and cheaper. The post-pandemic shift has also intensified easier access to individual or organisational data. Even though NATO and India have different and specific challenges, they also share common threats that can be divided into two main categories. The first one is related to state-sponsored sabotage and espionage.

India's Cybersecurity Landscape - Awareness and Understanding of Threats

In response to rising challenges for India's cybersecurity infrastructure, India has developed a multi-layered security landscape. Despite the challenges, India has made significant progress in implementing regulations and laws to strengthen the aspect of cybersecurity. In 2013, the National Cyber Security Policy was introduced as a guiding vision for the country's security domain.[36]Later, with rising vulnerabilities, demand for building more regulatory mechanisms emerged. Since 2021, the government has been working on its Cyber Security Strategy that ensures safeguarding critical aspects and mitigating national security threats. There is an urgent need for a holistic response mechanism that involves all stakeholders, including the state, private entities, nodal agencies like the Computer Emergency Response Team (CERT), and law enforcement agencies.[37]

This centralised structure will ensure that the response procedure is seamless and less time or energy-intensive. People and institutions need to develop cybersecurity awareness and an understanding of the complex web of threats. Cyber literacy drives can highlight the importance of knowledge sharing and ensuring people are less susceptible to fraud or scams. The advent of artificial intelligence in this interface is a boon as well as a bane. Undoubtedly, it makes data sharing and privacy breaches easier, but it can be leveraged as an effective tool that can predict attacks, generate warning systems, and even automate guidelines of safety. Furthermore, foreign attacks can be challenged by ensuring a self-reliant, robust cyber infrastructure devoid of any external dependency.

NATO's Cyber Threat Response- Cooperation Potential with Third Countries

The most significant response was elevating cyberspace to an operational domain, alongside the three traditional spheres of land, sea, and air. This represents the final stage of a process initiated after the cyber attacks perpetrated against Estonia in 2007. Consequently, NATO confirmed its intention to dedicate resources and personnel to the digital sphere, thus elevating the importance of cyberspace in the same strategic level. This decision resulted in enhanced operational capabilities developed by creating technical centres and specialised teams.

To give some examples, NATO established the NATO Cyber Security Centre (NCSC) is the main operational hub responsible for defending NATO's network from cyber attacks 24 hours a day, seven days a week. Its primary objective is to ensure the security of the political and military communications vital to the alliance's function. Furthermore, the Cooperative Cyber Defence Centre of Excellence (CCDCOE) has been founded. Its mission is to support the member states in research, training, and exercises in the field of cyber defence.[38]

The CCDCOE hosts the annual Locked Shields exercise, the world's biggest and most complex real-time cyber defence exercise. Locked Shields enables experts to enhance their skills in the field of defending critical infrastructures under attack. While technical centres handle the operational defence, a political commitment is required to ensure every state meets a minimum standard of preparedness for shared security. For this reason, in 2016, NATO members agreed on a Cyber Defence Pledge, an agreement with which the State decided to give priority to their national cyber defences to protect their critical infrastructures, ensuring they will defend the alliance in cyberspace as effectively as they are in the other domains.[39]

The pledge focuses on boosting digital defence capabilities and facilitating cooperation among the allies, sharing best practices, and providing education and training. Cyber defence cannot be achieved by any single State, regardless of its economic and military power.[40] Even an alliance constituted by some of the most advanced and rich countries in the world cannot do it alone, given the complexity and the evolution of the field. Therefore, the alliance must cooperate with third countries, international or supranational organisations, and the private sector. NATO already collaborates with the European Union, for example, given that the two organisations share many Member States and overlap geographically.

Thus, it is fundamental to broaden the circle of nations working with NATO, especially those that have developed advanced technologies and sophisticated capabilities in detecting and responding to cyber attacks.

Recommendations

NATO and India should cooperate in the field of cybersecurity because of a series of reasons. First of all, they have common threats, as described above, from non-state actors and state-sponsored groups, in particular coming from the Indo-Pacific region. Moreover, they already collaborate in other fields, like counterterrorism and military defence. Both of them possess capabilities that can advance their ability to prevent and respond to this type of attack.

- India should participate in specific NATO-led cyber defence exercises, like 'Locked Shields.' At the time being, an Indian delegation took part in this high-profile event, but the operation remains mainly for NATO's actors. Another fundamental exercise is named Cyber Coalition, which simulates the management of cyber crises that might target critical infrastructures.[41] The participation of India can offer crucial advantages like improved operational readiness and share tactics, techniques, and procedures.

