FINSJOURNAL

OF DIPLOMACY & STRATEGY

FINS
Initiate Interact Influence

Forum for Integrated National Security

Oct. - Dec. 2025 | Issue No. 04 Vol. 8 | ISSN 2581-6586

Nippon india Mutual Fund
Wealth sets you free
What's stronger than individuals?
Processes.

Editorial: World Ahead 2026 – End of Politics, Opening up of Leadership

As this impactful year 2025 ends, there are certain things one needs to know about the shifting global order. In global politics, 2025 was the year when an old order ended. President Donald Trump demolished decades-old norms and institutions dramatically. His tariffs bludgeoned multilateral trade system. Long-standing security alliances were refashioned into transactional relationships that monetised American military and economic heft.

2026 is poised as year of geopolitical fragmentation, challenging traditional alliances, shifting power dynamics, demanding greater resilience from nations. Geopolitical landscapes face increased volatility, shaped by shifting US foreign policy, growing US-China Indo-Pacific tensions, evolving European security dynamics post-Ukraine war and continued instability in Middle East post-Gaza conflict, with potential flashpoints in Taiwan, Korean Peninsula and Africa, along with major elections in Bangladesh, Brazil, Colombia, Hungary, Israel, Peru, Sweden and US – mid-terms, and global summits like APEC, and G20 in US, signalling a fragmented world order.

In 2026, beyond individual events, political fault lines will continue to shift with significant consequences for international trade and investments. The global economic environment is pivoting towards greater securitization, regional fragmentation and retreat from rule-based frameworks that defined much of post-war political and economic order.

The world of 2026 will be heavily shaped by efforts to restructure global economic and geopolitical order and how Washington's allies, adversaries and rivals seek to mitigate those risks or take advantage of new opportunities. China's economy will be much larger than America's and India's will be much larger than that of any individual European country. As these countries develop, so will their voracious appetite for natural resources and human capital. There will be global scramble for oil, water and skilled labour. China and India will become self-confident and will project their own ideas on concepts such as democracy and rule of law. If these trends are taken to their logical conclusions, 2026 will not see a new world order, but at least four. This quadripolar world would be split along two axes; between democracies and autocracies; and between countries seeking a balance of power and those that want a world organised around international law and institutions.

Four years after Russia's full-scale invasion of Ukraine, peaceful settlement remains far from reach. As long as Vladimir Putin continues his agenda to control not just Ukraine's eastern regions but entire Ukraine, Trump's negotiation with Putin is unlikely to resolve war in Ukraine. Ukraine must adapt its economy to a protracted war and strengthen its industrial capacity to produce more weapons and win technological race in drone interception and gains deep-strike capabilities from European allies. Russia continues to innovate. Its ballistic missiles are now better able to evade interceptors such as US-made Patriot system. Ukraine will need around $100 billion in military aid and financial support. NATO summit in Ankara in July 2026 could be crucial moment to shore up these commitments for Ukraine.

Middle East seems to be poised to dominate headlines. 2026 will test whether Middle East ceasefires can be foundation for meaningful diplomacy and sustainable peace agreements. US-brokered Gaza ceasefire in October offers rare moment of respite for Palestinians devastated by two years of war and famine. Donald Trump's involvement in regional diplomacy applied much-needed pressure on both Israel and Hamas, yet uncertainty continues to overshadow a process that still lacks detailed framework, timeline and commitments from either side. Sustained international engagement and political follow-through from regional powers, including Gulf States will be essential to transforming this ceasefire into broader political and reconstruction process. Lebanon and Syria remain mired in institutional fragility, leaving both vulnerable to renewed conflict and further Israeli strikes. Lebanon's parliamentary elections, scheduled for May 2026, could provide an opportunity to stabilize internationally backed technocratic government. But despite direct negotiation between Israel and Lebanon, unresolved questions over Hezbollah's disarmament and Israel's continued strikes in Lebanon persist.

Syria has completed its first parliamentary elections and violence has eased following Suwayda attacks, but reconstruction efforts are lagging. President Ahmed al-Sharaa's visit to White House in November 2025 and lifting of US sanctions may herald new economic opportunities for Syria. Spectre of another Israel–Iran confrontation looms after 12-day war in June 2025. Fresh round of diplomacy with Tehran will be essential to preventing resumption of Iran's nuclear programme. If Israel continues to focus on deterrence over diplomacy its isolation may deepen in 2026.

The trajectory of US–China relations should become clearer in 2026 as US President Donald Trump and Chinese leader Xi Jinping plan reciprocal visits which will offer clearer direction of whether they will agree to a new modus vivendi, following trade-war truce agreed in October 2025. Although American political and security establishment believes US must prepare for decades of strategic competition with China, Trump sees Beijing as partner with which he can do business, even as he deploys tactical threats to secure short-term advantages. Regardless of how Trump approaches Beijing, Xi is convinced that Washington is trying to constrain China in long term. When Chinese Communist Party launches its 15th Five-Year Plan in March, Xi is expected to accelerate China's push for technological and industrial self-reliance. The bumpy trajectory of US–China relations will affect rest of the world.

Bangladesh and Nepal are due to hold elections in first quarter of 2026, as they attempt to move on from their recent youth-led revolutions. New leaders of Japan and South Korea, Prime Minister Sanae Takaichi and President Lee Jae-myung, will try to manage political polarization and sluggish economic growth at home while balancing relations with US and China. Pakistan has begun to see some pseudo-economic stabilisation due to increased diplomatic ties with US over sanctions negotiations and energy development as well as continued relations with China through China-Pakistan Economic Corridor. Alongside security destabilisation stemming from tensions with India over insurgency and terrorism, political destabilisation prevails in Pakistan.

Intensifying global competition, louder public demands for reform and protracted security challenges will shape Africa in 2026. Interest from European, Asian and Gulf countries is likely to grow as they scramble to secure cobalt, copper and other minerals needed for energy transition. Opportunities will arise to reshape industrial supply chains and strengthen Africa's economy which continues to struggle with high youth unemployment, sluggish productivity and rising debt. Partnerships in 'cobalt-copper belt' are likely to expand in 2026, supported by greater investment in battery, refining and transport-corridor projects. In 2026, growth across Africa is expected to remain resilient, with East Africa approaching 6 per cent in select economies. West Africa will continue to diversify through industrial expansion and energy investment. Protracted conflicts, including war in Sudan, will continue to destabilize Africa. Gen Z-led protests across Kenya, Tanzania and Madagascar in 2024 and 2025 exposed growing dissatisfaction with entrenched elites, rigged elections and social inequalities.

Big surprise for global economy in 2025 was that Donald Trump actually did what he promised in US election campaign. World economy has suffered less than many predicted from such measures as raising average US tariff rate to its highest level since 1930s. International Monetary Fund is forecasting growth of just over 3 per cent in 2026 and global equity markets recently touched all-time highs. This resilience is partly due to other countries choosing not to retaliate against US tariff hikes and continuing to trade with each other under World Trade Organization terms. Whether these forces will continue to counterbalance negative effects of Trump's actions on US and global economies is a major question in 2026. One scenario would see sharp financial market correction, or even a crash.

New START, a nuclear arms treaty between Russia and US, is due to expire in February 2026, leaving countries without bilateral arms control for first time in more than 50 years. Can Russia and US find a way to extend treaty informally? Iran's nuclear programme will remain another flashpoint, after US strikes in June 2025 failed to destroy its facilities. As Tehran inches towards weapons-grade uranium and diplomatic options narrow, risk of renewed conflict between Iran and US or its regional partners will grow in 2026. China is believed to be expanding its arsenal rapidly and is said to be on course to reach 1,000 nuclear warheads by 2030. Though that would only be one-fifth size of Russia's or US's, Beijing is shifting the strategic balance. No talks with Moscow and Washington are on horizon, and each may use Beijing's actions as pretext to acquire more weapons. President Trump's announcement about resumption of testing American nuclear weapons heightens risk of escalation.

The danger is not that US will conduct test in 2026 but that such rhetoric could give Russia or China political cover to resume testing themselves. In April and May 2026, Non-Proliferation Treaty Review Conference meets to assess state of one of the most effective arms control agreements. Will it produce meaningful recommitment to non-proliferation norms?

International rule of law has been tested over 2025. Failure to address conflict in Gaza on same terms as West's response to Ukraine has prompted many states in Global South to distance themselves from core human rights and humanitarian principles. Donald Trump has encouraged more unilateral approaches by extending his coercive tariff campaign, deploying military force against alleged drug traffickers in Venezuela. The question for 2026 is whether international system can show sufficient resilience in defending rule of law. Can international trade withstand rise of unilateralism and resist interference with free trade? Will West be able to persuade other states that humanitarian principles are universal concerns, rather than tools of intervention into domestic affairs of states? Can confidence be restored in prohibition of use of force by ending violence in Ukraine? Answers to these questions are important in 2026.

In 2025, Indian geopolitical landscape was defined by balancing major power relations - US, Russia, EU and China, navigating regional instability - Pakistan, Bangladesh and Maldives, pursuing key trade deals with US and EU, managing energy security amid global conflicts in Ukraine and West Asia, and addressing economic pressures from Western tariffs, all while enhancing strategic partnerships in areas such as technology and cyber-security. Scourge of terrorism continued to visit India, as Pakistan remains global centre of terror. Pakistan-backed Pahalgam Massacre invoked massive response from India, hitting Pakistan hard in "Op Sindoor". Pakistan Afghanistan relations hit a new low, as Pashtuns made Durand Line live with cross-border action. Bangladesh remains in civil-war state after ouster of Sheikh Hasina, as interim government tries to distance from India and makes overtures to China and Pakistan. US-India dynamics included dealing with potential US tariffs, "America First" policies, renewed US-Pakistan ties and efforts to secure significant trade deal for better market access. India-EU relations are a deepening "strategic partnership" focused on trade with FTA talks ongoing, EU-India Trade and Technology Council (TTC) cooperation, security, and digital transformation. India continues delicate balance of trade with China despite border tensions while managing energy ties and geopolitical pressures over relations with Russia. President Putin's state visit to India on December 3-4, 2025 for 23rd India-Russia Annual Summit further strengthened Special and Privileged Strategic Partnership between India and Russia. Trade agreements with US, UK, EFTA, Qatar, New Zealand could boost investment.

