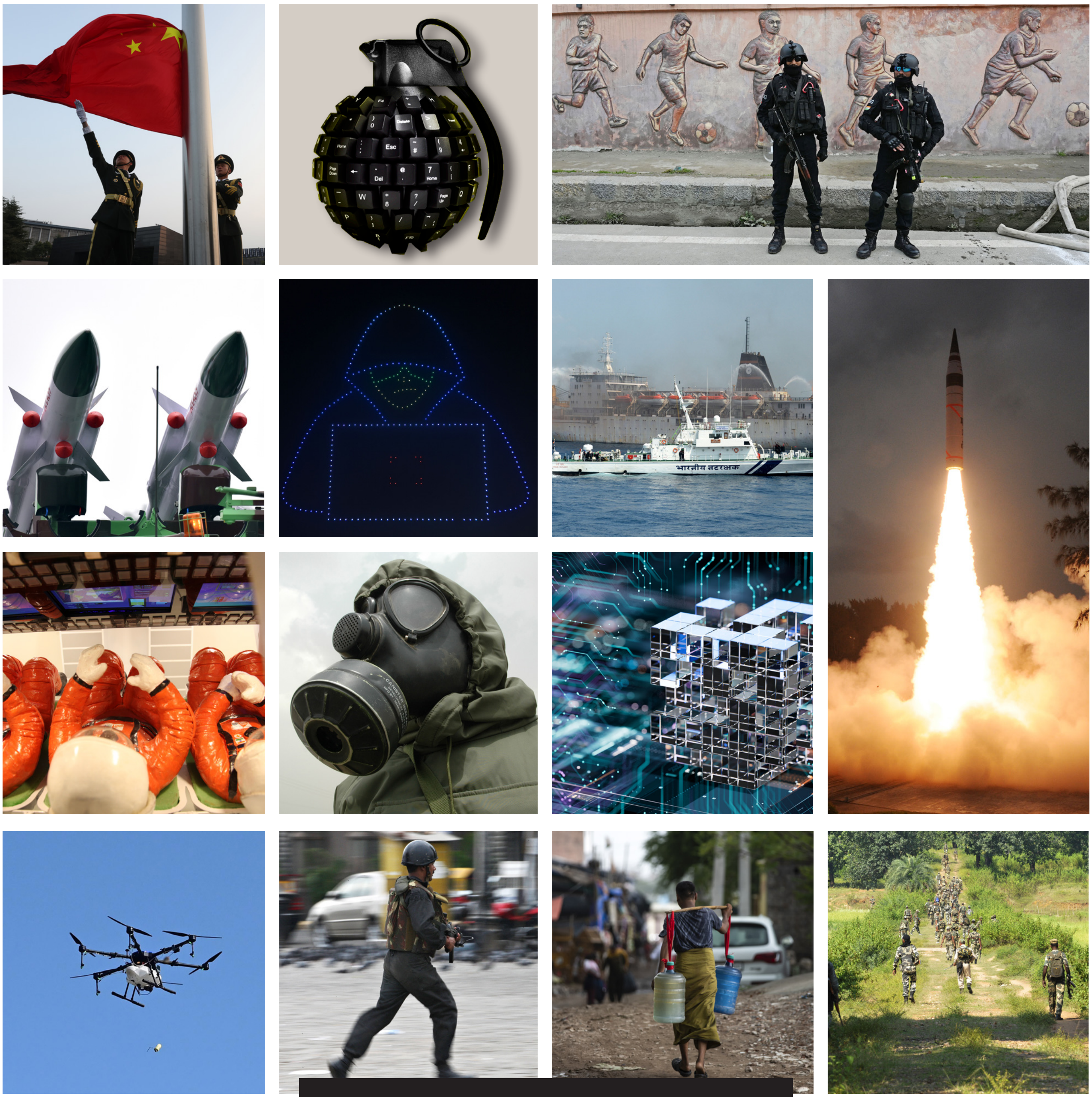
SPECIAL REPORT no. 245

Current Trends in India's National Security 2025

Harsh V Pant and Sameer Patil
Eds.



JANUARY 2025

Contents

I Critical Challenges

II Key Technologies

Introduction

Harsh V Pant and Sameer Patil

In a year marked by widening inter-state conflicts and intensified great-power hostilities, India's national security outlook remained complex. Even as the four-year-long border standoff with China in the Himalayas showed initial signs of thawing in 2024, it did little to bridge the trust gap or address the roots of India-China security competition. Beijing's sustained military and nuclear modernisation, along with its ever-expanding collusion with Pakistan, necessitates that India maintain its guard. Compounding New Delhi's threat perception is China's growing naval presence in the Indian Ocean and influence in India's neighbourhood. The spectre of instability in India's east, brought about by the violence in Manipur and the rapid spread of disorder in Bangladesh following the fall of the Sheikh Hasina government, only adds to these complications.

In India's west, Pakistan remained mired in instability in 2024 aggravated by the state's inability to tackle security challenges and stem economic decline. Yet, these precarious circumstances have not deterred the military establishment from carrying on with its anti-India terrorism campaign. The activation of militancy south of Pir Panjal and the continuing push for cross-border militant infiltration by the Pakistan Army has had unsettling consequences for Jammu and Kashmir's security situation. These dynamics threaten to undo the gains that followed the constitutional amendments of August 2019. More importantly, any potential revival of militancy in Kashmir Valley will boost the terrorist propaganda that endures despite the significant decline in terrorist violence globally.

Attribution: Harsh V Pant and Sameer Patil, "Current Trends in India's National Security 2025," *ORF Special Report No. 245*, January 2025, Observer Research Foundation.

Indeed, radicalisation has taken new channels, including social media propaganda, as seen in the stories of individuals apprehended last year in a spate of arrests across India of suspects belonging to al-Qaeda and the Islamic State.

Perhaps the only silver lining in this sobering landscape has been the decisive blow dealt by India's security forces to Left-Wing Extremism, with Chhattisgarh leading the heightened crackdown on the Naxalites' cadres and hideouts. Pursuing the battle to its logical end will require efforts not just on the security front but also economic development.

Overall, despite resource constraints, India's national security establishment has exerted earnest efforts to respond to the evolving security landscape. The military's push for jointness and theaterisation, as well as moves to bolster naval capabilities reveal its commitment to more effectively tackle the China challenge. Likewise, the focus on inter-agency coordination and intelligence-led operations in Naxalite-affected regions and Jammu and Kashmir has yielded pivotal results. The National Investigation Agency's steadfast clampdown on terrorist financing and money laundering has also dented the capabilities of terrorists and their ecosystem of supporters. As the developments in Manipur and Bangladesh show, however, New Delhi must become nimbler in anticipating emerging trends and adopting more appropriate and proactive measures. Reforms in the intelligence apparatus that complement these efforts are also imperative.

This also holds true in the domain of critical and emerging technologies, where a raft of advancements has taken place in cyber, drones, space, quantum computing, and chemical and biological weapons. New Delhi has ramped up its capabilities in the last decade, particularly in the cyber and space domains. It must adopt a similar strategy for its R&D in other technological innovations.

This inaugural edition of *Annual Trends in India's National Security* brings together ORF's subject matter experts to decipher the vital trends that were palpable in their respective areas in 2024. The report is divided into two sections.

The first section assesses the most crucial challenges to India’s national security. Essays in this section cover geographies like Jammu and Kashmir, the Northeast, China, and the Indian Ocean region while also understanding related issues such as defence reforms, cybersecurity, terrorism, Left-Wing Extremism, and intelligence. The second section delves into key technological domains such as space, nuclear, artificial intelligence, quantum computing, and chemical and biological weapons. The aim is to illustrate important technological developments not only in the domestic arena but beyond, and gauge their national security implications for India.

It is ORF’s intention to release this publication annually, to spur meaningful conversations on national security issues and stimulate debate about the strategies and pathways that the country’s policymakers must craft for a secure and stable India.

Harsh V Pant *is Vice President, ORF.*
Sameer Patil *is Director, Centre for Security, Strategy and Technology, ORF.*

I
Critical Challenges

China's PLA

India's Strategic Concerns

Atul Kumar

The year 2024 was marked by turbulence within China's People's Liberation Army (PLA). The ongoing purge of senior officials, which began in 2023, escalated internal power struggles, creating widespread chaos and instability. Amid this turmoil, the PLA underwent another round of restructuring, strengthening its capabilities in information warfare and operational security. Even further reorganisation cannot be ruled out.

Towards the end of the year, China's military-industrial complex unveiled a range of advanced military equipment and weapons systems, signalling imminent induction and expanded export offerings.[1] These developments paint a contradictory picture: despite internal turmoil, the PLA's pursuit of advanced capabilities remains undisturbed. China's defence industry continues to innovate and move towards state-of-the-art weaponry, but the PLA remains entangled in internal power struggles and systemic chaos. This duality underscores India's need to prioritise its capability accretion while closely monitoring the PLA's internal developments.

Anti-Corruption Purges and Instability

In 2024, President Xi Jinping's purge of the PLA's top leadership continued unabated with the dismissal of over 15 senior military officers.[2] These officials lost their positions and societal standing and saw the dismantling of their extensive patronage networks within the military. The Central Commission for Discipline Inspection (CCDI) further extended its scrutiny to those who benefited from these officers through promotions, privileges, or other forms of support, deepening the campaign's impact.

The resulting turmoil within the PLA has shaken the political leadership's confidence in the military. In response, China's top leaders have intensified their demands for absolute loyalty from the PLA's rank and file.[3] The tightening grip from above has curtailed the discretionary freedom of senior military officers in shaping security policy. At the same time, the persistent threat of anti-corruption investigations has unsettled corrupt generals, forcing them to focus on evading the CCDI's reach and safeguarding their ill-gotten gains and patronage networks. This pervasive sense of insecurity can erode the PLA's combat effectiveness and decision-making capacity. This situation, centralised control, and unstable military leadership would expand India's leverage in its interactions with China and the PLA.

The Restructuring

In April 2024, China dismantled the PLA's Strategic Support Force (SSF) and replaced it with three new deputy-theatre grade arms: the Information Support Force (ISF), the Aerospace Force, and the Cyberspace Force.[4] The ISF is responsible for safeguarding secure network information systems and ensuring communication security during high-intensity future conflicts. The Cyberspace Force conducts offensive information operations to disrupt, degrade, and neutralise adversary battlefield networks.

Drawing lessons from recent conflicts in Ukraine and the Middle East, the PLA identified its weaknesses in establishing a cohesive network information space for joint operations.[5] Key weaknesses include outdated data standards, inadequate network integration, flawed operational protocols, poor interoperability, and a weak foundational information environment.

These new forces aim to address these gaps and bolster the PLA's capabilities in modern warfare.

New Weapon System Developments

Corruption within the PLA and Xi's anti-corruption campaign did not hinder the progress of China's defence industry in developing new equipment and weapons systems in 2024. These hardware developments have enhanced PLA's inventory. The unique defence items that China showcased in 2024 include the Type 76 Landing Helicopter Dock (LHD), J-36 and another unnamed advanced stealth air combat aircraft, and Y-20-based Airborne Early Warning Aircraft.[6] The PLA also showcased refined versions of J-20 and J-35 fighters, ready for induction and export. In addition, China's third aircraft carrier, Fujian, started sea trials leading up to its commissioning. The sixth-generation stealth combat aircraft, which gained widespread attention on social media after its test flight on Mao Zedong's birthday on 26 December, along with its smaller advanced fighter, has ignited serious deliberation among China's adversary states on the future of combat aviation.

Implications for India

The establishment of the ISF is expected to enhance China's information protection and operational security capabilities—areas likely to be primary targets during the initial phase of any conflict. In contrast, India's Defence Cyber Agency, led by a two-star officer and equipped with cyber emergency response task forces, remains a defensive entity with limited scale and scope. The Indian military's approach has yet to reflect the level of preparedness needed to counter the emerging Chinese challenge in the information warfare domain.

Similarly, India's shortcomings in long-term military planning are evident in its failure to develop advanced fifth- and sixth-generation combat aircraft and multi-role large amphibious warships such as LHDs, which underscore limited capabilities in both air and amphibious warfare. The Indian Air Force faces a critical shortage of advanced combat aircraft, and its squadron strength is decreasing rapidly, while the Indian Navy's amphibious warfare capability remains limited.

To address these gaps, India must prepare for China's rapid military advancements and ensure that the capability gap between Indian and Chinese forces does not widen to a point that emboldens Chinese adventurism.

In 2025, India must prioritise the accelerated induction of advanced capabilities into its military inventory while keeping an eye on PLA developments.

Atul Kumar *is Fellow, National Security and China Studies, ORF.*

Jammu and Kashmir

Steadfast Zero-Tolerance Policy

Ayjaz Wani

Since 2019, New Delhi has firmly established a zero-tolerance policy to combat terrorist and separatist activities in Jammu and Kashmir (J&K) through kinetic and non-kinetic operations. The security forces and J&K administration have successfully reduced stone-pelting incidents, curtailed protests at encounter sites, and dismantled terrorist infrastructure. These resulted from proactive outreach, community trust-building, and addressing local grievances. In 2024, J&K saw a record voter turnout, particularly among the youth, in both Lok Sabha and assembly elections, without any terror incident.

Changing Geography

In 2024, security forces made progress in counter-terrorism operations despite a challenging security environment marked by the resurgence of terrorism in new areas. With a dwindling support base in the Valley, terrorists struggled to confront security forces in an urban environment, forcing them to shift terror operations to the forested areas south of Pir Panjal and the rugged terrain of Jammu. Since 2019, the security grid in the valley, especially in South Kashmir, has been largely successful in combating terrorism. Terrorists have resorted to engaging in their activities in the border districts of Rajouri and Poonch, as well as in Doda, Kishtwar, and Kathua in the Jammu region.

The complex terrain and diminished security grid after troop deployments in Eastern Ladakh allowed Pakistan-based terror organisations to exploit the gap, sending armed terrorists across the International Border (IB) and Line of Control (LoC), sometimes using tunnels. In 2024, terrorists killed 16 security personnel, 10 civilians, and two Village Defence Guards in the Jammu region, while security forces eliminated 13 terrorists.[1] In response to the rising terror incidents in Jammu, New Delhi developed an area domination plan, deploying additional troops and National Security Guards (NSG) commandos for rapid response.