- Another potential idea of collaboration can be forming joint working groups that involve experts from India and NATO's cybersecurity agencies to analyse emerging threats.

- The field of Research and Development can be a central arena where India and the NATO countries can partner on research projects, effectively understanding the technological infrastructure of each other.

- Sharing cybersecurity know-how holds much relevance, considering India and NATO countries face complex threats. This increases the need for establishing secure communication channels.[42]

Conclusion

In conclusion, cybersecurity is a core component of national as well as alliance-led security. India and the NATO member states face evolving cyberattacks, fraud, scams, and even digital espionage. Considering the nature of these threats, a collaborative approach between India and NATO can facilitate effective responses and coordinated solutions can tackle mutual threats. India must work on its gaps in terms of resources and legal frameworks, whereas NATO should develop its structured, cohesive cybersecurity policy to streamline ideas. Since challenges and opportunities overlap, the sector of cybersecurity opens avenues for potential collaboration between India and the NATO countries.

Concluding Remarks

India's close relations with NATO allies can sustain complementarity during further engagements and negotiations.

In conclusion, the relation between NATO member countries and India need to move beyond dialogue to tackle effective responses against common threats. Such exchanges need to identify potential areas of collaboration considering the gap lines regarding legal frameworks and resources. The two sides can utilise the current methods to safeguard their national security landscape through bilateral and multilateral engagements that includes partner countries of both NATO and India.

The effectiveness of defining the areas of collaboration can enable in assessing the capabilities of common adversaries for future conflicts and enhance public trust about the partnership in the international, national, and regional institutions. The collaboration between NATO and India need to advance long-term changes in the decision making landscape to advance simplification for time-sensitive collaboration frameworks during instances of state-sponsored sabotage and conflicts with common regional and global rivals.

Considering the emergence of multipolar world order marked growing presence from contradictory powers in the Indo-Pacific region, NATO can take the opportunity to engage India as a key partner considering its role as an economic and military power house with potential for innovation and emerge as a stabilising force outside the territory of NATO. India's close relations with NATO allies can sustain complementarity during further engagements and negotiations.

Additionally, India's and NATO's defence capabilities can build defence capabilities of both sides considering the joint historical record in sustaining long-term and short-term military operations, which is essential to build clear strategies for capacity development and interoperability.

References

1. Huria, Sonali. “India and the ‘Global NATO’: Expectations and Reservations | IPCS.” ipcs.org. Institute of Peace and Conflict Studies, January 25, 2009. https://www.ipcs.org/comm_select.php?articleNo=2790.

2. Ghadigaonkar , Arya . “NATO-India Relations: Potential for Defence Cooperation.” thegeostrata.com . The Geostrata , February 28, 2025. https://www.thegeostrata.com/post/nato-india-relations-potential-fordefencecooperation

3. Anon. “An Intellectual Inquiry: NATO-India Youth Conference.” thegeostrata.com. The Geostrata , March 2025. https://www.thegeostrata.com/nato-india-youth-conference.

4. E. Miller, Steven, Robert Legvold, and Lawrence D Freedman. “Nuclear Weapons in a Changing Global Order | American Academy of Arts and Sciences.” amacad.org. American Academy of Arts & Sciences, 2025. https://www.amacad.org/publication/nuclear-weapons-changing-global-order/section/4.

5. Joseph, Biyon Sony. “India and the Indo-Pacific in Trump’s Second-Term Strategy.” thediplomat.com. The Diplomat, December 10, 2025. https://thediplomat.com/2025/12/india-and-the-indo-pacific-in-trumps-second-term-strategy/.

6. Shah, Kamal. “Bharat Dynamics Limited’s Commitment to Defence Manufacturing and Innovation - Indian Aerospace and Defence Bulletin - News for Aerospace and Defence in India.” iadb.in. Indian Aerospace & Defence Bulletin, July 22, 2024. https://www.iadb.in/2024/07/22/bharat-dynamics-limiteds-commitment-to-defence-manufacturing-and-innovation/.

7. Ibid.

8. Patel, Shivam. “Exclusive: India Expects $200 Million Missile Deal with Philippines This Year, Sources Say.” reuters.com. Reuters, February 13, 2025. https://www.reuters.com/world/india/india-expects-200-million-missile-deal-with-philippines-this-year-sources-say-2025-02-13/.