India's 8.2 per cent GDP growth in Q2 of 2025-2026 was very encouraging. The year was marked by global structural shifts, increased nationalism, trade protectionism, and cyber-security threats. As 2026 approaches, India is expected to continue balancing its interests and global power competition, seeking strategic autonomy, positioning itself as a major economic and strategic power in a turbulent world. Expectations for India in 2026 point towards continued strong economic growth, solid market performance driven by domestic demand and policy support and significant anticipation surrounding the Union Budget 2026, with focus on tax fairness, support for sunrise sectors, consumer-facing reforms in healthcare and insurance. India's GDP is projected to grow between 6.5 and 7.4 per cent in 2026, reaching approximately $4.1 to $4.6 trillion in nominal terms, driven by strong domestic demand and robust liquidity. Focus areas include digital infrastructure, manufacturing incentives, and managing global economic uncertainties. Relations between India and China hold greater significance for Asia and global order. Together, two nations account for nearly 40 per cent of world's population, with India currently fourth and soon to be third largest, yet China-India relations remain complex. Tensions over long-standing and unresolved territorial dispute play significant role, but beyond that lies broader geopolitical rivalry. Both view themselves as civilizational states and their rising prominence is creating new ways of competition. West increasingly sees India only as counterweight to China, with limited interest in India's success.

2025 has proved to be one of toughest for India on diplomatic and economic front with policy makers striving to strike balance between rival powers on global stage while safeguarding India's sovereignty, economic interests and sensitivities. The primary challenge was handling unpredictability of US President Donald Trump who assumed office for second term in January. India was singled out for its economic and diplomatic closeness to Russia, a historical ally currently engaged in Ukraine war.

In August 2025, Washington imposed steep 50 per cent import duties on most Indian goods This included 25 per cent penalty specifically for purchasing discounted Russian oil. With US exports totaling approximately $86.5 billion in FY25, nearly a fifth of India's total, the move was omnious. But India did not blink. It chose to stick to tried and tested path of non-alignment and sovereignty and refused to stop its oil purchases from Russia while continuing to remain cordial and economically pragmatic with US. It stayed continuously engaged with US, trying to work out bilateral trade deal that would satisfy US, by providing market access for American industry and lead to roll back of steep duties on Indian goods. US wants market access for its genetically modified soya, corn and certain meat and dairy items that are highly sensitive in India. India is firm on its redlines but flexible in other areas. Indian exporters have shown resilience and guts by trying to continue to sell in US market to extent possible while looking for opportunities in other markets. Despite global upheaval, India's overall goods exports have not dipped this fiscal. In April – November 2025 period, exports posited 2.6 increase to $292.1 billion and as efforts to diversify continue, FY26 would end on positive note. India is maximising opportunities in multiple markets, so as not to stay dependent on just a few. India remained neutral on Israel-deep Palestine war. By sticking to original stance of supporting two-state solution, India has managed to remain close to Israel while not alienating Islamic nations. It is evident in India-Oman FTA being ready for signing while FTA talks with Israel have been initiated. India is hoping to multiply its low exports with Russia, as Moscow is keen to use up its Vostro accounts for payment of oil. While India played a difficult hand astutely in 2025, 2026 promises further hurdles. US is yet to make up its mind on terms for tariff reduction. EU remains firm on its Carbon Border Adjustment Mechanism (CBAM) and other regulatory hurdles. EFTA and UK FTA are yet to prove their worth. Bridging trade deficit with Russia may not be easy. China's role is unclear. For India, 2026 will not be a year to rest but to stay sharp and alert, perhaps more than before.

The start of 2026 will see governments across the world, forced to respond swiftly to mounting economic, social, security, environmental and technological challenges. These issues come amid a turbulent geopolitical context – a disintegration of post-war international order. Global cooperation is at low point and conflict is escalating. Traditional institutions like WTO and UN have proved ineffective in delivering broad global consensus or serving as a platform to resolve disputes. Global security order is too fragmented to either maintain or negotiate peace.

Geopolitical world in 2026 will signal end of politics and opening up of leadership. Leaders will not only need to address specific challenges in 2026, but do so while finding agreement to build a global framework for promoting peace and prosperity in place of aggression and economic uncertainty we are now experiencing.

If past is prologue, year 2026 ahead will be filled with surprises – some good, some bad- that no one would have predicted. In 2026, old cliché will certainly hold true: expect the unexpected.

Articles in this edition of the Journal examine various dimensions of Diplomacy and Security related issues. All authors have presented their views on topics ranging from White Collar Terrorism to India's Critical Infrastructure Programme to China's coercive activities around Taiwan, with well-planned research on the topics with deep thought process. Their views will surely help in instilling the subjects and topics under discussion in the minds of the readers.

China's Coercive Activities Around Taiwan: A Strategic Assessment and Implications for India

Abstract

The strategic landscape of the Indo-Pacific is increasingly defined by the People's Republic of China's (PRC) growing assertiveness, with the Taiwan Strait serving as its most volatile flashpoint. For the democratic world, and particularly for a major regional power like India, the escalating coercive activities directed by Beijing towards Taiwan represent more than a localized dispute. They are a litmus test for the rules-based international order, challenging the principles of sovereignty, maritime freedom, and stability in the Asian commons.

This article provides a strategic analysis of China's coercive campaign against Taiwan, delineating its multi-domain nature and its parallels with India. It then explores the profound implications for India's security calculus, economic resilience, and strategic stability in the Indo-Pacific.

Introduction

In the Indo-Pacific, the Taiwan Strait currently stands as the most critical focal point of escalating geopolitical rivalry. Beijing views self-ruled Taiwan as its breakaway territory, and seeks to enforce its claims by a rising tempo of coercive measures. China has deployed a sophisticated, multifaceted strategy encompassing military threats, economic leverage, and disinformation campaigns to undermine Taipei's government and unilaterally shift the status quo without resorting to open warfare. This calculated pressure ranges from massive military manoeuvres simulating a 'quarantine' to subtle 'gray-zone' actions, such as aggressive coast guard presence and targeted trade restrictions. This determined drive for "reunification" not only jeopardizes the regional power balance but also carries profound, cascading ramifications for international stability and global supply chains.

Despite the geographical distance, the volatile situation in the Taiwan Strait directly impacts India. New Delhi's relations with Beijing are themselves fraught with long-standing strategic tension, an unresolved land border dispute, and China's expanding naval footprint in the Indian Ocean Region (IOR). Crucially, there is now a growing perception that the coercive strategy utilized against Taiwan will be a standardized playbook employed by Beijing against any nation challenging its supremacy in Asia. The deeper implication for India lies in a fundamental restructuring of the regional power dynamic. Should China succeed in annexing Taiwan through coercion, it would inevitably feel emboldened to press its territorial demands against India more aggressively. Therefore, this article posits that China's pressure on Taiwan constitutes a pivotal strategic challenge for India, demanding a thoughtful adjustment of New Delhi's regional policy that reconciles its traditional adherence to strategic autonomy with the immediate requirement of counter-balancing a mutual security concern. The fate of Taiwan, therefore, represents not merely a regional dispute but a critical test case whose outcome will either constrain or unleash China's future hegemonic ambitions toward New Delhi.

Deconstructing China's Coercive Playbook Against Taiwan

China's pursuit of unification with Taiwan relies not merely on the threat of overwhelming force, but on a layered strategy of coercive activities designed to induce surrender through exhaustion and economic pain. This sophisticated playbook falls short of outright kinetic warfare, yet deliberately escalates pressure across military, maritime, and economic domains, establishing a new and more volatile status quo in the Taiwan Strait. This multi-domain coercion encompasses military, economic, informational, and diplomatic instruments.

Military and 'Gray Zone' Coercion

The most visible element of this strategy is the normalization of military intimidation[1]. Since 2020, the People's Liberation Army (PLA) has dramatically increased the frequency and scope of its Air Force (PLAAF) incursions into Taiwan's Air Defence Identification Zone (ADIZ), and its naval patrols around the island[2]. China's Eastern Theatre Command (ETC) is at the forefront of these illegal activities.

This pattern of sustained pressure, which includes the routine crossing of the Taiwan Strait's median line, serves to fatigue Taiwan's defence forces, erode the morale of its pilots and sailors, and continuously test its response capabilities. Chinese actions are designed to demonstrate the PRC’s intent and capability to enforce its claims, while simultaneously normalizing a heightened state of tension.

Complementing these daily encroachments is the strategic utility of simulation, specifically the practice of large-scale, encircling military exercises[3]. The PLA has repeatedly simulated blockades and maritime "quarantines" around the island, a non-kinetic form of coercion intended to disrupt Sea Lines of Communication (SLOCs) without requiring a shot to be fired[4]. This model provides a scalable and reversible option that can be used to threaten global supply chains and demonstrate the capability to isolate Taiwan, all the while remaining below the threshold for a full military response from the United States or its allies. These exercises, often following key political events such as visits by foreign dignitaries (e.g., the August 2022 exercises following Nancy Pelosi’s visit), serve as a form of military signaling and intimidation. The goal is to stress the Taiwanese military, degrade its readiness, and shrink its operational space. The increased use of the China Coast Guard (CCG) and maritime militia in these operations further blurs the line between military and civilian enforcement, a key element of Beijing's "gray zone" tactics. The gray zone tactics enable China to keep the dispute below the threshold of conventional armed conflict and yet force Taipei into political concessions.