From South Kashmir to North Kashmir

With the recent killing of five local cadres in South Kashmir, most of the local terror outfits were almost wiped out, with recruitment at an all-time low, as only seven youths joined the insurgency. A crackdown on terror funding, the Over Ground Workers (OGWs), and separatists in South Kashmir, along with a robust security grid, has forced terrorists, especially foreign operatives, to relocate to North Kashmir. In 2024, around 75 terrorists were killed across the Union Territory, with 60 percent identified as Pakistani nationals.[2] North Kashmir saw 17 encounters, resulting in the death of 27 terrorists and five security personnel.[3] Most terrorists were killed during infiltration attempts, with eight such incidents along the LoC. Islamabad is exploring new strategies to maintain relevance in the region.

A shift in youth perception towards Pakistan-supported terrorism and violence, coupled with all-time low local recruitment, has forced Islamabad to push more terrorists across the LoC and IB. New Delhi has responded by implementing additional measures, including increased troop deployments and improved operational readiness.

Rising Tech Usage Among Terrorist Groups

Since 2015, terror groups have leveraged the internet, expanding their presence across social media to recruit and radicalise in Kashmir. In response to increased surveillance and intelligence gathered from technical means (TECHINT), these groups shifted to using highly encrypted telecommunications equipment typically employed by the Pakistani Army.

New shadow groups such as the Kashmir Tigers and the People's Anti-Fascist Front have exploited technology to mislead Indian security agencies and spread their ideologies through online media, sharing videos and voice messages. These terrorist organisations use encrypted messaging platforms and social media, including Chirpwire, Enigma, Mastodon, and Telegram. They are using Artificial Intelligence (AI) to create propaganda videos and images aimed at radicalising youth and fuelling anti-India activities. In response, security agencies are reinforcing age-old HUMINT to complement TECHINT-based anti-insurgency operations.

Looking Ahead

Security agencies have implemented proactive strategies to restore the security grid and enhance coordination among various security forces, strengthening counter-terrorism efforts. The NSG commandos' presence in J&K will aid training for specialised police units, particularly in anti-terrorism operations in the rugged terrain and forests of Jammu. Similarly, the elite PARA special forces of the Indian Army have started training an anti-terror group of the J&K police force in Jammu. These joint training programmes will enhance operational coordination at lower levels.

Pakistan will likely continue attempting to push terrorists across the border and leverage encrypted apps and social media platforms for recruitment and anti-India propaganda, particularly in Jammu and North Kashmir. New Delhi needs coordinated efforts among security agencies to restore the security grid and actively monitor and filter social media campaigns. The proactive use of AI and technology will be crucial in curbing terrorism and OGWs. As the J&K security situation continues to evolve, there is a growing need for enhanced security collaboration in counter-terrorism operations.

Ayjaz Wani *is Fellow, Strategic Studies Programme, ORF.*

Northeast Region

Disturbances Threaten Progress

Sohini Bose and Sreeparna Banerjee

India's Northeast, comprising eight states,[a] is connected to the rest of the country through the narrow Siliguri Corridor. Although years of internal insurgencies and external security challenges[1] stunted its development,[b,2] a number of peace accords signed in the past decade[3] have brought relative stability to the region. This stability has fostered development and enabled these states' geopolitical potential to advance India's foreign policy aspirations.

With borders shared with five countries, the Northeast is a natural platform for India's Neighbourhood First and Act East policies,[c] aligning with its Indo-Pacific vision. Its strategic location also attracts Indo-Pacific powers seeking investment opportunities in the Bay of Bengal region.[d] Connectivity is thus being developed in the Northeast through domestic[e] and foreign investments.[4] However, the resurgence of ethnic violence in Manipur[5] and external disturbances in 2024 threaten this progress and challenge both human and state security in India.[f]

Impact of External Disturbances

The Northeast's proximity to neighbouring countries offers geopolitical advantages but also exposes it to external disturbances, particularly from Bangladesh, which borders four of the region's eight states.[g]

[a] The Northeast includes Assam, Meghalaya, Manipur, Mizoram, Tripura, Nagaland, Arunachal Pradesh, and Sikkim.

[b] The Northeast comprises 7.97 percent of India's territory and 3.78 percent of its population but contributes a modest 2.8 percent to India's GDP.

[c] India's "Neighbourhood First" policy was launched in 2008 and the "Act East" policy was launched in 2014.

[d] Northeast India borders five neighbouring countries: Bangladesh, Myanmar, Nepal, Bhutan, and China.

[e] The domestic initiatives include but are not limited to the Prime Minister's Development Initiative for North Eastern Region, PM Gati Shakti National Master Plan, and National Logistics Policy.

[f] National security has two elements: 'Human security' refers to the safety of people and 'State security' refers to the protection of a country's sovereignty and autonomy.

[g] Bangladesh shares borders with four of India's Northeastern states; Assam, Meghalaya, Mizoram, and Tripura.

The former Awami League government's strong counter-terrorism measures had eradicated several training camps and shelters of Indian insurgent groups in Bangladesh, contributing to cross-border stability.[6] However, the regime change in Dhaka in August 2024 and the subsequent release of Jama'at Mujahideen Bangladesh leaders necessitate increased surveillance[7] in the Northeast to counter clandestine activities of such groups. Although the Assam police have arrested operatives allegedly linked to the Ansarullah Bangla Team,[h,8] apprehensions prevail about future instability eroding the Northeast's developmental viability.

The Myanmar civil war, particularly the Arakan Army's (AA) capture of Rakhine state along the Bangladesh border in December 2024, has exacerbated tensions. While Sittwe, the state capital, remains under the Myanmar government's control, New Delhi is concerned about the future of its logistical projects along the Kaladan River, designed to improve the Northeast's connectivity. The AA's reported links with rebel groups such as United Liberation Front of Asom (ULFA), the National Socialist Council of Nagaland (Khaplang) [NSCN (K)][9] factions, and Kuki groups in the Northeast—facilitated by weapons and drug trafficking[10]—also have the potential to create instability in the region.

Illegal Migration

Illegal migration continued to be a pressing national security concern in 2024, with implications for demographic stability and internal security. Porous borders with Bangladesh and Myanmar enable undocumented migration, often orchestrated by well-organised transnational networks. These movements strain resources, disrupt ethnic harmony, and exacerbate regional tensions.

[h] Ansarullah Bangla Team is a Bangladesh-based militant group with reported links to Al-Qaeda.

As of May 2024, India hosted some 86,100 asylum seekers from Myanmar, including the Rohingya, but lacks a formal national refugee protection framework.[11] Many have taken refuge in Manipur and Mizoram, but under the Foreigners Act of 1946 and Passport Rules of 1950, 115 Myanmar nationals were detained and deported from Manipur between March and December 2024.[12]

The surge in violence in Bangladesh following last year's regime change, targeting minority communities such as Hindus, prompted attempts at mass migration into India.[13] However, heightened border patrols curbed cross-border movements. While precise asylum figures remain unavailable, the incidents underscored the region's vulnerability to migration crises.

The Free Movement Regime, facilitating India and Myanmar cross-border ties, faced scrutiny in 2024, with concerns about its discontinuation prompting resistance from Mizoram and Nagaland. Revised guidelines introduced at the end of December 2024 now allow residents within 10 km of the border to stay for up to seven days at designated points, aiming to curb illegal migration while allowing familial cross-border ties.[14]

Drug Trafficking

India's northeastern states, particularly those bordering Myanmar—a country that forms an integral part of the Golden Triangle—have seen an increase in drug seizures in recent years. This trend persisted in 2024, with some states in the region reporting notable confiscations.

In the first half of the fiscal year 2024-25, the Directorate of Revenue Intelligence seized 123 kg of methamphetamine across 11 cases, with a significant portion seized in Assam and Mizoram.[15] Between January and April 2024, Mizoram's Excise & Narcotics Department apprehended 2,297 individuals involved in drug trafficking and related activities.[16] These numbers underscore the region's ongoing battle with drug trafficking and its broader implications for security and public health. The surge in drug trafficking destabilises the region socially and economically, while insurgent groups exploit these routes for funding, fuelling narco-terrorism.[i,17]

[i] Both factions of the NSCN (NSCN-IM and Khaplang) reportedly collect 20% of drug values in Nagaland, while groups like the United National Liberation Front, People's Liberation Army, ULFA, and Kangleipak Communist Party sustain the operations through funds from drug and arms trafficking along Myanmar's borders.

To tackle this challenge, the 7th Myanmar-India Bilateral Meeting on Drug Control, held virtually in January 2024, emphasised international collaboration and the regulation of precursor chemicals. However, implementing these plans remains a pressing challenge, especially due to Myanmar's political instability. Strengthening border infrastructure, intelligence-sharing, and joint operations between India and Myanmar are critical to effectively combat the escalating drug menace.

Conclusion

India's Northeast region witnessed multiple challenges over the past year. Bangladesh's evolving political landscape and Myanmar's instability remain matters of serious concern, as they threaten to aggravate insurgencies in the region. Escalating concerns from drug trafficking and illegal migration further complicate its fragile equilibrium. While positive developments, such as the India-China agreement to resume border patrols along the Line of Actual Control from Ladakh to Arunachal Pradesh, offer hope for resolving a long-contested border issue,[18] security concerns dominate the current scenario. These realities will continue to shape Northeast's future, necessitating New Delhi to recalibrate its strategies to balance security imperatives with developmental aspirations and foster deeper regional and international partnerships.

Sohini Bose *is Associate Fellow, Strategic Studies Programme, ORF.*
Sreeparna Banerjee *is Associate Fellow, Strategic Studies Programme, ORF.*

Left-Wing Extremism

Decisive State Victory But Threats Persist

Niranjan Sahoo

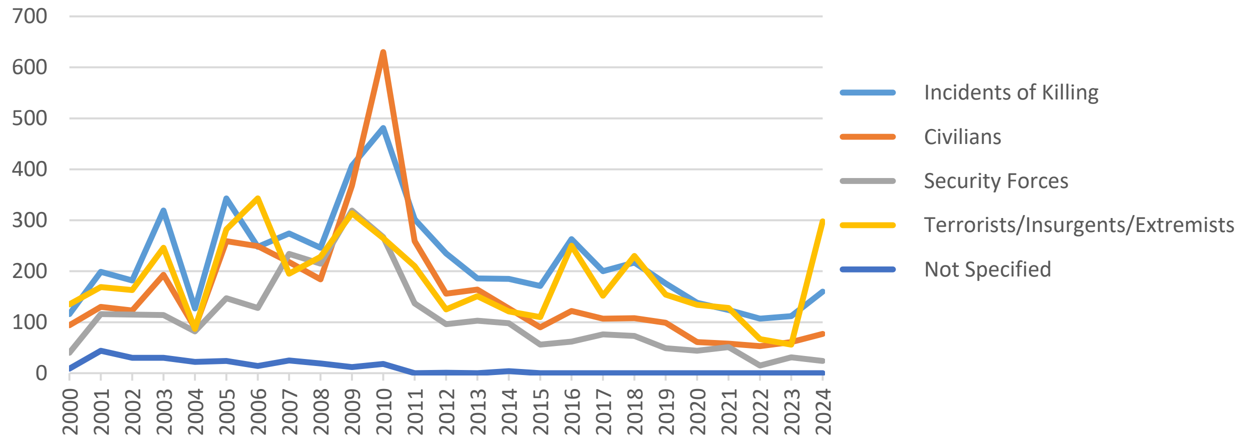
The year 2024 was a decisive one for India's counterinsurgency campaign against left-wing extremism. In its nearly six-decade existence, the Communist Party of India (CPI) (Maoist)[1] faced its biggest challenge for survival in 2024. The number of fatalities among the Maoists in 2024 alone is indicative; security forces eliminated 296 Maoists (Figure 1), many of them at the top and middle levels of the cadre, in addition to a large number of arrests and surrenders. Meanwhile, there were 24 fatalities among the security forces. The combined security forces were also able to breach strongholds of the Maoists, particularly several locations of the previously impenetrable Abujhmad in Chhattisgarh.[2] Three broad trends in counterinsurgency were clear in 2024.

Chhattisgarh Leads in Counterinsurgency Success

For a state that has been at the receiving end of Maoist domination since the late 2000s, Chhattisgarh provided the most decisive blow to the CPI (Maoist) in 2024. Combined operations (primarily by the District Reserve Guard, Border Security Force, Central Reserve Police Force, and State Special Task Force) eliminated a record 287 Maoists (more than 80 percent of the total casualties in the year), which included 14 top commanders.[3] Additionally, the forces arrested nearly 1,000 Maoist rebels and forced 837 of them to surrender to state police. Further, the combined forces successfully launched six major counterinsurgency operations in the year that resulted in heavy casualties among the Maoists. The biggest and most successful counter-operation was on 4 October 2024, when state forces eliminated 31 Maoists, including some top commanders in the forests of Abujmard.[4]

Besides these high casualties, in 2024, the state took control of territories long held by these groups and pushed them out of their strongholds. Improved road connectivity to previously inaccessible areas in the Bastar region allowed security forces to breach a number of the Maoists' fortresses. In February 2024, the joint forces flushed out Maoists from Puvarti, home of Maoist commander Hidma, and established a security post.

Figure 1: LWE-Related Fatalities (2000-2024)



Source: Ministry of Home Affairs (MHA) and South Asia Terrorism Portal, India

Abujhmad, which is the last recognised bastion of the Maoists, now has four police posts. In addition to decisive security actions, the state government dramatically improved its development outreach to tribal populations living in conflict zones under the Niyad Nellanar Yojana.[5]

Cooperative Federalism at its Best

The successes against the CPI (Maoist) in 2024 can be attributed to a strong partnership between the Centre and affected states across areas such as security, intelligence sharing, and development cooperation. The success in Chhattisgarh was aided by a proactive counterinsurgency push by the Centre and purposeful actions by the adjoining states. The Centre, particularly the Ministry of Home Affairs (MHA), oversaw security operations in "mission mode". While security-intelligence infrastructure and cooperation with Maoist-affected states were upgraded[6] under the United Progressive Alliance government between 2010 and 2013, these measures have been further strengthened under the National Democratic Alliance (NDA). The Centre, particularly the MHA, has strengthened security and intelligence cooperation with affected states and ensured improved coordination among other central agencies, such as National Investigation Agency (NIA), to target Maoist cadres and sympathisers. Maoist insurgency today remains limited to Abujhmad and a few tri-junction districts around Chhattisgarh, Jharkhand, Odisha, and Maharashtra.

A Maoist Revival?