9. Odakkal, Johnson. “Defence Budget 2025: Step Forward or a Sustenance Strategy?” financialexpress.com. Financial Express, February 2, 2025. https://www.financialexpress.com/budget/defence-budget-2025-step-forward-or-a-sustenance-strategy-3734804/.

10. Solomon, Shoshanna. “Israel Aerospace Gets $630m Missile Defense Deal for Indian Navy.” timesofisrael.com. The Times of Israel, April 21, 2017. https://www.timesofisrael.com/israel-aerospace-gets-630m-missile-defense-deal-for-indian-navy/

11. Press Information Bureau (PIB). "Aatmanirbhar Bharat: Rs 2,385 Crore Contract Inked with BEL for Electronic Warfare Suites & Aircraft Modification Kits for Mi-17 v5 Helicopters." pib.gov.in. Ministry of Defence, April 6, 2025. https://www.pib.gov.in/PressReleasePage.aspx?PRID=2119805&reg=3&lang=2.

12. Pasko, Nika. "South Korea Is on Track to Become a Defence Powerhouse | Lowy Institute." lowyinstitute.org/the-interpreter. The Interpreter, October 23, 2025. https://www.lowyinstitute.org/the-interpreter/south-korea-track-become-defence-powerhouse.

13. Wong, Hayley. "China Supplied 81% of Pakistan's Arms Imports in the Past 5 Years, SIPRI Says." scmp.com. South China Morning Post, March 16, 2025. https://www.scmp.com/news/china/military/article/3302515/china-supplied-81-pakistans-arms-imports-past-5-years-sipri-says

14. Insinna, Valerie. "The F-35 at 20: How Its Successes, Failures, Shaped the Aerospace Industry." breakingdefense.com. Breaking Defense, October 26, 2021. https://breakingdefense.com/2021/10/the-f-35-at-20-how-its-successes-and-failures-shaped-the-aerospace-industry/.

15. Miha Šlebir. "Weaponising the Edge of Space? Progress and Prospects of Military High-Altitude Platforms." Colombian Journal of Military and Strategic Studies 23, no. 51 (July 1, 2025): 566–88. https://doi.org/10.21830/19006586.1483.

16. Abels, Joscha. "Private Infrastructure in Geopolitical Conflicts: The Case of Starlink and the War in Ukraine." European Journal of International Relations 30, no. 4 (June 17, 2024): 842–66. https://doi.org/10.1177/13540661241260653.

17. Pant, Harsh V., and Ajey Lele. "India in Space: Factors Shaping the Indian Trajectory India in Space: Factors Shaping the Indian Trajectory." Space and Defense, 4, no. 3 (2010): 47–59. https://doi.org/10.32873/uno.dc.sd.04.02.1159.

18. Press Information Bureau. "India Joins Select Group of Nations, Destroys Live Satellite in Low Earth Orbit." pib.gov.in. Ministry of Defence, March 27, 2019. https://www.pib.gov.in/Pressreleaseshare.aspx?PRID=1569563&reg=3&lang=2.

19. Austin, Greg, Timothy Wright, and Rajeswari Pillai Rajagopalan. "Military Ambitions and Competition in Space: The Role of Alliances." iiss.org. IISS, February 5, 2022. https://www.iiss.org/research-paper/2022/02/military-ambitions-and-competition-in-space-the-role-of-alliances/.

20. Sharmin, Farjana. "China's Increasing Space Power and India–China Orbital Competitions: Implications in the Indo-Pacific with a Focus on South Asia." Air University (AU). Journal of Indo-Pacific Affairs, November 15, 2023. https://www.airuniversity.af.edu/JIPA/Display/Article/3588334/chinas-increasing-space-power-and-indiachina-orbital-competitions-implications/.

21. Ibid.

22. Beaumont, Peter. “Kashmir Crisis: What Is Lashkar-e-Taiba and Is It Supported by Pakistan?” theguardian.com. The Guardian, May 7, 2025. https://www.theguardian.com/world/2025/may/07/kashmir-crisis-pakistan-terrorist-groups-infrastructure.

23. Karadeli, Andreea Stoian. “NATO Defence against Terrorism.” utrgv.edu. Security Policy, June 2021. https://www.utrgv.edu/pass/_files/documents/nato-defense-against terrorism.pdf.