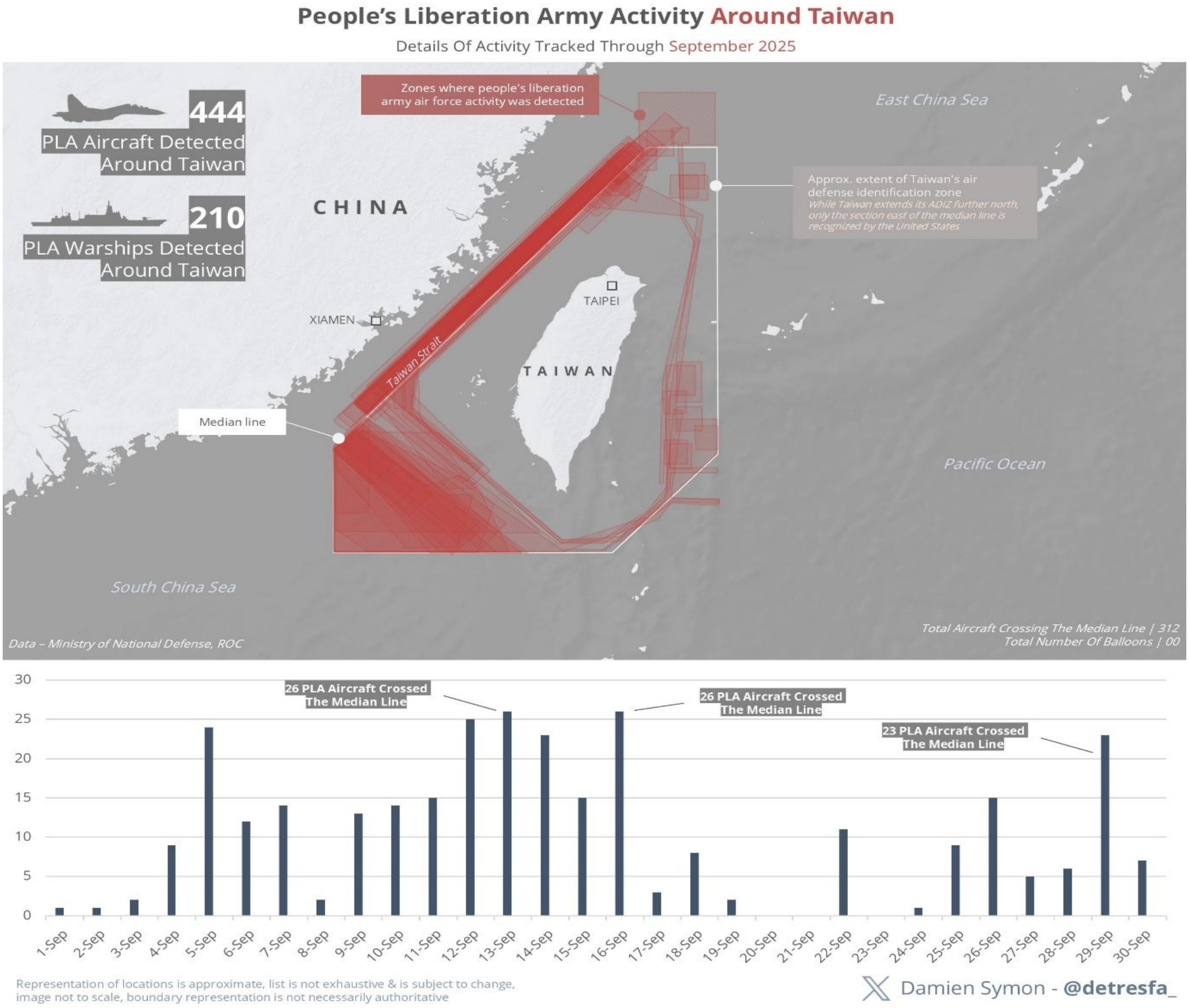
“Cold Start" Posture and Blockade Drills. Recent PLA exercises indicate a move towards a "cold start-style" operational posture - the capacity to initiate rapid, high-intensity offensive operations without obvious prior mobilization[5]. This reduces warning time for Taiwan and its allies. Crucially, exercises have increasingly focused on maritime and air "quarantine" or blockade scenarios, aiming to cut off critical imports like energy and food to isolate the island and force capitulation without a costly landing invasion[6]. Since 2015, China’s top civilian and military authorities have consistently promoted the doctrine of "start fast, end fast" (迅即开战，速决制胜). This strategy emphasizes the critical importance of maintaining constant readiness, executing rapid, integrated operations, and crucially, completing the mission before any external powers can intervene. This focus on speed is clearly reflected in recent developments, particularly a confidential address delivered by Chinese President Xi Jinping to officers of the Southern Theatre Navy (STC) in Zhanjiang on 11 April 2023. During this speech, he instructed the PLA to quickly field new capabilities and units, insisting on a reaction speed so swift that it denies opponents any chance to organize a counter-mobilization[7]. The Chinese military is also ramping up its capabilities by expanding missile infrastructure in eastern China. It has almost tripled its inventory of precision-attack ballistic and cruise missiles, and now operates 134 air bases that can sustain air operations near Taiwan[8]. Projections indicate that China's military will be capable of invading Taiwan as early as 2027[9].

Analyzing PLA Activities Around Taiwan: September to November 2025

Independent Open-Source Intelligence (OSINT) analyst Damein Symon has been regularly studying and analyzing Chinese military activities around Taiwan. His data shows a sustained pressure by China on Taiwan with no let-up. In September 2025, 312 out of the 444 aircraft detected around Taiwan crossed the median line[10]. On six days in the month, over 20 aircraft crossed the median line. 210 PLAN warships were detected around Taiwan in the same month. To understand the degree of brinkmanship by China, the 210 warships that were deployed around Taiwan constitute more than the entire warship strength of the Indian Navy. In October 2025, 427 aircraft and 205 warships were detected around Taiwan[11]. The number of aircraft crossing the median line reduced to 222, while more than 20 aircraft crossed the median line on two days. In November, 266 aircraft and one balloon violated Taiwan’s Air Defence Identification Zone (ADIZ) out of the 406 aircraft that were detected around the island country[12]. Significantly, on 06 November 2025, 31 aircraft crossed the median line. Over these three months, the Chinese Navy also operated its aircraft carriers around Taiwan, including the recently commissioned Fujian. A careful study of the pattern and quantum of forces deployed around Taiwan indicates a distinct possibility that the Chinese are preparing and practising for an armed intervention into Taiwan.

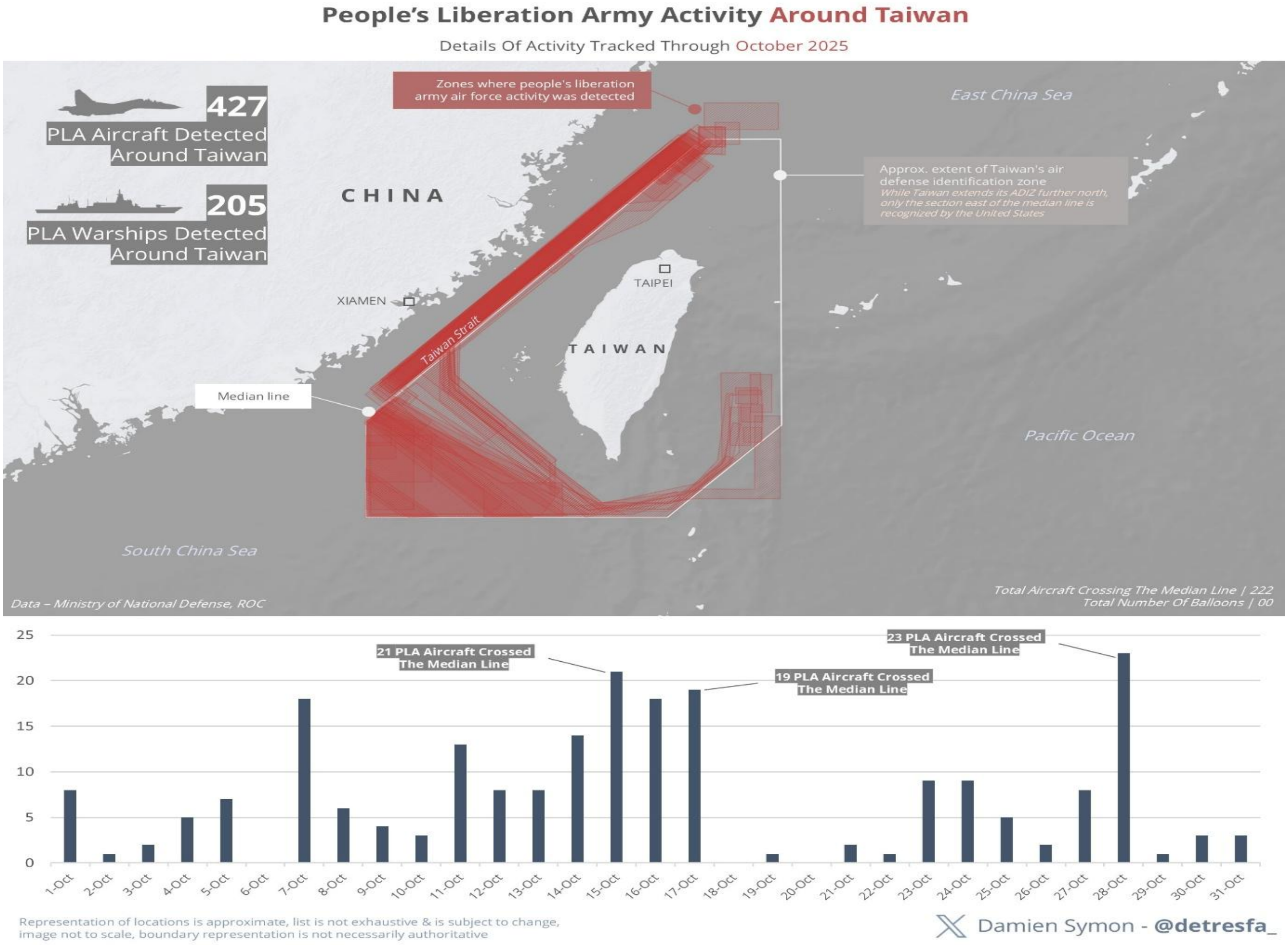
While the main focus was on the southwestern ADIZ, recent activities have shown a trend toward encircling the island. This includes increased crossings of the Bashi Channel into the Western Pacific, demonstrating longer-range operational capabilities and preparedness for joint combat readiness patrols on all sides of Taiwan, threatening its eastern coast - often considered the safest area[13]. The overall tempo and scale have intensified from episodic spikes to a sustained, high-level presence. Data from Taiwan's Ministry of National Defense (MND) indicates that the average daily number of detected aircraft has increased significantly over recent years, reflecting a shift toward military strategy and continuous operational dominance rather than purely diplomatic signaling[14]. Comprehensive visuals for the previous three months detailing China's PLA activity around Taiwan are given in the charts below:-