Despite these gains, it would be premature to declare a comprehensive victory over the CPI (Maoist). Despite losing most of their territories and cadre strength, Maoists in their strongholds still have the capacity to inflict heavy casualties among security forces and cause large-scale damage to state infrastructure. The attack on a security convoy in Bijapur, Chhattisgarh, on 6 January 2025, which killed eight District Reserve Guard (DRG) personnel is telling. State leadership and the central security establishment need to maintain a grip on ongoing counterinsurgency operations and remain vigilant.

The year 2024 revealed three key trends concerning the Maoist insurgency. First, India's long pursuit of ending a bloody and protracted insurgency has reached a decisive stage, aided by resolute actions by Chhattisgarh—a state that has suffered from Maoist violence for the last two decades. Second, the central leadership has strengthened its outreach and collaborative efforts with Maoist-affected states and has addressed security-intelligence gaps to corner the rebels. Finally, despite the increasing threats to the CPI (Maoist), they still have the firepower in their strongholds to inflict damage on security forces. Thus, while there are several positive takeaways for 2025, one thing is clear: the battle against Maoist insurgency is not yet over.

Niranjan Sahoo *is Senior Fellow, ORF.*

Counterterrorism

Adapting to Emerging Challenges

Soumya Awasthi

India's fight against terrorism has been marked by both persistent challenges and notable progress. The past year saw an intensification of regional conflicts, as the increasing misuse of digital platforms and cryptocurrencies[1] by extremist groups has added to the complexity.

Looking ahead to 2025, India is at a pivotal moment. The accelerating pace of technological advancements, particularly in Artificial Intelligence and cybersecurity,[2] will shape the contours of terrorism and counter-terrorism. While these tools offer powerful new capabilities for pre-empting threats, they also provide opportunities for exploitation by state and non-state actors. As India prepares to navigate the uncertainties of the coming year, its ability to anticipate and adapt to these emerging challenges will be critical in safeguarding its national security.

Digital Radicalisation

The increased use of social media and online platforms by terrorist groups has emerged as one of the most pressing concerns for Indian authorities. Platforms like Rocket Chat, Telegram, and Twitter, and gaming platforms, too,[3] are being exploited for propaganda, recruitment, and planning. 'Lone wolves' and small terror modules are particularly vulnerable to such digital radicalisation, often orchestrated by groups like Islamic State and their affiliates.

In 2024, a number of incidents highlighted the crystallisation of this trend. For instance, an engineering student in Bengaluru was arrested for plotting an attack under the influence of Islamic State propaganda[4] accessed through encrypted messaging apps. The suspect had been engaging with extremist content for several months before getting apprehended. In recent months, numerous arrests have been reported from Gujarat,[5] Uttar Pradesh,[6] and Jammu & Kashmir (J&K),[7] involving individuals disseminating pro-terrorist propaganda videos. These incidents highlight the alarming and unchecked proliferation[8] of extremist content.

Recognising this threat, the Indian government has prioritised monitoring social media platforms and encrypted networks. Specialised cybercrime units[9] have been deployed to identify and neutralise such threats before they materialise. Initiatives by the Ministry of Home Affairs, Government of India, such as Cyber Dost[10] with social media companies like Facebook, Instagram, and Telegram, as well as radio campaigns, are also being strengthened to curb[11] the dissemination of terror-linked content.

Misuse of Cryptocurrencies for Terror Financing

Another emerging trend is the use of cryptocurrencies for financing terrorism. With the anonymity offered by blockchain technologies, cryptocurrencies[12] like Bitcoin and Ethereum are increasingly being used to fund terror activities, thus posing a challenge to financial regulators.

The State Investigation Agency in J&K revealed a nexus between Pakistan operatives[13] and separatist groups using cryptocurrencies to procure arms and ammunition. Furthermore, the National Investigation Agency unearthed digital wallets[14] linked to extremist groups that have received substantial transfers via cryptocurrencies'[15] international sources in cases like the Mangalore blast (2022), the Popular Front of India case (2022), and the Hurriyat case (2017).

To address this, the Indian government has introduced stricter regulations[16] on cryptocurrency exchanges and enhanced its collaboration with international agencies to trace illicit financial transactions. In November 2024,[17] India hosted a regional conference on financial terrorism in New Delhi, where participants discussed strategies to counter the misuse of digital payment systems by terrorist organisations.

Concerns about Jammu and Kashmir

J&K remains a hotspot for terrorist activities, with separatist groups backed by Pakistan continuing to pose a challenge. Despite improved counter-terrorism operations, cross-border infiltration[18] and attacks targeting civilians and security forces have persisted. Pakistan proxy groups[19] Kashmir Tigers and The Resistance Front remain active in the region.

In one instance, in June 2024,[20] security forces intercepted a drone carrying weapons and drugs in the Kathua district of Jammu sent by Pakistan-based operatives. Additionally, terrorist attacks on migrant labourers in Pulwama in October 2024[21] highlighted ongoing attempts to destabilise the socio-economic environment in the region.

Nevertheless, India's counter-terrorism efforts in J&K have achieved certain milestones. In September 2024, during Operation Khandara at Kathua,[22] security forces neutralised a high-profile Jaish e Mohammad commander involved in multiple attacks, showcasing improved intelligence and operational efficiency.

Conclusion

Challenges such as the misuse of cryptocurrencies, regional instability, and digital radicalisation remain pertinent issues in India's security framework, even as the country has made progress. India dramatically improved its ranking in the Global Terrorism Index in 2024,[23] indicating the reduced occurrence of terrorist attacks and the decrease in the absolute number of casualties. Tackling terrorists' use of advanced technology and implementing security reforms have enhanced India's counter-terrorism performance. India's firm stance at the global level on cross-border terrorism[24] has also shown its commitment to fighting terrorism. Its achievements in counterterrorism strategies make it clear that the country is rapidly progressing towards becoming a global leader for peace and stability at both the local and international levels.

Soumya Awasthi, *Fellow, Centre for Security, Strategy and Technology, ORF.*

Defence

Greater Impetus for Reforms and Exports

Kartik Bommakanti

Three key issues will shape India's defence priorities in 2025. Union Defence Minister Rajnath Singh has declared that 2025 will be the year of substantive defence reforms. A review of the previous year and projections for the current one indicate continued progress in India's defence modernisation. Key areas to watch include theaterisation, the continued implementation of the Agnipath scheme, and increase in defence exports.

Theaterisation

In 2024, the Modi government's initiative to establish Theatre Commands (TCs) gained momentum. In May 2024, the government notified the Inter-Services Organisation (Command, Control and Discipline) (ISO) Act, which received presidential assent in August 2023 and came into effect in 2024. This represents the most substantive reorganisation of the armed forces since independence in 1947, providing legal backing for the creation of TCs.This move follows the establishment of the Chief of Defence Staff in 2019.

Defence Minister Rajnath Singh announced in early September 2024 that the implementation of theaterisation would occur within 12 and 18 months, with the TCs likely to be operational in 2025. Three commands will be created: the China-focused Northern Theatre Command (NTC) in Lucknow, the Pakistan-focused Western Theatre Command (WTC), also in Lucknow, and the Maritime Command (MC) in Thiruvananthapuram.

As part of the reorganisation, the Indian Air Force (IAF) Southern Air Command and the Indian Army's (IA) Southern Western Command (SWC), previously based in Jaipur, will be dissolved. The IA's Central Command (CC) in Lucknow will either merge with one of the TCs or have its assets redistributed between them. Jointness and integration to enhance tri-service operational cooperation, as well as the development of tactical, technical, and procedural elements for integrated warfighting, will be a key focus in 2025.

Agnipath Scheme

The implementation of the TCs coincides with another key initiative, the Agnipath scheme, introduced in 2022. Under the scheme, recruits are commissioned for a maximum term of four years, after which only 25 percent will be retained for permanent commission. The scheme aims to reduce pension costs for the IA.

However, the scheme has invited criticisms, particularly from India's political opposition, certain sectors of the veterans community, and prospective recruits to the IA. The Ministry of Defence (MoD) may revise the scheme in response to demands for a higher retention rate, with some suggesting 50 percent or even 60-70 percent for regular units, and 75 percent retention for specialised technical branches such as the signals corps, air defence, and engineering. The IA has raised concerns that a 25-percent retention rate is too low to meet combat and operational requirements. As of writing, no final decision has been made regarding the percentage of personnel to be retained for permanent commission.

Defence Exports

In 2023-24, India's defence exports saw an increase, reaching INR21,083 crore (US$2.63 billion) a 32.5 percent rise from the previous fiscal year's INR15,940 crore.[1]

The MoD has set an export target of INR50,000 crore by 2029, with India achieving nearly half of that figure in 2023-24. Since 2013-14, defence exports have surged by 31 times, with the private sector contributing 60 percent and the Defence Public Sector Units (DPSUs) the remaining share.

India exported a wide range of items, primarily components and subsystems such as ammunition, spares, and fuses. Boeing and Lockheed Martin received aircraft components such as wings and fuselages, while India also exported complete weapons systems such as the BrahMos and the Akash missiles, Pinaka rockets, radars, Dornier-228 aircraft, and armoured vehicles. The revenue generated by this growing export sector is expected to reinvest in India's defence industries, enhancing the development of defence products.

Conclusion

2025 is likely to provide greater clarity on the implementation of TCs, given the emerging consensus, especially among the services. However, addressing the Agnipath scheme will remain critical and should be handled promptly. While the scheme is being refined based on feedback from stakeholders, delays or dilution could undermine its original goal of streamlining the armed forces by reducing personnel costs and fostering a younger, more technologically equipped military.

Defence exports are expected to maintain their upward trajectory, continuing the growth observed over the past decade. The surge in exports will drive improved product development and strengthen India's domestic defence industrial base.

Kartik Bommakanti *is Senior Fellow, Defence and National Security, Strategic Studies Programme, ORF.*

Intelligence

India's Secret Services Come in from the Cold

Archishman Ray Goswami

2024 will be remembered as the year when India's intelligence community marked itself as a key player on the world stage. Heightened volatility within India's neighbourhood pushed Indian intelligence towards expanding its operational focus on clandestine diplomacy. Information warfare against India, often orchestrated by its primary strategic rival, China, also grew in terms of scale and sophistication over the past year, presenting new counterintelligence challenges. And through the targeted deployment of its intelligence resources, India established itself as a notable international player within this space, dovetailing with New Delhi's growing influence on the world stage.

Clandestine Diplomacy Takes Centre-Stage

The past year saw growing volatility within India's neighbourhood, as Myanmar's civil war continued amid rapid advances by the rebel forces of the Three Brotherhood Alliance (TBA), and Bangladesh's pro-India administration under Sheikh Hasina was overthrown in August 2024. Amid these shifting dynamics, clandestine diplomacy, "where intelligence services are used to engage in secret and deniable discussions with adversaries",[1] became an element in Indian foreign intelligence activity overseas.

Shifting conflict dynamics in Myanmar over the past year compelled India to adopt a pragmatic strategic posture—one that is more accommodating of the influence of rebel groups and ethnic armed organisations (EAOs) to sustain India's domestic and regional interests. In September 2024, the Indian government invited key members of the TBA, such as the Arakan Army, to New Delhi for the first time,[2] following fruitful negotiations with the group in March to allow work on the Kaladan Multimodal Transport Corridor to continue unimpeded.[3] Correspondingly, deteriorating ties between the Taliban regime in Kabul and Islamabad provided India with an opportunity to improve its ties with Afghanistan, culminating in a January 2025 visit to Kabul by Foreign Secretary Vikram Misri—the highest-profile diplomatic visit by an Indian official to Kabul since August 2021.[4]

In both cases, it is highly likely that clandestine diplomatic encounters, facilitated by India's foreign intelligence service, the Research and Analysis Wing (R&AW) provided the impetus for the progress of both bilaterals. The R&AW has historically maintained contacts with both Myanmar's myriad insurgent groups[5] and the Afghan Taliban.[6] In the absence of sufficient formal diplomatic channels, it can be reasonably concluded that clandestine diplomacy, facilitated by interlocutors within the intelligence community, has underpinned these shifts in foreign policy.

Information Warfare: New Actors and Counterintelligence Challenges

In the past year, state-sponsored disinformation posed a greater challenge for Indian counterintelligence services, even as the threat landscape in this space changed. A ban on social media site X by Pakistani authorities in February 2024 has likely resulted in the noticeable drop since the late 2010s and early 2020s in disinformation campaigns from Pakistan, usually sponsored by its Inter-Services Intelligence (ISI). The vacuum, however, is being filled by actors with greater resources and increasingly sophisticated campaigns. Indian counterintelligence services, particularly the Intelligence Bureau (IB) and the National Technical Research Organisation (NTRO), will need to establish new offensive and defensive mechanisms to address these emerging challenges.

China also intensified its cyber-disinformation campaigns against India over the past year. A spike in disinformation and inflammatory material on social media related to the ethnic violence in Manipur was observed beginning in early 2024, and was later established by researchers at the Australian Strategic Policy Institute (ASPI) to have been amplified by Chinese intelligence-linked bots. Likewise, following an exposé by the *New York Times* in 2023 on Chinese-sponsored disinformation against countries, including India,[7] law enforcement in India filed a chargesheet in May 2024 against one of the named web portals maintaining a disproportionate focus on India.[8] Such instances capture the growing counterintelligence challenges posed to India in 2024 by the nebulous issue of state-sponsored disinformation—a problem that is only likely to grow in 2025.

India: A Global Intelligence Player?

The past year also saw India utilise its intelligence resources to exercise outsized influence on the world stage, marking New Delhi's arrival as a global intelligence player.

A series of successful anti-piracy operations in early 2024 by the Indian Navy and Special Forces in the Arabian Sea and Indian Ocean attracted global attention and were aided by the collection and sharing of real-time signals intelligence (SIGINT) by the Information Fusion Centre-Indian Ocean Region (IFC-IOR), the Navy's SIGINT processing and dissemination unit and a focal point of South Block's global intelligence liaison partnerships. Additionally, unsubstantiated allegations of covert action by Indian agencies overseas, particularly by sections of the Western media and their governments, indicate New Delhi's growing reputation as a global intelligence actor.

Such perceptions are markedly different from past assumptions of the Indian intelligence community's overwhelming regional concentration and are intertwined with India's growing geopolitical heft in a polycentric world order. As this influence grows into and beyond the mid-2020s, it is only natural that South Block's intelligence resources play a critical role in augmenting this renewed global salience.