24. NATO. “NATO 2022 Strategic Report.” nato.int. Madrid: NATO, June 29, 2022. https://www.nato.int/en/about-us/official-texts-and-resources/strategic-concepts/nato-2022-strategic-concept.

25. Panda, Jagannath. “India’s Stance on the ‘Asian NATO’: Between ‘Status’ and ‘Security’ Dilemmas.” Strategic Analysis 46, no. 1 (March 12, 2022): 1–17. https://doi.org/10.1080/09700161.2022.2028494.

26. Staniland, Paul. “Improving India’s Counterterrorism Policy after Mumbai – Combating Terrorism Center at West Point.” Ctc.westpoint.edu 2, no. 4 (April 15, 2009): 1–3. https://ctc.westpoint.edu/improving-indias-counterterrorism-policy-after-mumbai/.

27. Press Information Bureau (PIB). “From Red Corridor to Naxal-Free Bharat: A Decade of Decisive Gains (2014–2025).” pib.gov.in. PIB Headquarters, 2025. https://www.pib.gov.in/PressReleasePage.aspx?PRID=2203440&reg=3&lang=1.

28. Ministry of External Affairs. “India and EU Hold 15th Counter-Terrorism Dialogue.” mea.gov.in. Ministry of External Affairs, September 9, 2025.https://www.mea.gov.in/press-releases.ht d tl/40120/India+and+EU+hold+15th+CounterTerrorism+Dialogue.

29. Olech, Aleksander. “Cooperation between NATO and the European Union against Hybrid Threats with a Particular Emphasis on Terrorism.” ine.org.pl. Institute of New Europe, March 17, 2021. https://ine.org.pl/en/cooperation-between-nato-and-the-european-union-against-hybrid-threats-with-a-particular-emphasis-on-terrorism/.

30. Sebastian, Clapp. “EU–NATO Cooperation.” Europarl.europa.eu. European Parliamentary Research Service (EPRS), June 23, 2025. https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI%282025%2977292.

31. Press Information Bureau (PIB), “PM Modi Has Redefined India’s Policy against Terrorism, Any Attack on Indian Soil Will Be Considered as an Act of War: Raksha Mantri in Srinagar,” pib.gov.in (Ministry of Defence, May 15, 2025), https://www.pib.gov.in/PressReleasePage.aspx?PRID=2128840®=3&lang=2.

32. Sahni, Varun. "Towards a New NATO Strategic Concept: A View from India." fes.de. Friedrich Ebert Stiftung , October 2010. https://library.fes.de/pdf-files/id/ipa/07517-20101122.pdf.

33. Meszaros, Krisztian. "NATO and India: Partners for a Peaceful, Free, and Democratic World." orfonline.org. Observer Research Foundation (ORF), February 23, 2024. https://www.orfonline.org/expert-speak/nato-and-india-partners-for-a-peaceful-free-and-democratic-world.

34. Allied Command Transformation (ACT), "Cyber Coalition," NATO, https://www.act.nato.int/activities/cyber-coalition/

35. North Atlantic Treaty Organisation, "Cyber Defence," NATO, https://www.nato.int/en/what-we-do/deterrence-and-defence/cyber-defence

36. Press Information Bureau (PIB). "Government of India Taking Measures to Protect Critical Infrastructure and Private Data against Cyber Attacks." pib.gov.in. Ministry of Electronics & IT, January 28, 2025. https://www.pib.gov.in/PressReleasePage.aspx?PRID=2116341&reg=3&lang=

37. Press Information Bureau (PIB). "Cyber Security Infrastructure." pib.gov.in. Ministry of Home Affairs, December 2, 2025. https://www.pib.gov.in/PressReleasePage.aspx?PRID=2197529&reg=3&lang=2.

38. Anon. "Locked Shields." ccdcoe.org. The NATO Cooperative Cyber Defence Centre of Excellence, n.d. https://ccdcoe.org/locked-shields/.

39. Lété, Bruno, and Daiga Dege. "A Roadmap to Resilience." jstor.org. Vol. 23. Washington D.C: German Marshall Fund of the United States, 2017. JSTOR. https://doi.org/10.2307/resrep18857.