Fig. 1



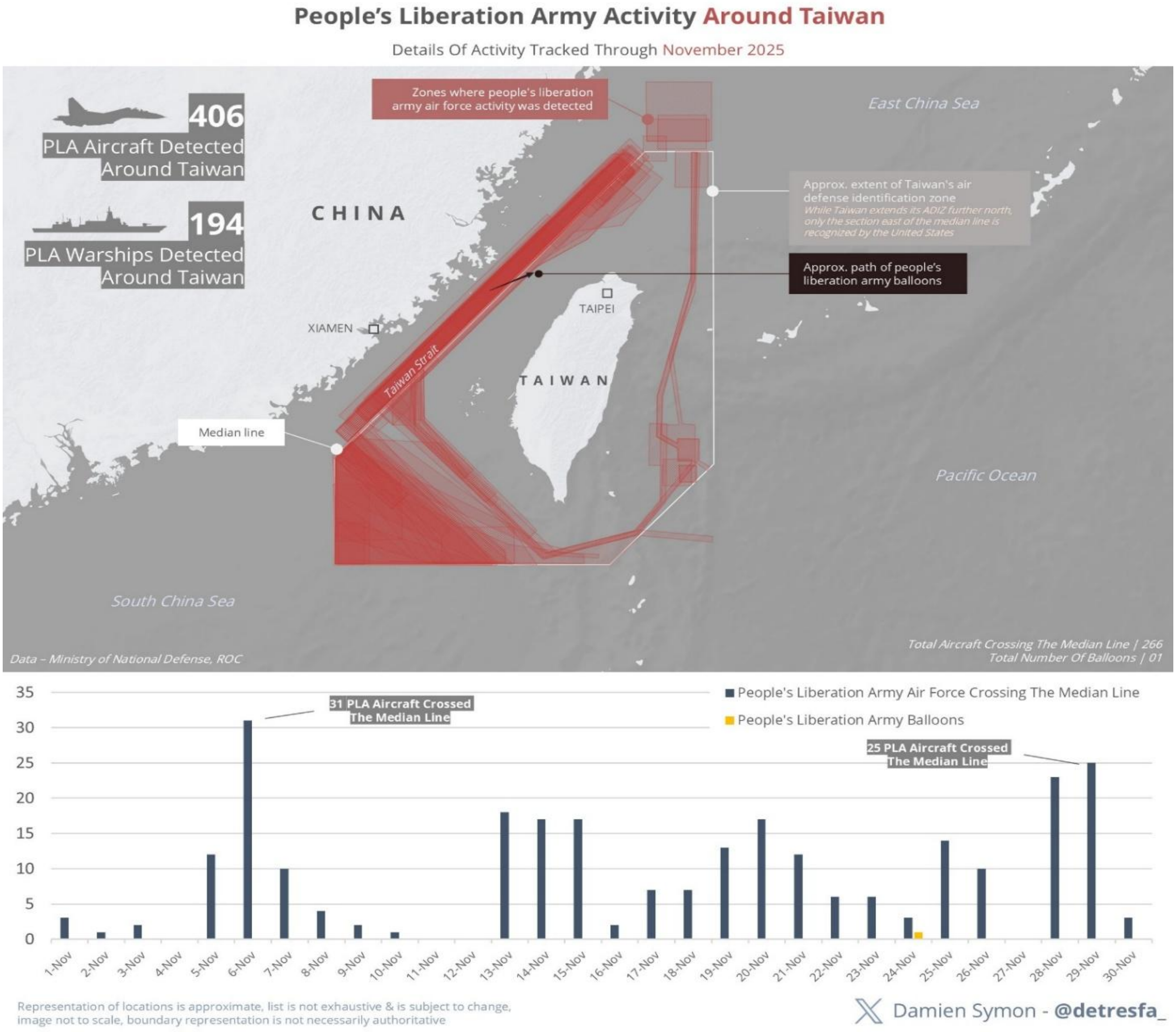
Source: X (formerly Twitter) handle of Damein Symon00

Fig. 2



Source: X (formerly Twitter) handle of Damein Symon

Fig. 3



Source: X (formerly Twitter) handle of Damein Symon

Economic Coercion: The "Silent Sanctions"

China's pressure campaign extends deep into Taiwan's economy through "silent sanctions" - a policy of weaponizing trade for political ends. Rather than imposing broad, international sanctions, Beijing leverages its vast market to apply highly targeted trade restrictions. These often invoke non-trade reasons, such as claiming the discovery of "quarantine pests" to ban imports of Taiwanese agricultural products (like pineapples or grouper fish), or initiating investigations into alleged violations of trade agreements. For instance, in 2024, Beijing suspended preferential tariff treatments under the Economic Cooperation Framework Agreement (ECFA) for petrochemical and other key Taiwanese industries[15]. These actions, which disproportionately harmed sectors whose constituents tended to support the ruling party in Taipei, were clearly timed to interfere with Taiwanese elections and discourage defiance of the Chinese Communist Party (CCP). China's actions sought to punish Taiwanese producers in an attempt to generate domestic dissatisfaction with the ruling political party. This economic pressure is strategically applied through the concept known as the "Beiping Model." This historical analogy, derived from the peaceful surrender of Beiping (now Beijing) in 1949, suggests that victory can be achieved through the political capitulation of the target state's elites[16]. China seeks to leverage the substantial economic dependence of Taiwanese businesses (or Taishang) on mainland markets to foster a cautious, pro-accommodation political environment.

By offering incentives and threatening penalties, Beijing encourages these influential elites to lobby Taipei's leadership to avoid open confrontation, thereby aiming to achieve unification without the military and economic costs of an invasion. This soft-power tactic seeks to erode political cohesion and create a sense of the inevitability of political alignment.

Anaconda Strategy

Beijing’s progressive squeeze on Taiwan’s sovereignty has been based on its "Three Warfares" strategy comprises public opinion warfare, psychological warfare, and legal warfare. China has executed varying components of this strategy on both friends and adversaries. Open, democratic societies such as those of Taiwan are often the target of this strategy that is executed with high intensity[17].

Disinformation Campaigns. State-backed entities, often operating from the mainland, deploy sophisticated disinformation and cyber campaigns across social media and digital platforms. The objective is to sow political discord, undermine public confidence in democratic institutions, and promote narratives favouring unification, thereby attempting to disrupt and subvert Taiwanese society.

To increase Taiwan’s isolation, Beijing has regularly severed undersea cables connecting the island to the global internet and communication network.

Cyber Attacks. Persistent cyber intrusions targeting critical infrastructure, government networks, and media outlets serve both intelligence gathering and preparatory functions for a potential conflict, aiming to disrupt command and control systems. According to its National Security Bureau, Taiwan faced an average of 2.4 million cyber-attacks daily in 2024, most of which were from China[18].

Beijing has been engaged in a sustained diplomatic offensive against Taiwan and has forced many nations to sever diplomatic ties with Taipei. In a recent case of ‘Wolf Warrior’ diplomacy, Chinese diplomats and media used abusive and threatening language against the Japanese Prime Minister, who spoke on Taiwan. China has created considerable strain on Taiwan’s international ties, including its membership in international bodies like the United Nations (UN). Such acts by China narrow Taiwan’s diplomatic options. Sir Alex Younger, former Chief of the UK Secret Intelligence Service, has described China’s campaign against Taiwan as “a textbook on subversion, cyber and political harassment”[19]. This all-encompassing strategy of China represents a traditional ‘Anaconda strategy’ that is designed to tighten gradually until Taiwan submits due to isolation and demoralization.

The Illusion of Deterrence: India's Size Does Not Deter China's Coercion

Since independence, one of India’s major foreign policy concerns has been the relationship with China. Official statements on the Indian side have regularly downplayed the underpinnings of the strategic rivalry and Chinese malfeasance towards India. Some writings by the so-called ‘China experts’ and diplomats have also favoured an accommodating policy towards China, conveniently overlooking the multi-domain threat we face from China. Evidently, the proponents of such a policy suffer from what is termed in psychology as an ‘Optimism Bias.’ In the context of diplomacy and national security, optimism bias leads decision-makers to **underestimate the probability of conflict or the severity of a rival's hostile intentions.** Indian policy on China has often displayed an optimism bias. This led to a profound underestimation of China's territorial ambitions in the Himalayas and a neglect of military preparedness along the Line of Actual Control (LAC). Till India was shaken from its stupor by the large-scale Chinese intrusions in Ladakh in 2020, this diplomatic optimism directly influenced operational and strategic negligence.