Archishman Ray Goswami *is Non-Resident Junior Fellow, ORF; and MPhil candidate, University of Oxford.*

Maritime Security

Emerging Contours and Complexities

Sayantan Haldar

The maritime domain occupies an important position in India's national security strategy, making a departure from its historically continental focus. In an era of seaborne globalisation, and given India's geographic orientation, safeguarding maritime interests is crucial amid the looming challenges of the complex Indo-Pacific region. As a principal maritime security actor in the Indian Ocean and a key player in the Indo-Pacific security architecture, India plays a critical role in shaping the region's maritime security agenda.

As the maritime dimension of India's national security has steadily gained prominence over the recent years, three key trends highlight its evolving priorities. First, the commissioning of *INS Arighaat* has marked progress in India's nuclear deterrence. Second, India has intensified maritime cooperation through minilateral forums, responding to the Indo-Pacific's volatile geopolitical landscape. Third, emerging aspects of maritime security increasingly influence India's national security priorities.

Bolstering Deterrence Capabilities

The commissioning of *INS Arighaat,* a nuclear-powered ballistic missile submarine (SSBN), on 29 August 2024 at Vishakhapatnam strengthens India's nuclear triad and underscores its commitment to self-reliance in defence manufacturing. This priority has become increasingly critical as ongoing wars in Europe and West Asia strain global defence supply chains. As an economic and military power, India's quest for indigenous defence production reflects its growing security needs and strategic imperatives.

Nuclear deterrence in the Indian Ocean has remained a doctrinally embedded priority for India. The commissioning of *INS Arighaat* continues efforts to enhance India's sea-based nuclear deterrence, building on *INS Arihant*, operational since 2018. With *INS Aridhaman*, expected to be commissioned in early 2025, India is visibly advancing its nuclear triad to fortify its maritime deterrence capabilities.

Cooperation Through Collaboration

Maritime security has also become a focus of India's engagements with minilateral groups, particularly in the Indo-Pacific. In 2024, two developments underscored India's efforts to advance partnerships through these platforms. First, the Colombo Security Conclave expanded with the inclusion of Bangladesh and Mauritius, both critical players in the Indian Ocean region. Second, the Conclave was further institutionalised through the signing of a charter by India, Sri Lanka, Maldives, and Mauritius. Anchored in cooperation on national security issues, the forum's emphasis on maritime collaboration is set to enhance security efforts. This reflects India's continued commitment to fostering cooperation in the domain of maritime security with its littoral neighbours in the Indian Ocean.

Similarly, the Quad (India, Australia, Japan, and the US) has solidified its role as a key minilateral platform for India. While its agenda initially focused on maritime issues such as Humanitarian Assistance and Disaster Relief (HADR) and freedom of navigation, it has since expanded to include technological cooperation, people-to-people ties, and health security. Despite this broadening scope, maritime security remained a focus in 2024, serving as a key element of the group's geopolitical signalling in the Indo-Pacific. Following the Quad Leaders' Summit in Wilmington and the Foreign Ministers' Summit in Japan, joint statements emphasised the importance of a free and open Indo-Pacific, expressing concerns over aggressive and coercive actions in the region. This reaffirmed the Quad's commitment to a rules-based order, particularly amid escalating tensions in the South China Sea driven by China's aggressive behaviour.

New Dimensions of Maritime Security

India's maritime security outlook has evolved to prioritise new dimensions, particularly maritime domain awareness. As security challenges and technologies evolve, new frontiers are shaping India's preparedness. Enhancing cooperation through information sharing and dissemination is getting more attention. Cybersecurity, particularly in maritime security, is emerging as a critical area of focus. With the growing reliance on the oceans for shipping and energy, a robust cybersecurity architecture is essential to protect India's maritime interests and assets. In this context, the Gurugram-based Information Fusion Centre–Indian Ocean Region (IFC-IOR) has increasingly emphasised cybersecurity as a vital aspect of maritime security.

Sayantan Haldar *is Research Assistant, Strategic Studies Programme, ORF.*

Cybersecurity

China's Grey Zone Tactics

Sameer Patil

Intensifying external threats and expanding digital vulnerabilities have shaped India's cybersecurity landscape in the past few years. In 2024, three trends dominated this landscape for India: China's persistent attacks on critical national infrastructure; foreign attempts to disrupt general elections; and the government's attempts to further streamline national cyber architecture.

Continuing Cyberattacks from China

In the last few years, Chinese state-sponsored cyberattacks against Indian computer networks, particularly critical national infrastructure, have become a recurring trend. This is seen in the case of persistent breaches of power grids in Mumbai and Ladakh.[1] This trend continued in 2024, with Chinese threat actors casting their net wider to include other targets.

In August 2024, media reports revealed that Chinese state-sponsored threat actor Volt Typhoon, which is known to target critical national infrastructure in the United States (US), had reportedly breached an Indian internet service provider to harvest data.[2] In an earlier breach, an unidentified Chinese hacking syndicate had stolen approximately 95.2 gigabytes of Indian immigration data as part of a larger campaign targeting the government departments of a number of countries.[3]

In their state-sponsored campaigns, China has frequently used ransomware as a tool. In June 2024, it was revealed that the Chinese cyberespionage group ChamelGang, which regularly targets organisations in the US and Japan, was responsible for the December 2022 ransomware attack on the All India Institute of Medical Sciences,[4] which harvested the sensitive health data of high-ranking government officials.

Together, these attacks underscored the continued attempts of Chinese threat actors to disrupt the functioning of India's critical national infrastructure while conducting cyber espionage campaigns.

Disinformation, Misinformation, and Elections

Worldwide, rogue actors and adversarial autocratic regimes have intensified their efforts to target the core exercise of elections in democracies through cyberattacks, targeting election infrastructure and engaging in disinformation campaigns. This is seen in several states in Europe, the Indo-Pacific, and North America. India is no exception.[5]

Chinese efforts to launch disinformation campaigns were evident in the Lok Sabha elections in April-May 2024. Microsoft, in its threat intelligence assessment, warned that China may be relying on Artificial Intelligence-generated content via social media to target Indian voters in alignment with its geopolitical interests.[6] These disinformation campaigns blended well with the domestic political parties' use of deepfakes and other misinformation campaigns through WhatsApp and other social media platforms.[7] According to Microsoft, while the possibility of Chinese content influencing public opinion remains low, China will reap dividends in the long run. This is part of Beijing's broader campaign to target general elections in various countries, including the US.

These developments crystallised the trend in recent years, wherein China and Pakistan have amplified anti-India disinformation and propaganda in cyberspace. Chinese disinformation campaigns typically focus on India's military capabilities, New Delhi's rising global profile, and its expanding foreign engagement, while Pakistan seeks to exploit Indian domestic developments and the fragile situation in Kashmir valley.

Streamlining Cybersecurity Administration

In 2024, India took steps to refine its cybersecurity framework, addressing the complexities around multiple agencies and ministries working in the domain and whose work often overlaps. As part of this, in September 2024, the National Security Council Secretariat (where the National Cyber Security Coordinator's office is located) was made responsible for "the overall coordination and strategic direction for Cyber Security".[8]

Likewise, the Department of Telecommunications (Ministry of Communications) is now tasked with the security of telecommunication networks, and the Department of Internal Security (under the Ministry of Home Affairs) is in charge of cybercrime-related issues. The Ministry of Electronics and Information Technology will extend its support to other central ministries and departments on cybersecurity. This streamlining is hoped to enhance coordinated response and reduce inter-agency frictions and turf wars that characterise India's cybersecurity administration.

The military, too, advanced its efforts towards jointness by introducing the "Joint Doctrine for Cyberspace Operations" in June 2024 to guide its commanders in the planning and conduct of cyberspace operations.[9] The doctrine follows the creation of the Defence Cyber Agency in 2019, the tri-service command that controls and coordinates the cyber operations of the three services.[10]

These steps, though commendable, will be inadequate until India operationalises the long-overdue National Cyber Security Strategy, which can act as a guiding framework for deploying cyber capabilities. Given the rapid evolution of cyber threats, India must also expedite its institutional response.

Conclusion

In 2025, these trends will likely escalate, particularly the attacks on critical national infrastructure and disinformation operations, as China intensifies the use of grey zone tactics and steps up its malicious cyber activities against adversarial states. The People's Liberation Army's increasing focus on cyberspace is evident through the creation of Cyberspace Force and Information Support Force.[11] These dynamics will shape India's cybersecurity landscape and push New Delhi to adapt to emerging cyber realities.

Sameer Patil *is Director, Centre for Security, Strategy and Technology, ORF.*

II
Key Technologies

Space

Challenges to Innovation

Chaitanya Giri

2025 could be a milestone year for India's defence space activities. The launch of the first uncrewed Gaganyaan mission—the result of collaboration between the Department of Space, Ministry of Defence (MoD), and Ministry of Science and Technology, among others—is scheduled this year.[1,2] Additionally, the MoD has prioritised cyber, space, and emerging technologies—such as Artificial Intelligence, robotics, hypersonics, and machine learning—as key reform areas within "2025: The Year of Reforms"—an initiative aimed at modernising the armed forces.[3] To achieve its goals in space defence, the Indian government must focus on three areas: enabling domestic financial provisions for space innovation, reducing the time from proof-of-concept to mass commercial manufacturing, and ensuring smooth execution of the planned defence satellite constellation to be built under public-private collaboration.

Domestic Financial Provisions for Space Innovation

In 2024, the Department of Space allocated INR 1,000 crores to a government-led venture capital fund to finance growth-stage and late-stage space-sector companies. The fund will be disbursed in phases from the upcoming financial year 2025-26 until 2029-30 and aims to provide risk capital to startups that struggle to secure private equity or institutional loans for technology development.[4] Through this fund, the Department of Space aims to instill confidence in private investors to encourage investment in these companies and ensure that capital-strapped businesses do not migrate abroad.

The country has a thriving space innovation ecosystem that aligns with the goals of Aatmanirbhar Bharat. While the Indian government has taken commendable steps, efforts to motivate private domestic institutional investors to raise at least an equivalent amount will be crucial this year. The global economic slowdown led to India's space sector funding experiencing a decline of 55 percent, from US$130.2 million in 2023 to US$59.1 million in 2024.[5] With the emergence of geopolitical conflict hotspots and the increase in protectionist policies adopted by Western economies, foreign institutional capital will remain constrained. Any additional financing in 2025, whether from domestic or foreign investors, will hinge on how effectively the current cohort of late-stage startups can demonstrate their products and secure domestic and international business contracts. 2025 should be the year when the Department of Space emphasises the global competitiveness of the Indian space innovation ecosystem—in terms of not only capital infusion but also technology demonstration and subsequent commercialisation.

Shortening the Gap Between Innovation and Commercial Manufacturing

In the 21st Subroto Mukherjee Seminar on "Aatmanirbharta in Space: Way Ahead", Indian Air Force Chief Air Chief Marshal Amar Preet Singh lamented the slow pace of delivery of the first 40 fourth-generation Tejas fighter jets, which began in 2016. The tardiness of the manufacturer and the lack of competition in manufacturing are affecting the Air Force's stance even as opponent forces are adopting fifth- and even sixth-generation fighter jets.[6]

As part of the "Year of Reforms", the MoD must carry out exercises to understand how efficiently and speedily a crucial space technology or service can mature from a proof-of-concept stage to a standardised and certified technology ready for deployment by the armed forces. To that end, the Directorate of Standardisation within the Integrated Defence Staff must ensure clearly defined military standardisation and codification of space technologies procured from private space companies.

The smoothness and clarity of such processes will ensure quick commercial manufacturing and deployment of strategically crucial space technologies that are being supported by the Mission DefSpace Challenge undertaken by the Innovation in Defence Excellence programme.

Defence Satellites with Commercial Players

In 2024, the Cabinet Committee on Security, led by the prime minister, approved phase III of the Space-Based Surveillance programme, which includes the launch of at least 52 military satellites—a project with a designated budget of nearly INR 27,000 crores.[7] Currently, the National Security Council Secretariat and the Defence Space Agency, both of which are overseeing the programme, aim to have 21 satellites built by the Indian Space Research Organisation (ISRO) and the remaining 31 satellites developed by private space companies. This programme will be a game-changer for the private space ecosystem, who will benefit from independent contracts for the 31 satellites and supplies for the ISRO-built satellites. In 2025, private players will have the opportunity to work on military-grade space hardware and software, along with ongoing contracts to operate and maintain the satellites with the National Security Council Secretariat and Defence Space Agency.

Conclusion

Owing to the MoD's reformative stance, the Indian space ecosystem will experience multiple benefits in 2025. To achieve mutual goals, emphasis should be placed on increasing the indigenisation of components needed for building defence space paraphernalia while reducing supply chain vulnerabilities. A dedicated effort must be made to enhance the contribution of products that benefit from ongoing production-linked incentive schemes to address the needs of defence space technologies.

Chaitanya Giri *is Fellow, Centre for Security, Strategy and Technology, ORF.*

Nuclear Weapons

A More Complex Reality in the Making

Rahul Rawat

For India's nuclear domain, 2024 was an important year, with three key trends: India's development of strategic capabilities for effective deterrence; China's nuclear modernisation; and the emergent threat of a changing conception of coercion with the use of Strategic Non-Nuclear Weapons (SNNWs) in conflict. These developments impact India's security calculus and are likely to influence future actions.

Sharpening Indian Strategic Capabilities

In 2024, India successfully demonstrated a series of capabilities to strengthen its second-strike capabilities and survivability element as part of its No First Use (NFU)-based deterrence. In August, India commissioned[1] *INS Arighaat*, a second SSBN (Ship, Submersible, Ballistic, Nuclear) submarine after *INS Arihant* in the series,[2] to create a robust second-strike capability. Arighaat can launch K-4 Submarine-launched Ballistic Missiles, strengthening India's deterrence vis-à-vis China and Pakistan in the Indian Ocean Region.

The Agni 5 Multiple Independently-targetable Reentry Vehicle capability test[3] in March 2024 was another milestone in developing strategic missile capability, aimed primarily at China. The MIRV capability provides India with improved second-strike capability and narrows China's offensive strike intentions and options. In November 2024, India tested the first[4] long-range hypersonic cruise missile capable of carrying multiple payloads, fulfilling the objective of establishing deterrence via technology.

The successful Phase II testing[5] of the Ballistic Missile Defence (BMD) programme enhances strategic stability by reducing the vulnerability and enhancing the survivability of second-strike capabilities within the framework of the NFU. In the long term, a robust BMD could help India escape missile threats from Pakistan and China.