40. NATO Communications and Information Agency (NCIA), "NATO Cyber Security Centre," NATO, https://www.ncia.nato.int/about-us/service-portfolio/nato-cyber-security-centr

41. Allied Command Transformation (ACT), "Cyber Coalition," NATO, https://www.act.nato.int/activities/cyber-coalition/

42. Maurizi, Giuliano. "Cyberspace Risks and Challenges to NATO/EU." nrdc-ita.nato.int. NATO, 2022.https://nrdc-ita.nato.int/newsroom/insights/cyberspace-risks-and-challenges-to-nato--eu-and-the-main-issues-to-conduct-cyberspace-operations-at-the-operationalevel.

Report Team

🔗 Authors

Anshika Malik, is a Research Associate at the Centre for Diplomacy and Innovation, The Geostrata.

Chiara Merlin, is the Deputy Director at the Mondo Internazionale APS.

Did Atal, is a Junior Researcher at the Centre for Diplomacy and Innovation, The Geostrata.

Francesco Oppia, is the Editor-in-Chief at the Mondo Internazionale APS.

Giulia Casot, is a Junior Researcher at the Mondo Internazionale APS.

Ishan Sinha, is a Research Associate at the Centre for Diplomacy and Innovation, The Geostrata.

Nandita Lata, is the Director of Covering China at The Geostrata.

Rosa Santa Serravalle, is a Senior Researcher in the Culture & Society Section at the Mondo Internazionale APS.

Sharon Giacomelli, is a Junior Researcher in the Politics Division at the Mondo Internazionale APS.

Valeria Picciolo, is the Deputy Editor-in-Chief at the Mondo Internazionale APS.

🔗 Designers of Strata

Ameya Gupta, is a Junior Associate at The Geostrata

Nakshatra H. M., is a Junior Associate at The Geostrata

A. Shreya Lakshmi, is a Senior Associate at The Geostrata

GEOSTRATA

Centre for Diplomacy and Innovation

- NATIONAL SECURITY
- MARITIME DESK
- CHINA DESK
- CYBERSECURITY
- NEIGHBORHOOD DESK
- NUCLEAR STUDIES

Pillars *of* CREATION

For a Distinctly Indian Take on World Affairs

Pillars *of* CREATION

For a Distinctly Indian Take on World Affairs

GEOSTRATA

The Geostrata, with a commitment to fostering a comprehensive understanding of global dynamics and thereby promoting a distinctly Indian take on world affairs, has structured its expertise into distinct pillars of creation. These pillars represent a synthesis of profound research, informed perspectives, and proactive engagement in each domain.

In our "Strategic Studies" division, we delve into critical issues ranging from national security challenges, such as aerospace threats and terrorism, to focused areas like maritime and cybersecurity. Recognizing the pivotal role of international relations, our "Diplomacy" pillar spans geographic-specific desks, ensuring we maintain a nuanced perspective on global interactions.

Our commitment to sustainable futures is evident in our "Environment" section, where we tackle everything from energy security to biodiversity conservation. Meanwhile, the "Trade and Development" segment ensures a comprehensive understanding of both global trade dynamics and intricate nuances of India's economic sectors.

The "History and Culture Desk" stands as a testament to our belief in the importance of understanding our past, rich cultural heritage, and linguistic diversities. With the rapid advancements in the technological sphere, our "Science and Technology" division remains at the forefront, analyzing developments from nanotechnology to AI.

Acknowledging the intricate weave of governance, our "Politics and Law" pillar delves deep into domestic and international legal frameworks and political landscapes. Similarly, the "Infrastructure" section focuses on the bedrock of urban and rural landscapes, ensuring we remain informed about key developmental facets.

Our endeavor to remain at the cutting edge is further cemented with our "Space Desk," where space exploration and technology come to the forefront. Lastly, our additional centers like the "Problem Identifier Center" and "Graphics Innovation Center" underscore our commitment to innovation, risk management, and holistic analysis.

Together, these pillars underscore The Geostrata's unwavering dedication to understanding and interpreting the world in its multifaceted complexity.

Team Pillars of Creation

Our Socials

Click on the icons to interact

Subscribe to our newsletter at THEGEOSTRATA.COM

For a Distinctly Indian Take on World Affairs

@THEGEOSTRATA

COVERING CHINA

@COVERINGCHINA

COVERING ISRO

@COVERINGISRO

@COVERINGMEA

@COVERINGPM

To download the full report, visit: thegeostrata.com

SCAN ME

JOIN US

Scan the QR code to fill out the 'Join us' Form

ENGAGE *with Strata*

January 2026

By The Geostrata's
Centre for Diplomacy and Innovation

CONNECT@THEGEOSTRATA.COM

+91 97970 66235