The huge difference between India and Taiwan in factors such as geography, size, population, and military power may habitually lead to downplaying the extent of the threat from China to India. Statements by some political leaders and in the seminar circuit frequently cite “India is too big and powerful to be cowed by China”, when comparisons are drawn to China’s behaviour with Taiwan and with India. This proposition misses quite a few fundamental facts. China has devoured Indian territory and seeks more. It openly propagates “Taiwan’s reunification” with mainland China - a euphemism for grabbing the territory of Taiwan, just as it harbours designs to assimilate Arunachal Pradesh. In both cases, the Chinese have spun a narrative that these regions were historically a part of China.

By deliberately employing ‘negationism’ - the denial of undisputed, well-documented historical facts and the most extreme form of historical revisionism, China has woven strange ‘fairy tales.’ This proves that China has made no distinction between Taiwan and India, regardless of the size, population, and power of India.

Asymmetric Warfare. Like Taiwan, India too has faced and continues to face the "Three Warfares" and gray zone tactics[20]. The cyberattacks on India’s critical infrastructure linked to Chinese entities mirror the cognitive and cyber warfare directed at Taiwan. Chinese cyber warfare against India is not a new phenomenon. A strategy of “killing us softly”[21] has long been employed and continues unabated. China’s strategic encirclement of India through economic inducements, security partnerships, nuclear proliferation, and political interference in India’s neighbourhood belies Chinese claims of friendship towards India. Beijing refuses to negotiate a settlement to the border issue. On the contrary, it engages in ‘legal warfare’ by renaming parts of Arunachal Pradesh. By “agreeing” to consider the supply of items critically required by India, such as tunnel boring machines, rare earths, and opening the Mansarovar pilgrimage, China has created an illusion of its softening stance towards India. The reality is different and grim. The recent case of an Indian citizen from Arunachal Pradesh being detained illegally and treated inhumanely in Shanghai is a stark reminder of China’s continued resort to coercive gray zone tactics. On trade, China remains unrelenting in denying meaningful market access to key Indian products and industries. India’s annual bilateral trade deficit of US$100 billion is strategically used not only to economically coerce India but also to strengthen the PLA. India’s deep, structural economic dependence on China represents a significant vulnerability that Beijing could easily exploit in a crisis, mirroring its economic coercion against Taiwan. China has been active in propagating an “anti-India” chronicle in India’s neighbourhood and amongst countries of the global south. In essence, China's efforts involve both active influence operations (covert social media campaigns, economic pressure) and strategic media narratives designed to undermine confidence in India's regional and global leadership capabilities.

Strategic Implications for India

The Chinese military and coercive buildup around Taiwan have profound and multifaceted implications for India, directly affecting its strategic autonomy, border security, economic resilience, and its role in the emerging Indo-Pacific security architecture. It presents a geopolitical as well as geoeconomic challenge. India’s core strategic objective remains the maintenance of a Free and Open Indo-Pacific (FOIP). Instability in the Taiwan Strait directly undermines this vision. The Taiwan Strait and the broader South China Sea region serve as a crucial artery for global commerce. Nearly 55% of India’s trade with the Indo-Pacific region, including vital commerce with key partners like Japan and South Korea, transits these SLOCs[22]. A cross-strait conflict or a prolonged Chinese blockade would severely disrupt global supply chains, leading to a catastrophic spike in energy and commodity prices, which would deal a massive blow to India's energy and food security.

Taiwan's self-governance is critical for India, as the island nation serves as an essential economic partner. This partnership ensures a broad stream of trade passes through the Taiwan Strait and into Northeast Asia. The commercial relationship is substantial, evidenced by Indo-Taiwanese trade reaching US $8.2 billion in 2023, with a projected growth rate of 26.6 percent. India's stake is further amplified by its significant trade volumes with Japan (US $22.9 billion) and South Korea (US $27.5 billion) in 2023[23] . Consequently, India has a profound interest in preserving unrestricted maritime traffic through the Taiwan Strait and the South China Sea. Should any military action toward reunification occur, the consequences for India's economy and commercial interests would be severe, potentially costing the nation as much as eight to nine percent of its GDP, according to a recent assessment by Bloomberg[24].

The Quad Imperative. As a key member of the Quad alongside the U.S., Japan, and Australia, India is strategically entangled in the Taiwan question, whether New Delhi explicitly acknowledges it or not. The Quad’s stated goal of maintaining a rules-based order makes a passive response to China’s unilateral alteration of the Taiwan status quo, untenable. While India maintains a carefully ambiguous position (urging restraint and de-escalation), a crisis would force New Delhi to take clearer, high-stakes positions that it has thus far avoided[25].

The absence of an Indian statement on the latest China-Japan disagreement reflects deep uncertainty in New Delhi regarding its willingness to challenge Beijing over the Taiwan issue or to firmly endorse the Quad's vision of a Free and Open Indo-Pacific by taking a decisive stand. India's refrain from calling out China is surprising given that Japan is its strategic partner, and is therefore likely to be perceived by the Quad as demurring in upholding international norms. An armed invasion of Taiwan could throw another possibility. As a major defence and strategic partner of the U.S. and a Quad member, the U.S. may expect logistical assistance for its warships/ aircraft at Indian bases, including the Andaman & Nicobar Islands. India's naval posture in the Indian Ocean Region (IOR) may raise China's heckles, potentially escalating tensions on the border. However, such pessimistic thoughts originate more from an awe of perceived Chinese power than a carefully evaluated assessment of the military potential of Quad. It has been argued that enhancing the military power of Quad is the key to countering China's expansionism, coercion, and revisionism in the Indo-Pacific[26]. By putting pressure on China's Achilles' Heel (the Malacca Straits and the IOR), New Delhi can prevent Beijing from restricting India's options in a Taiwan contingency.

Brahma Chellaney postulates that the attempt to integrate Taiwan serves as a critical test case for China, one that transcends simple territorial gain. It is the proving ground, whether a united security framework among democracies and economic stakeholders can withstand the challenge posed by authoritarian regimes seeking to revise global norms[27]. China's provocative actions and brinkmanship in the region risk triggering an armed confrontation that could spiral into a major war. Deterrence through military capability is hence Nulla est alia electio (no other choice/ alternative).

Learning from Taiwan's Fight Against Chinese Coercion

China's relentless intimidation of Taiwan offers valuable lessons in the conduct of hybrid warfare on one hand (China) and resilience on the other (Taiwan). That a relatively small island democracy can successfully withstand the might of a major power is a testimony to the steadfast citizens of Taiwan and the values they hold close. Taiwan's success in building societal and technological resilience against this hybrid aggression offers a crucial template for India's own security and defence planning. The valuable lessons derived from Taiwan's development of "resilience as deterrence" against cognitive warfare are highly relevant for other democracies[28] such as India, Japan, the Philippines, and South Korea, who have been subjected to Chinese subterfuge. A crucial element of India's strategy in the Indo-Pacific must be building resilience against China's coercive model. This requires a coordinated approach covering both economic de-risking and the adoption of counter-coercion tactics, with Taiwan's experience offering invaluable lessons.

Proactive Narrative Defence. Taiwan treats narrative defence as proactive competition. The government and civil society actively work to counter disinformation. China's cognitive and information campaign in India (e.g., against Indian politicians, or during military stand-offs) mirrors the political warfare directed at Taiwan. India must learn to use open-source intelligence and civilian technology to identify, debunk, and rapidly expose China-backed disinformation campaigns[29].

Media and Digital Literacy. Taiwan focuses on public education and media literacy to inoculate its population against manipulation. India could benefit from integrating media literacy programs to enhance societal immunity to propaganda that aims to sow political/religious discord or undermine trust in democratic institutions[30].

Asymmetric and Hybrid Capabilities (Gray Zone). Taiwan's military strategy emphasizes agility, survivability, and cost-effective deterrence over conventional parity, which is crucial for India given the resource imbalance with China. Taiwan is prioritizing asymmetric defence capabilities like coastal defence missile systems, advanced drone technology, and anti-access/area denial (A2/AD) capabilities. For India, this translates to accelerating investment in air power, swarm drones, electronic warfare, and specialized forces for mountainous terrain, shifting the cost-imposition equation on the LAC. Simultaneously, Indian doctrine should embrace developing multi-domain asymmetric offensive capabilities to inflict substantial and unsustainable costs on China.

Law Enforcement Over Military. Taiwan frequently uses its Coast Guard Administration (CGA) for monitoring and responding to routine Chinese maritime incursions and illegal sand dredging. This strategy of responding with a law enforcement vessel rather than a warship keeps the response below the threshold of military conflict while still asserting jurisdiction and publicizing the incursions[31]. India can judiciously and selectively apply this philosophy on its maritime expanse to counter ambiguous gray zone operations.

Transparency as Deterrence. Taiwan's policy of publicizing Chinese military and gray zone activities (e.g., releasing daily PLA aircraft statistics) exposes Beijing's coercion to international scrutiny. India must similarly increase transparency in documenting and reporting Chinese incursions and cyber-attacks. Not only will it help enlighten our population about the nefarious designs of China, but also help build a case for collective international action.

Tech Diplomacy. India should leverage its growing technological capabilities in IT services sector and Digital Public Infrastructure (DPI) to strengthen partnerships with fellow democratic nations, especially within the Quad framework. This cooperation should guarantee that the participating countries possess the means for sharing cyber threat intelligence and developing quick response mechanisms collectively[32].

Network of Excellence. Taiwan has sought to build a regional 'Network of Excellence' to share lessons on countering maritime gray zone issues and lawfare. India should proactively establish bilateral and multilateral platforms with Taiwan, the Philippines, Japan, and other affected nations to institutionalize this sharing of expertise[33].