Chinese Nuclear Modernisation

China's nuclear modernisation amid frosty relations with India has intensified the gap in the two countries' asymmetrical military capabilities in addition to more sophisticated conventional long-range strike weapons and nuclear asymmetry. Reportedly, Beijing is set to resume[6] nuclear testing, with activities observed at Lop Nur site, and may test the new class of warheads and capabilities. China has developed a robust capacity for land-based Inter-Continental Ballistic Missiles (ICBMs) and Inter-mediate Range Ballistic Missiles (IRBMs) which, in the United States (US) Department of Defense's assessment, numerically surpasses[7] even those of the US. The Chinese DF ICBM series is primarily strategic and could carry both conventional and nuclear warheads. China's GDF-600,[8] a multi-payload hypersonic weapon, provides it with the advantage of speed and manoeuvrability.

Together, these developments suggest a change[9] in China's NFU posture. Given this acceleration and expansion of its arsenal, the security competition,[10] and the border dispute with India, the threat of nuclear escalation cannot be overlooked.

The China-Pakistan nexus worsens India's threat perceptions and forces it to respond through capability building to achieve a more effective yet calibrated deterrence posture. China has previously assisted Pakistan in JF-17 aircraft joint development[11] and has now integrated[12] with Ra'ad II nuclear-capable air-launched cruise missiles. The Pakistan Air Force also claims[13] to possess a hypersonic missile, thereby boosting its air-based deterrence against India. In the naval domain, Pakistan is seeking[14] China's help to develop a sea-based nuclear deterrent, which is currently limited to Babur III Submarine-launched Cruise Missile.

Coercive Role of SNNWs

The threat[15] of Tactical Nuclear Weapons (TNWs) is now combined with SNNWs, as evident from Russia's use of the Oreshnik missile against Ukraine in December 2024. SNNWs, especially long-range strike missiles, can be as devastating as[16] nuclear-based strikes, thus producing[17] strategic-level effects. At the same time, the impact of SNNWs can be regulated[18] by states through context-specific employment such as the nature of targets, end goals, and the coercive effect of the weapon on the adversary's denial capabilities. Thus, conventional nuclear distinction is transforming into a continuum through the increased use of SNNWs to gain strategic objectives.

The battlefield utility of SNNWs adds to the complexity[19] for decision-makers, who confront the issue of limited time to determine a counter-response. Consequently, they may force a rethinking of strategic redlines and the escalation matrix.

Following the Galwan clash, Indian policymakers began reflecting[20] on New Delhi's deterrence asymmetry vis-à-vis China. Its modernising DF-5 MIRV capabilities[21] can help China achieve offensive goals independently[22] and contribute to other functional roles. The use of SNNWs is intertwined with the Chinese goal of victory by eliminating the option of force survivability by hitting Indian targets in strategic depth. China may likely use SNNWs to deny India the option of escalation in the nuclear domain. Consequently, Indian policymakers need to enhance conventional, dual-role missile capabilities.

Conclusion

China's nuclear modernisation necessitates a change[23] in India's responses. Indian policymakers must adapt to the complex realities of the third nuclear age[24] in South Asia. There is a need to frame the country's strategic mindset as adversaries gain momentum in nuclear and SNNW capabilities. While India is developing, diversifying, and upgrading its missile force, it also needs to explore the role of TNWs[25] and SNNWs at the three levels of warfare:[26] tactical, operational and strategic. This will help resolve the complexities arising from the conventional nuclear continuum.

Rahul Rawat *is Research Assistant, Strategic Studies Programme, ORF.*

Chemical and Biological Weapons

India's Strategic Moves

Shravishtha Ajaykumar

India is dealing with a challenging environment in the domains of biological and chemical weapons. To prevent the future emergence of even more severe threats, India requires more effective strategies, including biosecurity and chemical weapons defence.

The inauguration of a new Biosafety Level 4 (BSL-4) laboratory at the Defence Research and Development Establishment (DRDE) in 2024 was an important step.[1] The high-tech centre was established to boost India's research and development in biological and chemical threats, which could enhance the development of advanced defence technology and the country's preparedness against high-risk pathogens.

Risks, Policy, and Defence Frameworks

Adding this second BSL-4 will help address biosafety and biosecurity concerns and outbreaks, to which India is vulnerable due to its population and climate. In the last decade alone, India has experienced multiple anthrax outbreaks, the most recent in April 2023 in Koraput District in Orissa.[2] Addressing the outbreaks and other public health concerns has been a challenge for the Indian government. The Department of Biotechnology (DBT), under the Ministry of Science and Technology, has been the central agency that governs all biosafety and biosecurity concerns and has been pivotal to the formation of the National Biotechnology Development Strategy (NBDS, currently in its second iteration, 2021-2025), catalysing the acceleration of innovations in the biological sciences field.[3] Nevertheless, along with potential benefits, there are clear risks in irresponsible use, innovation, and naturally occurring threats. In India, regulators, including the Genetic Engineering Appraisal Committee (GEAC), have addressed these risks, particularly concerning agriculture involving Genetically Modified Organisms (GMO) and the trade of genetically altered seeds and crops.[4]

While it ramps up biosecurity measures, India has also adopted an anticipatory position with regard to chemical weapons. As a signatory to the Chemical Weapons Convention (CWC) since 1997, India made considerable efforts to destroy its chemical weapon stockpiles and successfully destroyed its declared chemical weapons by 2009, well ahead of the CWC's deadline.[5] This responsibility includes intense, continued monitoring and regulation of chemical substances with dual-use capabilities so that chemicals that could be used for military purposes are tightly controlled. These responsibilities fall on the National Authority Chemical Weapons Convention (NACWC), which is in charge of chemical agent misuse, prevention, and adherence to CWC treaty obligations in India.

India's Recognition in Chemical Security

The establishment of the new BSL-4 under DRDE is also a response to global efforts in biochemical weapon defence and disarmament. Globally, India has shown its commitment to disarmament and responsible innovation in upholding the implementation of the CWC and the Biological Weapons Convention (BWC).

In November 2024, the India Chemical Council was recognised by the Organisation for the Prohibition of Chemical Weapons (OPCW) for exceptional contributions to the global chemical weapons disarmament cause.[6] Further, at the CWC Meeting of State Parties (MSP) in December 2024, India contributed 10,000 euros to the OPCW's Voluntary Fund for Assistance.[7] These resources fund emergency supplies, training, and medical equipment to address chemical weapon threats. India's commitment to the OPCW is a testament to the country's dedication to chemical weapons release and a world without arms. India has also regularly participated in these discussions, highlighting the need to enhance chemical security and participating in discussions on the emulsion of chemical security with emerging technology.

Additionally, India has actively contributed to the BWC and participated in its MSP in December 2024.[8] The meeting saw a number of discussions on enhancing the global framework for biosecurity and improving international cooperation in combating biological threats in a world with rapidly emerging disruptive technologies, including Artificial Intelligence.

Bilateral Cooperation for Track II Biosecurity

India's joint work with foreign partners is another aspect of its developing biosecurity and chemical weapons strategy. One notable collaboration has been a track II dialogue between India and the United States (US), co-hosted by the Regional Centre for Biotechnology Department of Biotechnology in the Indian Ministry of Science and Technology and the Johns Hopkins Center for Health Security (CHS). Supported by the CHS, the two countries have built on their cooperation in biosecurity and are seeking ways to strengthen surveillance, facilitate the sharing of critical information between countries and among bodies, and strengthen partnerships between their experts to improve biosecurity.[9] The shared experience of the two countries in the context of heightening biosecurity risks can serve as a template for future international collaborations on biodefence and biosecurity.

Conclusion

India is strengthening its capabilities by implementing the right policy approach, collaborating internationally, and innovating in technology. It is also participating in global initiatives for disarmament and non-proliferation. The emerging patterns in India's biosecurity and chemical weapons industries are highlighting the emerging role of resilience and preparedness in responding to the challenges of a dynamic threat environment.

Shravishtha Ajaykumar *is Associate Fellow, Centre for Security, Strategy and Technology, ORF.*

Quantum Technology

India Solidifies Foundation

Prateek Tripathi

The Quantum Technology (QT) landscape experienced a sizeable shift in 2024, marking a critical juncture in its evolution. While the year witnessed a surge in innovation in areas such as quantum computing (QC), progress was tempered by the announcement of new export control regulations and the ongoing global attempt to decouple from China.

India solidified its foundation in the domain through the launch of its National Quantum Mission (NQM) and the subsequent establishment of four Thematic Hubs (T-Hubs) at premier institutions across the country. These hubs are envisioned to attract both domestic and foreign talent and investment, playing a crucial role in the future development of this nascent yet critical technology. However, the security implications of QT pose a challenge for India, particularly when it comes to international collaboration, which is pivotal for advancing any emerging technology.

Developments in Quantum Technology

The national security implications of QC cannot be overstated. A large-scale quantum computer is capable of dismantling most of the current security encryption protocols in a matter of seconds.

The year concluded with Google announcing its Willo processor in December,[1] claiming that its error correction scales exponentially with the number of qubits. This shift towards error correction marks a turning point in the development of QC, potentially ushering in the era of practically useful quantum computers. India is advancing QC through its NQM, with institutions such as the Tata Institute for Fundamental Research (TIFR) and IIT Mandi leading the charge. TIFR Mumbai, along with the Defence Research and Development Organisation, successfully tested a 6-qubit quantum computer in 2024, with plans to complete it imminently.[2] Startups are also entering the field, with Bengaluru-based QpiAI securing US$6.5 million in its first external investment round in June.[3] The year should serve as a learning experience for the country, encouraging a shift toward error correction and scalability, rather than focusing on increasing the numbers of qubits.

Due to its importance in enabling secure communication, India has been pursuing both free-space and fibre-optic quantum communication. While institutions such as IIT Madras and the Indian Space Research Organisation (ISRO) have been active in this field, the Physical Research Laboratory (PRL) in collaboration with Centre for Development of Telematics (C-DOT) was able to demonstrate both fibre-optic and free space-based quantum key distribution in March.[4]

A number of institutions are also working on quantum sensing and quantum materials. The Raman Research Institute (RRI) has made breakthroughs in quantum magnetometry and quantum optics in 2024, holding massive potential for quantum sensing.[5] A spinoff company from the institute, nexAtom Research and Instruments, was established earlier in the year and will manufacture precision laser systems for quantum optics laboratories.[6]

The Rise of Export Controls

In addition to QC, developments in quantum communication and quantum sensing have prompted nations across the world to enact strict export control regulations on QT, due to their potential military applications. For instance, the United States, United Kingdom, France, Spain, Netherlands, and Canada have all enacted nearly identical export controls on quantum computers possessing 34 or more physical qubits at a specified error rate.[7]

QT is still in its early stages and requires substantial investment before it can become commercially viable. Consequently, these regulations pose a challenge for QT development, particularly for developing nations like India, which lack the economic power of countries like the US. For India, overcoming these restrictions will require strategic geopolitical manoeuvring, attracting and nurturing talent, and encouraging more investments in the field.

Implications of Decoupling from China

The global push for decoupling from China could impact the development of QT, primarily because QT hardware manufacturing requires limited raw materials, including semiconductors and rare-earth metals, for which China plays a critical role in the global supply chain. While recent initiatives such as the US CHIPS and Science Act (2022) and the US–India Initiative on Critical and Emerging Technology (iCET) aim to address these gaps, building alternative supply chains for materials like semiconductors is a complex, resource-intensive process that will likely take years. In the meantime, procuring these materials presents a global challenge for the evolution of QT.

In addition to initiatives like the iCET, international cooperation will be critical for India's pursuit of QT. The precedent has been set through the Quad, with initiatives such as the Quad Investors Network (QUIN) and the Quad Center of Excellence in Quantum Information Sciences, both established in 2023. Other minilateral initiatives, such as the India-South Korea-US Trilateral Technology Cooperation agreement initiated in 2023, also hold promise. Furthermore, multilateral platforms such as the United Nations offer viable avenues for collaboration. The groundwork for this has already been laid with the UN's official declaration of 2025 as "The International Year of Quantum Science and Technology," which emphasises its recognition of QT's importance for the future of humanity.[8]

Prateek Tripathi *is Junior Fellow, Centre for Security, Strategy and Technology, ORF.*

Artificial Intelligence and Drones

India’s Strategic Embrace

Amoha Basrur

The technological developments driven by the wars in Ukraine and Gaza continued in 2024, with both conflicts serving as testing grounds for cutting-edge Artificial Intelligence (AI) and drone technologies. While India is not at the forefront of the development and use of these technologies, they play an important part in its defence strategy and considerations. This is evident in three main areas: the securitisation of AI, the deployment and countering of drones along the border, and the challenges arising from the proliferation of non-state actors.

Securitisation of AI

As global technology competition heightens, AI has become a critical component of the race. Aware of China’s significant advancements, India has taken steps to bolster its AI preparedness. In March 2024, it established the Signals Technology Evaluation and Adaptation Group to advance military communications technologies, including AI.[1] The defence establishment has also strengthened collaboration with the private sector and academia to foster innovation in defence AI. The Indian Army established an AI Incubation Centre in partnership with Bharat Electronics Limited,[2] and the Defence Research and Development Organisation (DRDO) has collaborated with the Indian Institute of Technology Bhubaneswar for undertaking AI-based surveillance projects.[3] To accelerate AI integration, the Ministry of Defence (MoD) launched the Evaluating Trustworthy Artificial Intelligence Framework and Guidelines in October.[4] These efforts mark a shift towards transforming India’s national security and defence framework with AI as a key driver.