India's Strategic Options and Policy Pathways

India's path to growth and prosperity is dependent upon a stable Indo-Pacific where the balance of power is not tilted in China's favour. Building individual capacities is time-consuming and costly. However, forming strong partnerships, including quasi-military alliances with nations at the receiving end of Chinese belligerence will economize costs, shorten timelines in building capacities and provide a credible deterrent to China. Questions may arise if such arrangements will compromise India's strategic autonomy. The counter-argument is that in the face of a rising, revisionist power like China, strategic autonomy must maximise India's options and capabilities. Quasi-alliances become a tool to strengthen autonomy, not restrict it. Strategic autonomy is only viable when a nation possesses the requisite Comprehensive National Power (CNP) to make independent choices. China's assertiveness and the power differential between the two nations limits India's autonomy. By partnering with the Quad and East Asian nations, India can create a collective regional equilibrium. China is less likely to engage in coercive or aggressive actions against an individual nation (India) when it faces a unified front of like-minded regional powers. This can act as a viable deterrence and preserve India's freedom of action. India's gains with such an alliance could include access to critical military intelligence, advanced technology (via groups like the Quad's Initiative on Critical and Emerging Technologies - iCET), and joint exercises (like Malabar) that rapidly enhance its naval and defence capabilities. Strengthening India's core power through partners makes its autonomy more credible.

India must significantly bolster its security and intelligence exchanges with Taiwan, even if they are termed 'unofficial.' This includes sharing best practices on cybersecurity, cognitive warfare defence, and drone technology - areas where Taiwan is a global leader Such cooperation enhances mutual resilience without overtly crossing China's political red lines. India should leverage its rising stature in global institutions to consistently call out and condemn destabilizing gray zone activities by any state, promote a clear defence of international law, freedom of navigation, and a rules-based maritime order. This will strengthen the normative framework that secures India's own interests in the Indo-Pacific. A crucial element of India's strategy in the Indo-Pacific must be building resilience against China's coercive model. This requires a coordinated approach covering both economic de-risking and the adoption of counter-coercion tactics, with Taiwan's experience offering invaluable lessons.

Conclusion

China’s coercive campaign against Taiwan is a strategic paradigm that encapsulates its aspirations for regional hegemony, demonstrating a willingness to leverage all instruments of national power - military, economic, and informational to alter the status quo. For India, this crisis is not a distant event but a critical challenge that intersects directly with its core security, economic, and geopolitical interests. The primary strategic challenge for New Delhi is managing the risk of Chinese escalation on the LAC while simultaneously contributing to the stability of the Indo-Pacific. A failure to build resilience and strategically align with partners on the Taiwan issue would not only expose India’s burgeoning economy to catastrophic disruption but also grant China significant leverage over India's strategic choices.

Therefore, India’s path forward requires a decisive shift: transforming its economic vulnerability into strategic resilience through supply chain diversification, leveraging partners like Taiwan for critical technologies (e.g., semiconductors), and proactively using the Quad and other forums to strengthen collective deterrence against gray zone tactics and uphold the norms of a peaceful and open Indo-Pacific. However, diplomacy without the backing of genuine hard power is just thin air. China respects strength, and hence, building military power, especially naval, air, and asymmetric capabilities, is essential to underpin India's strategic autonomy and create the necessary deterrence gradient to make Beijing see sense. The strategic stability of the Taiwan Strait and the security of the Himalayan frontier are two sides of the same coin, demanding a coherent, all-of-nation strategy that unifies military readiness, diplomatic leverage, and rapid, indigenous technological development (Aatmanirbharta). In the face of a revisionist China, the choice between partnership and appeasement is existential. Placating Beijing at the expense of partnering with regional democracies, especially Taiwan, will only bring strategic despair and systemic instability to Asia, India included.

Endnotes

1. https://rnamedia.in/international/china-simulates-attacks-on-foreign-ships-in-strait-as-taiwan-expands-intelligence-sharing-with-partners/11443#:~:text=Taiwan%20views%20these%20operations%20as,%2C%E2%80%9D%20took%20place%20in%20April.
2. Benjamin Lewis, Thomas Shattuck, ‘A New Frontier: PRC Flight Activity to the East of Taiwan’, Global Taiwan Brief, Vol 9, Issue 17 available at https://globaltaiwan.org/2024/09/a-new-frontier-prc-flight-activity-to-taiwans-east/#:~:text=The%20main%20point%3A%20Since%20Taiwan's,flights%20east%20of%20Taiwan%20is
3. Bonny Lin, Brian Hart, Matthew P. Funaiole, Samantha Lu, and Truly Tinsley, CSIS Brief, 05 June 2024 available at https://www.csis.org/analysis/how-china-could-quarantine-taiwan-mapping-out-two-possible-scenarios#:~:text=In%20August%202022%20and%20April,Taiwan%20and%20its%20outlying%20islands.
4. Craig Singleton, Rear Adm Mark Montgomery (retd), Benjamin Jensen, ‘Chinese Coercion of Taiwan’s Energy Lifelines: A Contest Taiwan and the West Can’t Afford to Lose’, 17 November 2025 available at https://www.fdd.org/analysis/2025/11/17/chinese-coercion-of-taiwans-energy-lifelines-a-contest-taiwan-and-the-west-cant-afford-to-lose/#:~:text=Through%20consistent%20exercises%2C%20the%20People's,control%20over%20critical%20sea%20lanes.

5. Suyash Desai, ‘A ‘Cold Start’ Military Posture with Chinese Characteristics’, 24 November 2025 available at https://chinapower.csis.org/analysis/pla-cold-start/

6. Estelle Huang, ‘The Taiwan test: Why Europe should help deter China’, 25 November 2025 available at https://ecfr.eu/publication/the-taiwan-test-why-europe-should-help-deter-china/

7. Suyash Desai, op cit

8. Timothy A. Walton & Thomas H. Shugart, ‘Concrete Sky: Air Base Hardening in the Western Pacific’, 07 January 2025, Hudson Institute Report available at https://www.hudson.org/arms-control-nonproliferation/concrete-sky-air-base-hardening-western-pacific-timothy-walton-thomas-shugart#:~:text=now%20has%20134%20air%20bases%20within%201%2C000%20nautical%20miles%20of%20the%20Taiwan%20Strait

9. Estelle Huang, op cit

10. Damien Symon on X (formerly Twitter) @detresfa_ , available at https://x.com/detresfa_ posted on 07 October 2025

11. Damien Symon on X (formerly Twitter) posted on 04 November 2025, https://x.com/detresfa_

12. Damein Symon, https://x.com/detresfa_

13. K. Tristen Tang, Less Politics, ‘More Military: The Outlook for China’s 2025 Military Incursions into Taiwan’s Airspace and Waters’, Journal of Indo-Pacific Affairs, 21 April 2025, available at https://www.airuniversity.af.edu/JIPA/Display/Article/4176900/less-politics-more-military-the-outlook-for-chinas-2025-military-incursions-int/

14. Ibid

15. Hung Tran, ‘Expect Chinese economic retaliation against Taiwan after the DPP’s presidential victory’, 25 January 2024 available at https://www.atlanticcouncil.org/blogs/econographics/expect-chinese-economic-retaliation-against-taiwan-after-the-dpps-presidential-victory/#:~:text=A%20month%20before%20Taiwan's%20elections,Taiwan's%20discriminatory%20policies%20against%20Chinese

16. ‘The Beiping model: How China could absorb Taiwan without a war’, Lowy Institute, 15 May 2025, available at https://www.lowyinstitute.org/the-interpreter/beiping-model-how-china-could-absorb-taiwan-without-war#:~:text=It%20needs%20only%20to%20offer,to%20its%20leadership%2C%20and%20wait.

17. Dr Philip Shetler-Jones, ‘Taiwan’s Evolving Response to China’s Grey Zone Actions’, 31 March 2025, available at https://www.rusi.org/explore-our-research/publications/policy-briefs/taiwans-evolving-response-chinas-grey-zone-actions

18. Yimou Lee, Reuters, 06 January 2025 available at https://www.reuters.com/technology/cybersecurity/chinese-cyberattacks-taiwan-government-averaged-24-mln-day-2024-report-says-2025-01-06/

19. Dr Philip Shetler-Jones, op cit

20. Eerishika Pankaj, ‘Lessons for India: How Taiwan Handles Chinese Political Warfare’, Global Taiwan Brief, Vol 10, Issue 13, 02 July 2025 available at https://globaltaiwan.org/2025/07/lessons-for-india/

21. Praveer Purohit, ‘Killing Us Softly: Chinese Cyber Warfare Against India’, CASS Journal, October-December 2024, Vol 12, No. 3, pp 1-18

22. Harsh V. Pant, ‘India and the China-Taiwan Conflict: The Military Dimension’, 27 March 2023 available at https://www.orfonline.org/research/india-and-the-china-taiwan-conflict

23. Souhardya De & William Budd, 'India's Taiwanese Security Policy: A Priority for Regional Security in the Indo-Pacific', 02 October 2024, available at https://globaltaiwan.org/2024/10/indias-taiwanese-security-policy/

24. Dhruva Jaishankar, 'Why Taiwan's Future Matters for India', 18 January 2024, available at https://orfamerica.org/newresearch/indian-foreignpolicy-2024

25. Ivan Lidarev, 'China-Japan Taiwan Row: India's Strategic Hesitations', 01 December 2025, available at https://www.isas.nus.edu.sg/papers/china-japan-taiwan-row-indias-strategic-hesitations/

26. Praveer Purohit, 'Enhance the Military Power of Quad for a Stable Indo-Pacific', FINS Journal of Diplomacy & Strategy, Jan-Mar 2025, Issue No. 1, Vol 8, pp 29-37

27. Brahma Chellaney, 'Taiwan the fulcrum of deterrence', Taipei Times, 19 May 2025, available at https://www.taipeitimes.com/News/editorials/archives/2025/05/19/2003837112

28. Eerishika Pankaj, op cit

29. Ibid

30. Dr Philip Shetler-Jones, op cit

31. Huynh Tam Sang, 'Taiwan's Coast Guard: Countering China's Gray-Zone Actions', 10 June 2025, available at https://pacforum.org/publications/yl-blog-129-taiwans-coast-guard-countering-chinas-gray-zone-actions/

32. Angad Singh, 'Why India Should Push Back Against China's Belligerence', The Diplomat, 18 March 2024

33. Dr Philip Shetler-Jones, op cit

About the Author:

Gp Capt Praveer Purohit (retd) is a former IAF pilot with over three decades of service. He writes regularly on defence and strategic issues. His articles, Op Eds and analyses have been published in a variety of digital and print media such as Indian Express, Financial Express, Millennium Post, Sakal, Tarun Bharat, CASS Journal, Journal of Defence Studies, USI Journal, Air Power Journal, FINS Journal of Diplomacy & Strategy, FINS Bulletin, South Asia Monitor etc. The author can be contacted at praveerp@rediffmail.com and his X (formerly Twitter) handle is @aparagonpilot

Towards Institutionalising India's Critical Infrastructure Protection Programme: Twin Pillars, One Foundation, and One Measurable Framework

Abstract:

This paper examines India's fragmented Critical Infrastructure Protection (CIP) landscape at a time when asymmetric threats, cyber intrusions and systemic vulnerabilities have elevated CIP from a technical concern to a strategic necessity[1] . Current arrangements under the National Critical Information Infrastructure Protection Centre (NCIIPC) remain confined to information assets and leave physical infrastructures, sectoral interdependencies and resilience standards outside effective oversight. To address this gap, the paper advances an integrated statutory and evaluative architecture built on the Critical Infrastructure Protection Act (CIPA), which provides inspection authority, penalties, incident reporting and coordinated response, and the Bharat National Resilience Index (BNRI), which establishes quantifiable resilience thresholds across preparedness, mitigation, response and recovery. The approach moves beyond Western standalone critical-sector templates and incorporates India-specific sectoral clusters previously detailed by the author and published in this journal, capturing the country's system-of-systems vulnerabilities, federal asymmetry and hybrid threat exposure. Through the combined structure of the Twin Pillars, One Foundation and One Measurable Framework, the model shifts CIP from voluntary aspiration to legal mandate[2]. By aligning technological, cyber-geopolitical, economic, disaster-management, statutory, governance and national security perspectives within one measurable framework, the paper presents an India-specific criticality lens that offers a coherent blueprint for institutionalising CIP and a normative reference for states across the Global South confronting comparable structural constraints.

1. Introduction

India's infrastructure ecosystem is exposed to expanding and intricate risks as hybridised threats exploit cyber-physical interdependencies and generate cascading failures across essential networks. Current governance rests on the mandate of the National Critical Information Infrastructure Protection Centre (NCIIPC) under Section 70A of the IT Act. This mandate remains confined to information assets and does not extend to physical infrastructure, operational linkages or inter-sector dependencies that shape real-world vulnerabilities[3]. The limits of this arrangement have already appeared. The RedEcho-linked intrusion targeting India's power infrastructure, publicly examined by Recorded Future and reviewed by Indian authorities, coincided with the 2020 Mumbai outage and illustrated how a digital compromise can align with physical disruption and produce wide economic impact, even though official attribution remains cautious[4]. The episode affirmed a larger structural issue. Cyber-only frameworks cannot manage systemic risks that travel across sectors, operational environments and federal jurisdictions[5].

Comparative experiences clarify the constraints and possibilities for India. The United States relies on voluntarism and private-sector coordination under the National Infrastructure Protection Plan, an approach shaped by its regulatory culture and market structure[6]. The European Union enforces uniform obligations through the NIS2 Directive and applies common security baselines across member states[7]. China follows concentrated administrative control. Australia's SOCI Act incorporates mandatory incident reporting, supply-chain scrutiny and foreign-investment monitoring, an approach enabled by its legislative design[8]. These models are informative but emerge from institutional and economic environments very different from India's federal and resource conditions. Prior research therefore calls for an India-specific criticality lens that treats infrastructure as a system of systems where local failures can spill into governance, economic continuity and national security[9].

This paper develops a Critical Infrastructure Protection Programme (CIPP) around three linked elements: Twin Pillars, One Foundation and One Measurable Framework. The first pillar, the Critical Infrastructure Protection Act (CIPA), provides statutory authority for inspections, reporting, audits and multi-ministerial coordination and brings legal clarity to responsibilities that currently remain dispersed.

The second pillar, the Bharat National Resilience Index (BNRI), introduces measurable resilience indicators that capture redundancy, recovery timelines and systemic continuity and aligns institutional expectations with quantifiable outcomes. The foundation expands sectoral attention beyond energy, transport and ICT to include logistics, agriculture, water ecosystems, public health, judicial systems and maritime corridors. These domains rarely appear in global frameworks even though they remain central to India's socio-economic and strategic stability.

The measurable framework assesses resilience across seven analytical dimensions that encompass technology, legal preparedness, economic structures, disaster governance, institutional capacity and national security. This integrated structure reduces fragmented reporting and weakens silo-driven oversight by consolidating assessment within a single evaluative logic.

Taken together, these elements position India's CIP pathway as distinct from prevailing Western or Chinese templates and more comprehensive than incremental extensions of cyber-centric requirements. They establish a statutory, metrics-based and sector-expanded governance structure in which coordination and evaluation operate within one combined programme. Through this shift, India strengthens its role as a normative contributor within the Global South and shapes resilience approaches suited to federal diversity and resource-constrained operational settings[10].

2. The Foundation: Reimagining Sectoral Priorities

The foundation of a Critical Infrastructure Protection Programme (CIPP) for India must begin with a decisive shift in how sectors are prioritised. Conventional templates drawn from advanced economies cannot be transferred without modification. As argued in Towards a Critical Infrastructure Protection Programme for India: Reconceptualising Sectoral Priorities for Strategic Resilience and National Security[11], the direct use of frameworks such as the United States National Infrastructure Protection Plan or the European Union's NIS and NIS2 regimes would be misaligned with India's developmental stage, socio-economic variation and federal asymmetry. These models function effectively in industrialised contexts that concentrate on capital-intensive infrastructures including energy, ICT, finance and transportation. They leave aside several sectors that remain structurally fragile and essential in India.

India requires an India-specific criticality lens that interprets vulnerability not as isolated sectors but as interlinked dependencies that function as a system of systems[12]. India's fragility is rooted in water, agriculture, logistics, health systems and judiciary infrastructure. Disruptions in these domains create ripple effects. Water scarcity in drought-prone states can weaken food security, constrain hydro-electric output and place pressure on urban resilience. Instability in agriculture combined with interruptions in logistics often leads to food inflation, heightened public health risks and political tension. The COVID-19 pandemic demonstrated the interconnected operations of healthcare, transport corridors, ICT networks and pharmaceutical supply chains. Judicial infrastructure, including e-courts and digital registries, supports the continuity of governance. If compromised, it would slow institutional processes and weaken public trust. Global studies of developing economies show similar patterns where shocks disproportionately destabilise food and health systems and reinforce the need for widened sectoral prioritisation [13].

Maritime corridors and blue-water infrastructure hold comparable weight. Ports, undersea cables and coastal economic zones are often absent in Western CIP lists, yet for India they support Indo-Pacific engagement, trade security and defence logistics[14]. Their protection has direct strategic implications. Innovation ecosystems that include MSMEs, start-ups, semiconductor clusters and advanced research networks also represent critical assets. These nodes contribute to technological sovereignty, and their compromise through cyber-physical intrusions would undermine digital exports, advanced manufacturing and knowledge-driven growth.

Operational experience reinforces the limitations of narrow classifications. NCIIPC's mandate under Section 70A of the IT Act remains restricted to information systems. Repeated intrusions such as the RedEcho activity linked to the Mumbai power grid highlight how digital compromise can coincide with physical disruption and wider systemic paralysis, even in the absence of full attribution[15].

This confirms that India cannot rely on a cyber-focused framework. A national CIPP must codify a wider sectoral base that includes conventional assets such as energy, ICT, finance and the defence industrial base, socio-economic backbones including water systems, agriculture, healthcare, judiciary and public service delivery chains, strategic frontiers that encompass maritime corridors, nuclear plants, space assets and rare-earth or semiconductor ecosystems, and innovation clusters comprising MSMEs, start-ups, frontier research centres and digital platforms.

This shift reflects statutory necessity rather than conceptual preference. Without legal recognition, these sectors will remain under-protected. As stressed in Hybrid dimension of critical information infrastructure security: Why India needs a CIPA to attain cyber-physical resilience[16] and Compulsions of enacting a Critical Infrastructure Protection Act[17], hybrid threats routinely exploit the intersections where governance, economic activity and societal reliance converge. Experiences across the Critical Five nations further illustrate this evolution. Australia's SOCI Act integrates supply-chain resilience and foreign investment scrutiny. The United Kingdom's Critical National Infrastructure Knowledge Base identifies dependencies beyond classical sectors[18]. UNDRR similarly notes that resilience frameworks in the Global South must include non-classical infrastructures such as water systems, natural ecosystems and dense urban settlements because they often act as catalysts for cascading disruption[19].

By embedding this reimagined taxonomy into law, India must set the foundation of its CIPP. This broadened structure ensures that resilience planning incorporates ecological pressures, federal asymmetry, population density and hybrid warfare risks. Such codification provides the structural depth required to absorb shocks, adapt to shifting threats and sustain functional continuity without systemic collapse.

3. The First Pillar: Critical Infrastructure Protection Act (CIPA)

A major gap within India's Critical Infrastructure Protection landscape is the absence of statutory authority. The National Critical Information Infrastructure Protection Centre (NCIIPC) under Section 70A of the IT Act governs information infrastructure, yet its jurisdiction does not cover physical systems, sectoral interdependencies or hybrid threat environments that increasingly shape national vulnerability[20]. This narrow cyber focus has produced a fragmented protection ecosystem that cannot keep pace with environments where cyber intrusions, physical disruption and geopolitical interference interact with growing frequency. As highlighted across multiple policy analyses[21], the Critical Infrastructure Protection Act (CIPA) has become essential, not as a procedural refinement but as a statutory instrument required for national security and strategic resilience.