Drones and Border Security

India has been actively developing its domestic drone manufacturing ecosystem since 2021, with efforts accelerating in 2024. To strengthen border security, the Indian Army installed anti-infiltration grids along the Line of Control, incorporating UAVs.[5] Additionally, a man-portable counter-drone system was installed in Jammu and Kashmir to address growing drone threats.[6] The Union Home Minister, Amit Shah, has announced the government's intent to create a comprehensive anti-drone unit to secure its borders.[7]

A notable development in October 2024 was India's agreement with the US to procure 31 armed MQ-9B SkyGuardian and SeaGuardian drones.[8] These drones will be crucial for maritime operations, providing real-time intelligence and reconnaissance support, particularly in the Indian Ocean Region. The deal is an exception to India's drone import restrictions due to the technology's strategic importance. Growing national security concerns also led the Indian Army to halt the acquisition of 200 logistics drones in the first half of the year.[9] These drones, intended for the India-China border, were flagged after allegations that Chinese parts were used in their manufacture.[10] In June 2024, the MoD cautioned Indian manufacturers against the use of Chinese components in military drones after intelligence agencies expressed concern about potential security risks.[11]

Proliferation of Non-State Actors

A key concern as these technologies evolve is their use by non-state actors. In 2024, 286 drones were seized along the India-Pakistan border,[12] a sharp increase from 110 in 2023.[13] These drones were primarily used for smuggling arms and drugs, with hotspots in Punjab, as well as incidents in Rajasthan and Jammu. In an unprecedented event, militants in Manipur used locally assembled drones to launch rocket-propelled grenades, marking a troubling development in the conflict.[14]

In India, the primary concerns surrounding AI are the rise in AI-driven information warfare and cyberattacks. During the 2024 elections, there was a surge in deepfakes and disinformation.[15]

Although these did not have the catastrophic effect on democracy that some feared, they remain a cause for concern as AI tools complicate efforts to distinguish between authentic and manipulated information. Indeed, India was the second-most targeted nation for cyberattacks in 2024,[16] with a 46-percent increase in attacks from the previous year.[17] This rise is partly attributed to AI's role in automating malware creation, refining phishing campaigns, and developing adaptive attack strategies.

Conclusion

The developments in 2024 indicate India's ongoing strategic embrace of emerging technologies. With a focus on indigenisation and aligning with global defence trends, India will continue to invest heavily in military AI and drones. Going into 2025, India must ensure that these investments effectively tackle the dynamic challenges of its national security landscape.

Amoha Basrur *is Junior Fellow, Centre for Security, Strategy and Technology, ORF.*

Endnotes

China's PLA
India's Strategic Concerns

1 Liu Chenghui, "China's next-generation fighter jet images blew up foreign media: shocking! China's aviation industry has achieved another milestone [中国下一代战机画面引爆外媒：震撼！中国航空工业实现了又一里程碑]," *Observer News Network*, December 27, 2024, https://www.guancha.cn/internation/2024_12_27_760307.shtml

2 Atul Kumar, "Corruption and the purge in the PLA: Apprehension and distrust," *ORF Expert Speak,* December 02, 2024, https://www.orfonline.org/expert-speak/corruption-and-purge-in-the-pla-apprehension-and-distrust

3 Huaxia, "Xi Focus: Xi stresses PLA's political loyalty at crucial meeting held in old revolutionary base," *Xinhua,* June 19, 2024, https://english.news.cn/20240619/f978a22b64bb450bbde978d3869c2425/c.html

4 "The Information Support Force of the Chinese People's Liberation Army was officially established! [中国人民解放军信息支援部队，正式成立！]," *Xinhua,* April 22, 2024, https://tyjr.sh.gov.cn/shtyjrswj/sjxx/20240422/5131cb10c38b444d813ccd77ea26044f.html

5 Wang Liyong, "Building a unified network information space for joint operations [打造联合作战统一网络信息空间]," *Liberation Army Daily,* February 22, 2018, http://www.81.cn/jfjbmap/content/2018-02/22/content_200081.htm

6 "The world's first catapult-type "drone carrier"! Take a quick look at the powerful capabilities of the Type 076 amphibious assault ship [全球首艘弹射型"无人机航母"！带你速览076型两栖攻击舰的强大能力]," *CCTV,* December 28, 2024, https://news.sina.cn/gn/2024-12-28/detail-ineayftc1928865.d.html; Liu, "China's next-generation fighter jet images blew up foreign media: shocking! China's aviation industry has achieved another milestone;" Zhong Xinjun, "Farewell to the old and usher in the new, a group of powerful national weapons appeared [辞旧迎新，大国利器组团亮相]," *China News Network,* January 03, 2025, https://www.chinanews.com.cn/sh/2025/01-03/10346897.shtml.

Jammu and Kashmir
Steadfast Zero-Tolerance Policy

1 Ravi Krishnan Khajuria, "Bodies of 2 Jammu village guards killed by terrorists found," *Hindustan Times,* November 9, 2024, https://www.hindustantimes.com/india-news/bodies-of-2-jammu-village-guards-killed-by-terrorists-found-101731092713247.html

2 Rajeev Ranjan, ""60% Terrorists Killed In 2024 Were Pakistani": Army Chief On J&K Situation," NDTV, January 13, 2025, https://www.ndtv.com/india-news/army-chief-gen-upendra-dwivedi-on-situation-at-india-pakistan-border-loc-india-china-border-lac-7462271

3 KL News Network, "27 Militants Killed in 19 Gunfights Across North Kashmir in 2024," *Kashmir Life*, December 27, 2024, https://kashmirlife.net/27-militants-killed-in-19-gunfights-across-north-kashmir-in-2024-377582/

Northeast Region

Disturbances Threaten Progress

1 Aarti Betigeri, "India's northeast: An integral piece of the puzzle," *The Interpreter*, February 2, 2022, https://www.lowyinstitute.org/the-interpreter/india-s-northeast-integral-piece-puzzle

2 Soumya Bhowmick, "India's Northeast: Partnerships for economic prosperity," Observer Research Foundation, April 22, 2024, https://www.orfonline.org/expert-speak/india-s-northeast-partnerships-for-economic-prosperity#:~:text=India's%20Northeast%2C%20with%20its%20rich,2.8%20percent%20of%20India's%20GDP.

3 Ministry of Home Affairs, North East Division, Government of India, *Major Initiatives and Peace Process in North Eastern Region (NER)* (New Delhi: Ministry of Home Affairs, 2024), https://www.mha.gov.in/sites/default/files/2024-01/NE_MajorInitiativesPeaceProcess_22012024.pdf

4 Rupakjyoti Borah, "Japan's Infrastructure Investment in Northeast India," *The Diplomat,* February 6, 2022, https://thediplomat.com/2022/02/japans-infrastructure-investment-in-northeast-india/

5 Mayuresh Konnur, "Waiting for peace in Indian state divided by violence," *BBC*, August 9, 2024, https://www.bbc.com/news/world-asia-india-66260730

6 Sohini Bose, "Concluding the 'Golden Chapter'," Observer Research Foundation, August 6, 2024, https://www.orfonline.org/expert-speak/concluding-the-golden-chapter

7 Prabin Kalita, "Terror alert in NE over Bangladesh outfits' plan to target region," *Times of India*, November 8, 2024, https://timesofindia.indiatimes.com/city/guwahati/heightened-terror-alerts-in-northeast-india-due-to-jmb-activities/articleshow/115059570.cms

8 Kalita, "Terror alert in NE over Bangladesh outfits' plan to target region"

9 Ministry of Home Affairs, Government of India, *Notifications under the Unlawful Activities (Prevention) Act UAPA, 1967*, https://www.mha.gov.in/en/commoncontent/notifications-under-unlawful-activities-prevention-act-uapa-1967

10 Chandrakala Choudhury, "The Rise Of Arakan Army & Fall Of Rakhine State: What It Means For India, Northeast Security," *ETV Bharat*, January 3, 2025, https://www.etvbharat.com/en/!international/the-rise-of-arakan-army-and-fall-of-rakhine-state-what-it-means-for-india-northeast-security-enn25010303584

11 "India: Immediately halt forced returns of Myanmar refugees in Manipur and respect the non-refoulement principle," *ICJ*, May 10, 2024, https://www.icj.org/india-immediately-halt-forced-returns-of-myanmar-refugees-in-manipur-and-respect-the-non-refoulement-principle/#:~:text=India%20hosts%2086%2C100%-20refugees%20and,Chin%20State%20and%20Magway%20Region.

12 "Manipur Deports 26 Myanmar Nationals, Reaffirming Stance On Illegal Migration," *NDTV*, January 6, 2025, https://www.ndtv.com/video/manipur-deports-26-myanmar-nationals-reaffirming-stance-on-illegal-migration-884662

13 "BSF sends back 1,000 men, mostly Hindus at India-Bangladesh border in Cooch Behar district," *The Hindu*, August 10, 2024, https://www.thehindu.com/news/national/bsf-sends-back-1000-men-mostly-hindus-at-india-bangladesh-border-in-cooch-behar-district/article68508490.ece#:~:text=Tension%20prevailed%20at%20the%20Sitalkuchi,to%20India%20and%20seek%20refuge.

14 Prawesh Lama, "Myanmarese living within 10km of Manipur border can enter state with a pass: MHA letter," *Hindustan Times*, December 25, 2024, https://www.hindustantimes.com/india-news/myanmarese-living-within-10km-of-manipur-border-can-enter-state-with-a-pass-mha-letter-101735067656873.html

15 “DRI seizes 123 kg Methamphetamine in H1FY25; max cases in Assam, Mizoram,” *Business Standard*, December 8, 2024, https://www.business-standard.com/india-news/dri-seizes-123-kg-methamphetamine-in-h1fy25-max-cases-in-assam-mizoram-124120800134_1.html

16 Sreeparna Banerjee, “From Poppy Fields to Black Markets: Understanding the Drug Trade Across India and Myanmar,” Observer Research Foundation, October 3, 2024, https://www.orfonline.org/research/from-poppy-fields-to-black-markets-understanding-the-drug-trade-across-india-and-myanmar#_edn55

17 Banerjee, “From Poppy Fields to Black Markets: Understanding the Drug Trade Across India and Myanmar.”

18 “India says it reached deal with China on army patrols along disputed border,” *Al Jazeera*, October 21, 2024, https://www.aljazeera.com/news/2024/10/21/india-says-it-reached-deal-with-china-on-army-patrols-along-disputed-border

Left-Wing Extremism
Decisive State Victory But Threats Persist

1 South Asia Terrorism Portal (SATP), https://satp.org/terrorist-profile/india/communist-party-of-india-maoist-cpi-maoist-all-its-formations-and-front-organizations

2 Prawesh Lama, “Security forces take on Maoists in terrain unchartered since British Era,” *Hindustan Times*, October 2, 2024, https://www.hindustantimes.com/india-news/security-forces-take-on-maoists-in-terrain-uncharted-since-british-era-101727866811102.html

3 Rahul Tripathi, “4 Maoists killed in Bastar, search operation still on,” *The Economic Times*, January 5, 2025, https://economictimes.indiatimes.com/news/defence/4-maoists-killed-in-bastar-search-operation-still-on/articleshow/116971632.cms?from=mdr

4 Mayank Kumar, “31 Maoists killed in Chhattisgarh’s biggest anti-naxal op: How security forces plotted the deadly onslaught,” *The Print*, October 4, 2024, https://theprint.in/india/28-maoists-killed-in-chhattisgarhs-biggest-anti-naxal-op-how-security-forces-plotted-deadly-onslaught/2297868/

5 Sumi Rajappan, “Chhattisgarh’s Niyad Nellanar scheme boosts development in vulnerable areas,” *India Today*, November 27, 2024, https://www.indiatoday.in/india/story/chhattisgarhs-solar-powered-initiative-boosts-development-in-vulnerable-areas-2640759-2024-11-27

6 Niranjan Sahoo, “Half a Century of India’s Maoist Insurgency: An Appraisal of State Response,” *ORF Occasional Paper*, 2019, https://www.orfonline.org/search?q=half-a-century-of-indias-maoist-insurgency-an-appraisal-of-state-response-51933

Counterterrorism
Adapting to Emerging Challenges

1 Soumya Awasthi, comment on “Exploring the nexus: Cryptocurrency, Zakat, and Terror Funding,” Observer Research Foundation, comment posted May 08, 2024, https://www.orfonline.org/expert-speak/exploring-the-nexus-cryptocurrency-zakat-and-terror-funding (Accessed January 2, 2025)

2 Morgan Stanley, “AI and Cyber Security: A New Era: Morgan Stanley,” https://www.morganstanley.com/articles/ai-cybersecurity-new-era

3 Soumya Awasthi, comment on “Gaming Platforms: A new Frontier for extremist recruitment and radicalization,” Observer Research Foundation, comment posted

December 05, 2024, https://www.orfonline.org/expert-speak/gaming-platforms-a-new-frontier-for-extremist-recruitment-and-radicalisation (Accessed January 02, 2025)

[4] Sagay Raj and Karishma Saurabh Kalita, “Bengaluru Cafe blast mastermind 'high value' ISIS asset in India: Top points,” *India Today,* April 13, 2024, https://www.indiatoday.in/india/story/bengaluru-cafe-blast-mastermind-high-value-isis-asset-in-india-top-points-2526700-2024-04-13

[5] HT News Desk, “4 suspected ISIS terrorists from Sri Lanka arrested at Ahmedabad airport,” *Hindustan Times,* May 20, 2024, https://www.hindustantimes.com/india-news/4-isis-terrorists-hailing-from-sri-lankan-arrested-at-ahmedabad-airport-101716197479673.html

[6] PTI, “Uttar Pradesh ATS arrests four men allegedly linked to ISIS’ Aligarh module,” *The Hindu*, November 12, 2023, https://www.thehindu.com/news/national/other-states/uttar-pradesh-ats-arrests-four-men-allegedly-linked-to-isis-aligarh-module/article67526904.ece

[7] The Hindu Bureau, “Four ‘terrorist associates’ arrested at Tral in J&K,” *The Hindu*, January 01, 2025, https://www.thehindu.com/news/national/jammu-and-kashmir/four-terrorist-associates-arrested-at-tral-in-jk/article69050756.ece

[8] PTI, “Three Arrested in Kashmir for Circulation of ISIS Propaganda,” *NDTV,* July 12, 2021, https://www.ndtv.com/india-news/three-arrested-in-jammu-and-kashmirs-anantnag-for-circulation-of-isis-propaganda-2485088

[9] Neeraj Chauhan, “Specialised unit within NIA to lead probes into cyberattacks,” *Hindustan Times,* August 12, 2023, https://www.hindustantimes.com/india-news/specialised-unit-within-nia-to-lead-probes-into-cyberattacks-101691867415960.html

[10] Ministry of Electronics and Information Technology, *Cyber Dost*, by C-DAC Vikaspedia, https://education.vikaspedia.in/viewcontent/education/digital-literacy/cyber-dost?lgn=en

[11] Ministry of Women and Child Development, Government of India, https://pib.gov.in/PressReleseDetailm.aspx?PRID=2085609&reg=3&lang=1

[12] Clara Broekaert, “Blockchain and Bloodshed: The Role of Cryptocurrencies in Terrorist Financing,” The Soufan Center, October 16, 2024, https://thesoufancenter.org/intelbrief-2024-october-16/ (Accessed January 02, 2025)

[13] Zulfikar Majid, “ISI using Bitcoin trade to fund terrorism in J&K: SIA probe,” *Deccan Herald,* August 03, 2022, https://www.deccanherald.com/india/isi-using-bitcoin-trade-to-fund-terrorism-in-jk-sia-probe-1132614.html#google_vignette

[14] The Hindu Bureau, “India has seized significant amounts from proscribed terrorists: FATF,” *The Hindu,* September 21, 2024, https://www.thehindu.com/news/national/india-has-seized-significant-amounts-from-proscribed-terrorists-fatf/article68664709.ece

[15] Soumya Awasthi, comment on “Exploring the nexus: Cryptocurrency, Zakat, and Terror Funding,” Observer Research Foundation, comment posted May 08, 2024, https://www.orfonline.org/expert-speak/exploring-the-nexus-cryptocurrency-zakat-and-terror-funding (Accessed January 2, 2025)

[16] Dipanita Saha, comment on “The New Age of Crypto: India’s 2024 Regulatory Framework Unveiled,” Impact and Policy Research Institute, comment posted September 09, 2024, https://www.impriindia.com/insights/crypto-india-regulatory-framework/#:~:text=Anti%2DMoney%20Laundering%20(AML)%20and%20Know%20Your%20Customer%20(,KYC%20requirements%20on%20crypto%20businesses (Accessed January 03, 2025)

[17] Ministry of Home Affairs, Government of India, https://pib.gov.in/PressReleaseIframePage.aspx?PRID=2071250

[18] Auqib Javeed, “Surge in Attacks brings fear to calmer parts of Kashmir,” *BBC*, July 24, 2024, https://www.bbc.com/news/articles/c728l7n57n7o

[19] Ayjaz Wani, comment on “Pakistan’s proxy war intensifies in Kashmir,” Observer Research Foundation, comment posted December 07, 2024, https://www.orfonline.org/expert-speak/pakistan-s-proxy-war-intensifies-in-kashmir

[20] PTI, “Pakistani drone loaded with arms shot down by BSF along IB in J&K,” *Times of India*, June 20, 2020, https://timesofindia.indiatimes.com/india/bsf-shoots-down-drone-that-entered-jks-kathua-from-pakistan/articleshow/76476385.cms

21 Peerzada Ashiq, “Two Jawans, two Army porters injured in militant attack in J&K’s Baramullah,” *The Hindu*, October 25, 2024, https://www.thehindu.com/news/national/soldiers-injured-in-attack-on-army-vehicle-in-jammu-and-kashmir-baramulla/article68792552.ece

22 News Desk, “Two terrorists killed during encounter with security forces in J&K’s Udhampur,” September 11, 2024, https://timesofindia.indiatimes.com/india/encounter-breaks-out-between-security-forces-and-terrorists-in-jammu-kashmirs-udhampur/articleshow/113255861.cms

23 Institute for Economics & Peace, *Global Terrorism Index 2024*, https://www.economicsandpeace.org/wp-content/uploads/2024/02/GTI-2024-web-290224.pdf

24 Lok Sabha Secretariat, Parliament House, Government of India, https://sansad.in/getFile/lsscommittee/External%20Affairs/pr_files/PRESS%20RELEASE%20GLOBAL%20TERRORISM.pdf?source=loksabhadocs

Defence

Greater Impetus for Reforms and Exports

1 Bhaswar Kumar, “Indian Defence Exports: From BrahMos to Akash, Who are the Major Buyers?,” *Business Standard,* October 28, 2024, https://www.business-standard.com/external-affairs-defence-security/news/indian-defence-exports-from-brahmos-to-akash-who-are-the-major-buyers-124102800396_1.html.

Intelligence

India’s Secret Services Come in from the Cold

1 Len Scott, “Secret Intelligence, Covert Action and Clandestine Diplomacy,” *Intelligence and National Security* 19, no. 2 (2004): 330.

2 Wa Lone and Devjyot Ghoshal, “Exclusive: India extends unprecedented invite to Myanmar's anti-junta forces, sources say,” *Reuters*, September 23, 2024, https://www.reuters.com/world/asia-pacific/india-extends-unprecedented-invite-myanmars-anti-junta-forces-sources-say-2024-09-23/.

3 Kallol Bhattacherjee, “Rajya Sabha member, team meet rebel Arakan Army inside Myanmar, discover poor condition of Kaladan project on Myanmar side,” *The Hindu,* March 1, 2024, https://www.thehindu.com/news/national/indian-delegation-led-by-rajya-sabha-member-vanlalvena-meets-rebels-of-myanmar-to-discuss-infrastructure/article67902979.ece

4 Sudha Ramachandran, “India Steps Up Engagement with the Taliban Regime,” *The Diplomat,* January 10, 2025, https://thediplomat.com/2025/01/india-steps-up-engagement-with-the-taliban-regime/

5 Randeep Ramesh, “Burmese rebels accuse India of betrayal,” *The Guardian,* October 8, 2007, https://www.theguardian.com/world/2007/oct/08/india.burma

6 Rushita Shetty, “My Enemy’s Enemy: India in Afghanistan from the Soviet Invasion to the US Withdrawal by Avinash Paliwal,” *CLAWS*, October 7, 2021, https://www.claws.in/my-enemys-enemy-india-in-afghanistan-from-the-soviet-invasion-to-the-us-withdrawal-by-avinash-paliwal/

7 Mara Hvistendahl et al., “A Global Web of Chinese Propaganda Leads to a U.S. Tech Mogul,” *The New York Times*, August 5, 2023, https://archive.ph/pVfm0

8 Ujwal Jalali, “NewsClick case: Delhi Police chargesheet says funds taken for ‘anti-India’ agenda,” *The New Indian Express,* May 2, 2024, https://www.newindianexpress.com/cities/delhi/2024/May/02/newsclick-case-delhi-police-chargesheet-says-funds-taken-for-anti-india-agenda

Cybersecurity
China's Grey Zone Tactics

1 Insikt Group, "Continued Targeting of Indian Power Grid Assets by Chinese State-Sponsored Activity Group," Recorded Future Blog, April 6, 2022, https://www.recordedfuture.com/continued-targeting-of-indian-power-grid-assets/

2 Katrina Manson, "Chinese Hackers Breach US, India Internet Firms, Lumen Says," *Bloomberg*, August 27, 2024, https://www.bloomberg.com/news/articles/2024-08-27/chinese-hackers-breach-us-internet-firms-via-startup-lumen-says

3 Christian Shepherd et al., "Leaked files from Chinese firm show vast international hacking effort," *The Washington Post*, February 22, 2024, https://www.washingtonpost.com/world/2024/02/21/china-hacking-leak-documents-isoon/

4 Jonathan Greig, "Suspected Chinese gov't hackers used ransomware as cover in attacks on Brazil presidency, Indian health org," *The Record*, June 27, 2024, https://therecord.media/chamelgang-china-apt-ransomware-distraction

5 Sameer Patil, "Securing Elections in the Digital Age," in *Global Dynamics in a Year of Domestic Contestation and Political Shifts*, ed. Karim El Aynaoui, Paolo Magri and Samir Saran (Observer Research Foundation, December 14, 2024), https://www.orfonline.org/research/global-dynamics-in-a-year-of-domestic-contestation-and-political-shifts

6 "China tests US voter fault lines and ramps AI content to boost its geopolitical interests," Microsoft, April 4, 2024, https://blogs.microsoft.com/on-the-issues/2024/04/04/china-ai-influence-elections-mtac-cybersecurity/

7 Rohini Lakshané, "Indian Elections 2024: Social Media, Misinformation, and Regulatory Challenges," Heinrich Böll Stiftung Regional Office New Delhi, April 9, 2024, https://in.boell.org/en/elections-2024-media

8 Cabinet Secretariat, "The Gazette of India," September 27, 2024, https://cabsec.gov.in/writereaddata/allocationbusinessrule/amendment/english/1_Upload_3934.pdf

9 Ministry of Defence, Government of India, https://pib.gov.in/PressReleaseIframePage.aspx?PRID=2026240

10 "India Set to Get Defence Cyber Agency to Fight Pak, Chinese Hackers," *NDTV,* April 30, 2019, https://www.ndtv.com/india-news/india-set-to-get-defence-cyber-agency-to-fight-pak-chinese-hackers-2030798

11 Kartik Bommakanti, "China removes the PLASSF and establishes ISF: Implications for India," Observer Research Foundation, May 15, 2024, https://www.orfonline.org/expert-speak/china-removes-the-plassf-and-establishes-isf-implications-for-india

Space
Challenges to Innovation

1 Ministry of Science and Technology, Government of India, 2025, https://pib.gov.in/PressReleseDetail.aspx?PRID=2091563&reg=3&lang=1.

2 Ministry of Science and Technology, Government of India, 2024, https://pib.gov.in/PressReleasePage.aspx?PRID=2047037.

3 Ministry of Defence, Government of India, 2025, https://pib.gov.in/PressReleaseIframePage.aspx?PRID=2089184.

4 Department of Space, Government of India, 2024, https://pib.gov.in/PressReleasePage.aspx?PRID=2067667.

5 BW Online Bureau, "India's Space Sector Sees 55% Funding Dip in 2024 Amid Global Slowdown," *Business World Disrupt*, January 7, 2025.

6 Divyam Sharma, ""First 40 Tejas Still Not...": Air Force Chief as China Tests 6th Gen Jets," *NDTV*, January 8, 2025.

7 Shishir Gupta, "Exclusive: CCS clears launch of 52 surveillance satellites," *Hindustan Times*, October 11, 2024.

Nuclear Weapons

A More Complex Reality in the Making

[1] Ministry of Defence, Government of India, https://pib.gov.in/PressReleasePage.aspx?PRID=2049870

[2] Shishir Gupta, “India Launches 4th Nuclear-missile Submarine,” *Hindustan Times*, October 22, 2024, https://www.hindustantimes.com/india-news/india-launches-4th-nuclear-missile-submarine-101729560730642.html.

[3] Amrita Nayak Dutta and Amitabh Sinha, “Mission Divyastra: PM Modi hails first test of Agni-5 with multiple warhead technology,” *The Indian Express*, March 12, 2024, https://indianexpress.com/article/india/pm-modi-agni-missile-drdo-agni5-weapons-system-9208122/.

[4] Hemant Kumar Rout, “India First to Develop Long-range Hypersonic Missile: Defence Experts,” *The New Indian Express*, December 1, 2024, https://www.newindianexpress.com/states/odisha/2024/Dec/01/india-first-to-develop-long-range-hypersonic-missile-defence-experts.

[5] “DRDO Successfully Tests Phase-II Ballistic Missile Defence System,” *The Hindu*, July 24, 2024, https://www.thehindu.com/sci-tech/science/drdo-successfully-tests-phase-ii-ballistic-missile-defence-system/article68442838.ece.

[6] Kartik Bommakanti, “Is China Resuming Nuclear Testing?,” Observer Research Foundation, January 10, 2024, https://www.orfonline.org/expert-speak/is-china-resuming-nuclear-testing.

[7] US Department of Defence, *Military and Security Developments Involving the People’s Republic of China* (US Department of Defence, 2024), https://media.defense.gov/2024/Dec/18/2003615520/-1/-1/0/military-and-security-developments-involving-the-peoples-republic-of-china-2024.pdf.

[8] Gabriel Honrada, “China’s New Hypersonic Weapon Could Black Out US, Taiwan,” *Asia Times*, November 19, 2024, https://asiatimes.com/2024/11/chinas-new-hypersonic-weapon-could-black-out-us-taiwan/.

[9] Li Bin Tong Zhao, ed., *Understanding Chinese Nuclear Thinking* (Carnegie Endowment for International Peace, 2016), https://carnegie-production-assets.s3.amazonaws.com/static/files/ChineseNuclearThinking_Final.pdf.

[10] Šumit Ganguly et al., “Introduction,” in *The Sino-Indian Rivalry: Implications for Global Order* (United Kingdom: Cambridge University Press, 2023), 3–13, https://doi.org/10.1017/9781009193542.002.

[11] Anil Chopra, “Abstract- China, Pakistan Aerospace Connect,” *Journal of the United Service Institution of India* CL, no. 619 (2020), https://www.usiofindia.org/publication-journal/china-pakistan-aerospace-connect.html.

[12] “Pakistan Arming JF-17 Jets with Ra’ad Nuke Missiles,” *The Times of India*, July 3, 2024, https://timesofindia.indiatimes.com/world/pakistan/pakistan-arming-jf-17-jets-with-raad-nuke-missiles/articleshow/111454243.cms.

[13] Usman Ansari, “Pakistan’s Air Force Says It Has a Hypersonic-capable Missile,” *Defense News*, January 19, 2024, https://www.defensenews.com/global/asia-pacific/2024/01/18/pakistans-air-force-says-it-has-a-hypersonic-capable-missile/.

[14] Bhashyam Kasturi, “Why Is Pakistan Asking China for Second-strike Capability?,” *Firstpost*, December 26, 2024, https://www.firstpost.com/opinion/why-is-pakistan-asking-china-for-second-strike-capability-13847786.html.

[15] Heather Williams, “Why Russia Keeps Rattling the Nuclear Saber,” *Center for Strategic & International Studies*, October 11, 2024, https://www.csis.org/analysis/why-russia-keeps-rattling-nuclear-saber.

[16] “A look at the Hypersonic Oreshnik missile, which Russia has used for the first time,” *AP News*, December 9, 2024, https://apnews.com/article/russia-oreshnik-hypersonic-missile-putin-ukraine-war-345588a399158b9eb0b56990b8149bd9.

17 Fabian R. Hoffmann, “The Strategic-level Effects of Long-range Strike Weapons: A Framework for Analysis,” *Journal of Strategic Studies*, May 28, 2024: 1–37, https://doi.org/10.1080/01402390.2024.2351500.

18 Hoffmann, “The Strategic-Level Effects of Long-Range Strike Weapons: A Framework for Analysis.”

19 Colin S Gray, “Understanding Airpower Bonfire of the Fallacies,” *Strategic Studies Quarterly* 2, no. 4 (2008): 43–83, https://www.airuniversity.af.edu/Portals/10/SSQ/documents/Volume-02_Issue-4/Gray.pdf.

20 Sunil Srivastava, “Transformation of the Indian Armed Force,” *Centre for Joint Warfare Studies*, 2021, https://cenjows.in/publications/transformation-of-the-indian-armed-force/.

21 Kartik Bommakanti and Satyam Singh, “China’s Military Modernisation: Recent Trends - 2024,” Observer Research Foundation, September 24, 2024, https://www.orfonline.org/research/contemporary-trends-in-china-s-military-modernisation#_ednref228.

22 Ron Christman, “Conventional Missions for China’s Second Artillery Corps,” *Comparative Strategy* 30, no. 3, July 1, 2011: 198–228, https://doi.org/10.1080/01495933.2011.587679.

23 Rajeswari Pillai Rajagopalan, “India’s Changing Attitude Toward Nuclear Expansion,” The National Bureau of Asian Research, May 22, 2024, https://www.nbr.org/publication/indias-changing-attitude-toward-nuclear-expansion/.

24 Andrew Futter and Benjamin Zala, “Strategic Non-Nuclear Weapons and the Onset of a Third Nuclear Age,” *European Journal of International Security* 6, no. 3, February 11, 2021: 257–77, https://doi.org/10.1017/eis.2021.2.

25 Arun Sahgal and PR Kumar, “Strategic Stability in Southern Asia and the Role of Non-strategic Nuclear Weapons,” Observer Research Foundation, October 21, 2024, https://www.orfonline.org/expert-speak/strategic-stability-in-southern-asia-and-the-role-of-non-strategic-nuclear-weapons.

26 Andrews S Harvey, “The Levels of War as Levels of Analysis,” *Military Review- Army University Press*, November 2021, https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/November-December-2021/Harvey-Levels-of-War/.

Chemical and Biological Weapons
India’s Strategic Moves

1 P Naveen, “From DRDO, Powerful Step In India’s Biosecurity,” *The Times of India*, November 11, 2024, https://timesofindia.indiatimes.com/city/bhopal/drdo-boosts-indias-biosecurity-with-new-bsl-4-laboratory-and-detection-facility/articleshow/115191760.cms.

2 Debaprasad Parai et al., “Investigation Of Human Anthrax Outbreak In Koraput District Of Odisha, India,” *Travel Medicine and Infectious Disease*, November 1, 2023, https://doi.org/10.1016/j.tmaid.2023.102659.

3 Department of Biotechnology, “National Biotechnology Development Strategy,” Ministry of Science and Technology, Government of India, https://dbtindia.gov.in/about-us/strategy-nbds.

4 Ministry of environment, Forest, and Climate, Government of India, https://pib.gov.in/PressReleaseIframePage.aspx?PRID=1844666.

5 “National Authority Chemical Weapons Convention,” https://www.nacwc.gov.in/content.php?page=420.

6 “OPCW Conference Of the States Parties Opens,” Organisation for the Prohibition of Chemical Weapons, November 25, 2024, https://www.opcw.org/media-centre/news/2024/11/opcw-conference-states-parties-opens.

7 “India Contributes €10,000 To Support OPCW Assistance Activities,” Organisation for the Prohibition of Chemical Weapons, December 18, 2024, https://www.opcw.org/media-centre/news/2024/12/india-contributes-eu10000-support-opcw-assistance-activities.

8 “CBW Events - BWC Review Conference Reports,” CBW Events, https://www.cbw-events.org.uk/bwc-rep.html.

[9] "US - India Biosecurity Dialogue," Johns Hopkins Center for Health Security, https://centerforhealthsecurity.org/our-work/research-projects/us-india-biosecurity-dialogue.

Quantum Technology
India Solidifies Foundation

[1] Hartmut Neven, "Meet Willow, Our State-of-the-art Quantum Chip," Google, December 9, 2024, https://blog.google/technology/research/google-willow-quantum-chip/

[2] "DRDO, TIFR Test 6-qubit Quantum Processor: What It Means For India's Quantum Future," *India Today*, September 1, 2024, https://www.indiatoday.in/science/story/drdo-tifr-test-6-qubit-quantum-processor-what-it-means-for-indias-quantum-future-2591688-2024-09-01

[3] Matt Swayne, "India-Based QpiAi Secures $6.5 Million In Pre-Series A Funding," *The Quantum Insider,* June 21, 2024, https://thequantuminsider.com/2024/06/21/india-based-qpiai-secures-6-5-million-in-pre-series-a-funding/

[4] Ministry of Communications, Government of India, https://pib.gov.in/PressReleaseIframePage.aspx?PRID=2011690

[5] Ministry of Science And Technology, Government Of India, https://dst.gov.in/quantum-interferences-atomic-medium-facilitate-light-storing-useful-high-precision-quantum-sensors

[6] Chethan Kumar, "RRI's First Spinoff To Produce Cost-Effective Laser Systems For Quantum Optics," *Times Of India,* July 19, 2024, https://timesofindia.indiatimes.com/india/rris-first-spinoff-to-produce-cost-effective-laser-systems-for-quantum-optics/articleshow/111858581.cms

[7] Prateek Tripathi, "Impediments In Global Quantum Technology Collaboration," Observer Research Foundation, December 6, 2024, https://www.orfonline.org/expert-speak/impediments-in-global-quantum-technology-collaboration

[8] UNESCO, "International Year of Quantum Science and Technology," https://quantum2025.org/en/

Artificial Intelligence and Drones
India's Strategic Embrace

[1] "Indian Army: Indian Army Establishes Elite Tech Unit STEAG to Research Future Communication Technologies," *The Economic Times*, March 18, 2024, https://economictimes.indiatimes.com/news/defence/army-raises-elite-unit-to-work-on-critical-technologies-having-military-applications/articleshow/108588068.cms?from=mdr.

[2] Saurabh Sharma, "Indian Army Unveils AI Incubation Centre to Lead in Technological Innovation and Warfare," *The Sunday Guardian Live*, December 18, 2024, https://sundayguardianlive.com/tsg-on-weekdays/indian-army-unveils-ai-incubation-centre-to-lead-in-technological-innovation-and-warfare.

[3] "DRDO to Collaborate with IIT Bhubaneswar for AI-Driven Surveillance, Other Projects," *Deccan Herald*, May 8, 2024, https://www.deccanherald.com//india/odisha/drdo-to-collaborate-with-iit-bhubaneswar-for-ai-driven-surveillance-other-projects-3013145.

[4] Ministry of Defence, Government of India, https://pib.gov.in/PressReleaseIframePage.aspx?PRID=2065847#:~:text=The%20ETAI%20Framework%20focuses%20on,criteria%20for%20evaluating%20trustworthy%20AI, 2024.

[5] Shivani Sharma, "AI-Powered Fences, Drones: How Army Is Strengthening Security along LoC," *India Today*, September 16, 2024, https://www.indiatoday.in/india/story/indian-army-pakistan-border-loc-security-ai-fences-drones-infiltration-terror-attacks-2600826-2024-09-16.

[6] "Indian Army Gets Indigenous Man Portable Counter Drone System," *Financial Express*, June 10, 2024, https://www.financialexpress.com/business/defence-indian-army-gets-indigenous-man-portable-counter-drone-system-3520311/.

[7] "India to Create Comprehensive Anti-Drone Unit for Border Security: Amit Shah," *The Hindu*, December 8, 2024, https://www.thehindu.com/news/national/india-to-create-comprehensive-anti-drone-unit-for-border-security-amit-shah/article68961523.ece.

[8] "India Finalises $3.5 Billion Deal to Acquire 31 Predator Drones from US," *Business Today*, October 15, 2024, https://www.businesstoday.in/india/story/india-finalises-35-billion-deal-to-acquire-31-predator-drones-from-us-450064-2024-10-15.

[9] Dalip Singh, "Army Puts on Hold Acquisition of 200 Drones from Dhaksha Unmanned Systems," *BusinessLine*, August 28, 2024, https://www.thehindubusinessline.com/news/army-puts-on-hold-acquisition-of-200-drones-from-dhaksha-unmanned-systems/article68577549.ece.

[10] Snehesh Alex Philip, "Intel Agencies Flag Chinese Components in Drones Procured, Army to Formulate New Policy," *The Print*, September 4, 2024, https://theprint.in/defence/intel-agencies-flag-chinese-components-in-drones-procured-army-to-formulate-new-policy/2252367/.

[11] Dalip Singh, "Defence Ministry cautions firms using Chinese parts for drones," *Business Line*, August 28, 2024, https://www.thehindubusinessline.com/news/national/defence-ministry-cautions-firms-using-chinese-parts-for-drones/article68573070.ece.

[12] "286 Drones Seized along India-Pak Border in '24: BSF," *Hindustan Times*, January 1, 2025, https://www.hindustantimes.com/cities/chandigarh-news/286-drones-seized-along-india-pak-border-in-24-bsf-101735670571417.html.

[13] Dinesh Bothra, "India Working on Anti-Drone Unit to Protect Borders: Shah," *Hindustan Times*, December 9, 2024, https://www.hindustantimes.com/india-news/india-working-on-anti-drone-unit-to-protect-bordersshah-101733682551756.html.

[14] Vijaita Singh, "Manipur Drone Attack: Looted Ammunition Said to Have Been Used," *The Hindu*, September 4, 2024, https://www.thehindu.com/news/national/manipur/drones-used-in-manipur-violence-may-have-been-assembled-locally/article68602252.ece.

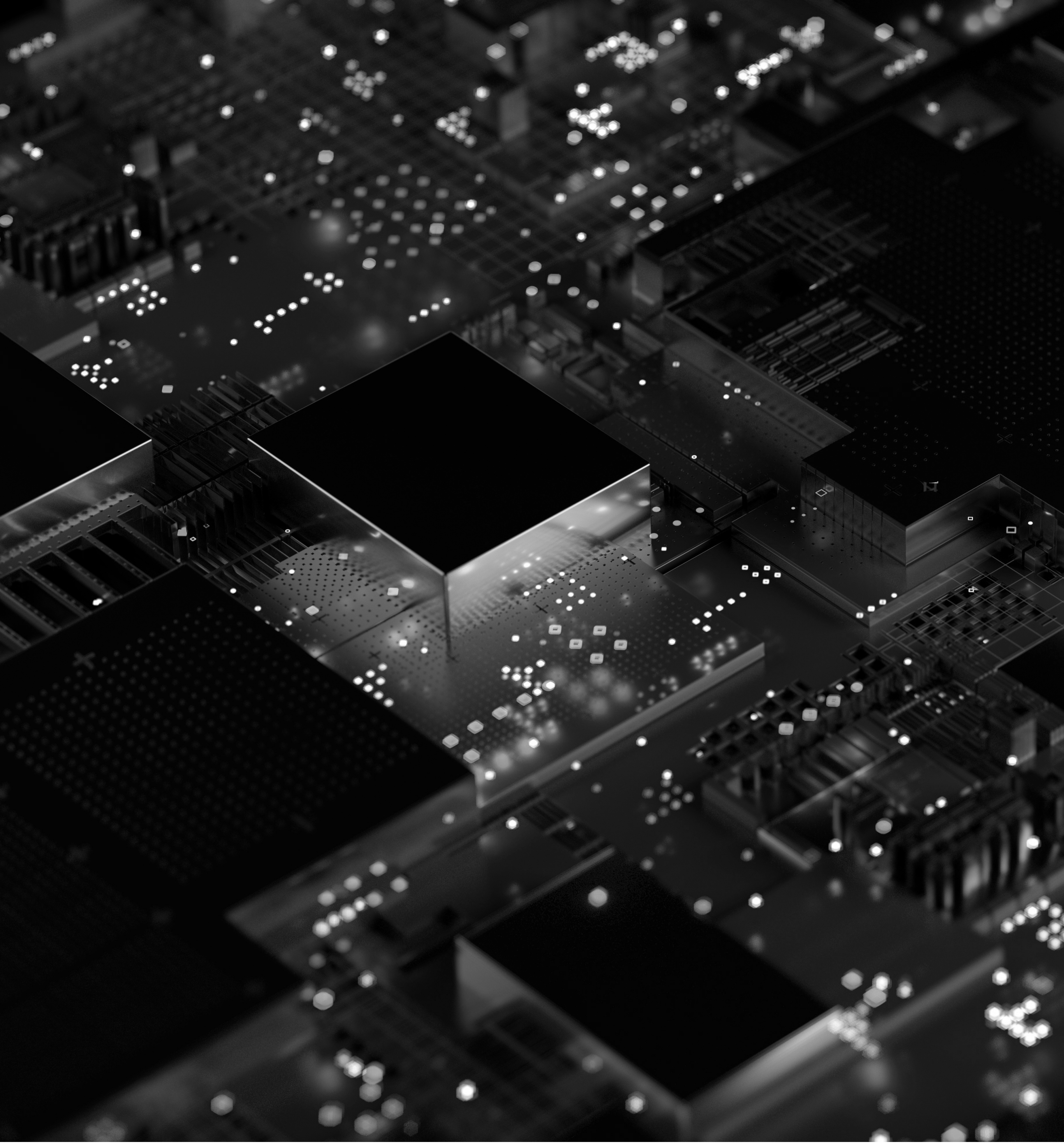
[15] Meryl Sebastian, "AI and Deepfakes Blur Reality in India Elections," *BBC*, May 16, 2024, https://www.bbc.com/news/world-asia-india-68918330.

[16] "India Second Most Targeted Nation in Terms of Cyberattacks: CloudSEK," *Business Standard*, January 2, 2025, https://www.business-standard.com/technology/tech-news/india-second-most-targeted-nation-in-terms-of-cyberattacks-cloudsek-125010200905_1.html.

[17] "Global Cyber Attacks Surge 30% in Q2 2024, India Hit Hard," *The Times of India*, July 21, 2024, https://timesofindia.indiatimes.com/spotlight/planning-to-pursue-product-management-heres-how-isbs-product-management-programme-can-help/articleshow/100518780.cms.

All photographs used for the cover collage are from Getty Images. From L to R, top to bottom: China News Service; Peter Dazeley; Hindustan Times; Hindustan Times; NurPhoto; Arun Sankar; Pallava Bagla; Pallava Bagla; Pallava Bagla; Just Super; Hindustan Times; Indranil Mukherjee; Anadolu; Hindustan Times.

Back cover image: Getty Images/Andriy Onufriyenko



OBSERVER
RESEARCH
FOUNDATION

Ideas . Forums . Leadership . Impact

20, Rouse Avenue Institutional Area,
New Delhi - 110 002, INDIA
Ph. : +91-11-35332000. **Fax :** +91-11-35332005
E-mail: contactus@orfonline.org
Website: www.orfonline.org