3.1 Geopolitical and Hybrid Threat Drivers

The South Asian and Indo-Pacific regions remain volatile, and state as well as non-state adversaries continue to target critical infrastructure to weaken India's strategic posture. Pakistan's support for cross-border attacks against transport systems, energy networks and defence sites remain documented across several assessments[22]. China's dual approach, which combines assertiveness along the Line of Actual Control with infrastructure leverage through Belt and Road corridors in Sri Lanka, Nepal and Bangladesh, creates a two-tier vulnerability where sabotage could be paired with pressure in the grey zone. Bangladesh has also experienced extremist strikes against infrastructure, signalling spillover risks along India's porous borders[23]. Global precedents reinforce this pattern. The Nord Stream pipeline sabotage demonstrated how critical infrastructure can become an instrument of geopolitical confrontation in contested regions[24].

Threats of this nature cannot be managed through voluntary arrangements or isolated departmental mandates. Hybrid conflict blends cyber disruption with narrative manipulation and physical sabotage. Responding to this environment requires statutory inspection authority, enforceable compliance and rapid operational capability. Without CIPA, India remains reactive, capacity-fragmented and institutionally dispersed in the face of adversarial intent[25].

3.2 Structural Mandates of CIPA

CIPA should establish the National Critical Infrastructure Protection Authority (NCIA) with jurisdiction that spans sectors and ministries and with the ability to issue emergency directives when national interests require unified action. Its mandates include risk audits and sectoral inspections conducted independently and benchmarked against global models that draw from United States federal directives and mandatory European Union risk assessment requirements[26]. It should also enforce incident reporting and transparency through compulsory disclosure within twenty-four hours of any cyber or physical disruption, in line with NIS2 expectations and replacing the opaque reporting tendencies currently observed[27]. CIPA must mandate resilience drills and red teaming through annual sector-level exercises and bi-annual integrated national drills, a practice central to both the United States NIPP approach and the methodologies followed by the Critical Five nations[28]. Emergency directive powers would authorise shutdowns, activation of continuity mechanisms or issuance of immediate protection orders during national emergencies. This parallels element of the Chinese sovereign approach while being adapted to India's federal democratic structure[29].

CIPA should also establish accountability within public private partnerships through mandatory resilience clauses, penalties for concealment and structured liability for operators who fail to meet compliance obligations[30]. Sectoral notification and expansion must include non-traditional sectors such as judiciary, logistics, agriculture and maritime infrastructure, aligning with the broadened taxonomy established earlier and ensuring that statutory protection spans all domains that contribute to national continuity[31].

3.3 Economic and Strategic Justifications

The economic purpose of CIPA aligns with investor confidence and India's position within global value chains. The objective of making India a manufacturing and supply-chain hub rests on assured resilience across essential systems. Cyberattacks on banking networks and ransomware incidents that have disrupted healthcare facilities demonstrate how vulnerabilities undermine operational stability and weaken investor trust[32]. By embedding resilience requirements in law, CIPA positions security as an economic enabler and a prerequisite for predictable growth[33]. Global investment studies show a clear link between statutory resilience regulation and inward capital flows, particularly in emerging economies where risk perception directly influences investment decisions[34].

CIPA also contributes to national strategic autonomy. As examined in Protecting India's Critical Infrastructure[35], failures in infrastructure do not remain confined to operational or financial domains. They can trigger national security shocks that evolve into political or governance crises. Legislating baseline resilience expectations strengthens deterrence against intentional disruption and reinforces India's credibility within global security frameworks.

3.4 Global Precedents and the Legislative Imperative

Global experience shows why statutory protection of critical infrastructure has become indispensable. The United States adopted the Homeland Security Act after 9/11 to institutionalise integrated protection. The United Kingdom introduced legal resilience standards following the Manchester attack. Australia's SOCI Act created a Critical Infrastructure Centre with authority over foreign involvement. Israel consolidated cybersecurity oversight under a National Cyber Directorate, while Germany enacted the IT Security Act to enforce resilience obligations across essential operators[36]. Scholarship concludes that statutory authority is the decisive threshold separating voluntary resilience from enforceable resilience, particularly where interdependent systems are exposed to hybrid threats[37]. For India, the implication is direct. Without legal codification, responses to hybrid attacks will remain fragmented and reactive, and interdependency governance will continue to suffer from institutional gaps. A national CIPA would close these gaps, establish accountability across operators and embed resilience within the legal framework of national security. It is not a procedural addition. It is a strategic requirement.

4. The Second Pillar: Bharat National Resilience Index (BNRI)

Resilience cannot be institutionalised without measurement, and a framework cannot influence behaviour unless it is enforceable. India's current CIP approach lacks quantifiable benchmarks, which leaves resilience framed as policy language rather than legal requirement. Existing tools such as the Resilience Measurement Index[38] or lifecycle methodologies developed by Fraunhofer and OECD offer conceptual direction but do not align with India's governance realities. Federal asymmetry, uneven institutional capacity and development disparities make direct adoption impractical. India therefore requires its own statutory index that calibrates resilience against systemic vulnerabilities and sets mandatory compliance across operators. The Bharat National Resilience Index (BNRI) addresses this dual need. It functions as a regulatory instrument that creates accountability and as a knowledge system that supports continuous learning. Comparative research has already concluded that indices without statutory authority remain voluntary guidelines and cannot deliver enforceable obligations[39].

4.1 Conceptual Foundations

BNRI is grounded in the premise that resilience is measurable across preparedness, mitigation, response and recovery. It begins with the recognition that Indian infrastructures operate as interconnected systems rather than isolated sectors and that they reflect system-of-systems vulnerabilities[40]. The index therefore evaluates both sector-level robustness and the strength of interdependencies across diverse critical sector and sectorial clusters. BNRI formalises resilience as a property of networks and not as a sum of silos. By placing BNRI within the structure of the Critical Infrastructure Protection Act (CIPA), ambiguity in responsibilities is removed. Operators cannot treat resilience as discretionary expenditure, and statutory inspection, measurable thresholds and liability enforcement ensure that compliance becomes compulsory.

4.2 Structure of BNRI Metrics

BNRI applies a tiered structure comprising Tier-A, Tier-B and Tier-C. This avoids a single uniform mandate and ensures proportional compliance across operators with varying capacities. The approach is necessary in India because a common standard would either overwhelm small operators or leave nationally critical assets inadequately protected. Graduated obligation becomes the organising logic. Systems with higher national importance carry a greater statutory burden, while those with limited systemic impact maintain essential baselines.

Tier-A assets, which include nationally indispensable systems such as ports, major reservoirs and power substations, require the highest level of protection. They must conduct mandatory digital-twin simulations to map systemic vulnerabilities and to allow stress testing before real incidents occur. A failure in one major substation, for instance, could reveal cascading impacts across water pumping operations, hospitals or aviation networks. Digital twins expose weaknesses in controlled conditions. Tier-A systems must also adopt AI-driven anomaly detection with predictive analytics[41], since advanced tools identify micro deviations that signal hostile intrusion or technical deterioration. Predictive alerting is essential for these assets because reactive approaches cannot contain national-scale risks. Continuous red teaming across cyber and physical environments is also required. Red teams simulate adversarial behaviour and uncover insider risk, physical gaps and digital weaknesses. Finally, Tier-A resilience must include statutory codification of Mean Time to Recovery (MTTR). MTTR determines whether a disruption stays contained or escalates into systemic paralysis. Embedding MTTR in law compels redundancy planning, continuity protocols and rapid restoration capacity.

Tier-B assets, such as regional water systems, airports and regional power grids, hold significant yet geographically bounded importance. These systems must meet compulsory Multi-Factor Authentication and cyber hygiene standards, since regional networks are frequent ransomware targets due to weak authentication. BNRI establishes MFA as the minimum defence baseline. Mandatory incident reporting within twenty-four hours is also required because underreporting increases the likelihood that local failures evolve into broader disruptions. Annual resilience audits must be conducted across cyber, physical and operational dimensions. These audits examine technical controls, staff readiness, fallback procedures and exposure to environmental or hazard risks.

Tier-C assets, which include entities with limited systemic impact such as rural hospitals or regional logistics hubs, follow requirements that focus on patch management, reporting and basic workforce training. These measures establish a national resilience floor and prevent Tier-C entities from becoming entry points for wider compromise. Ransomware incidents targeting unpatched rural health systems have already demonstrated how seemingly small breaches can propagate into national digital platforms.

This calibrated structure avoids excessive regulation of small operators while strengthening resilience in critical systems. Tier-A carries binding statutory obligations. Tier-B applies proportionate requirements, and Tier-C maintains a mandatory minimum baseline. The tiering framework places resilience within a connected continuum rather than a fragmented set of protections.

4.3 Integration with Global Practices

BNRI draws on international experience but avoids direct replication. Many global indices assume uniform institutional capacity, a condition that India does not share. NIST's Cybersecurity Performance Goals[42] and the EU's NIS2 Directive function within environments that maintain strong enforcement and high compliance culture. The Critical Five models, most notably Australia's SOCI Act, underline the importance of supply-chain resilience and mandatory audits[43]. India faces different vulnerabilities. Long-term water scarcity, an agriculture-dependent economic base and uneven digitalisation within judiciary systems require an adaptive model rather than a transferred one. Codifying BNRI allows India to function as a normative designer instead of a passive adopter. Just as NIST evolved into a global reference for cyber maturity, BNRI holds potential to serve as a resilience framework for the Global South. Scholarship already recognises that resilience models for developing states cannot rely on Western sectoral checklists and must reflect contextual realities and operational constraints[44].

4.4 Regulatory and Research Dualism

BNRI carries a dual purpose. As a regulatory instrument, it equips NCIA with enforceable tools. Mandatory drills, statutory audits and incident reporting create measurable compliance and legal accountability[45]. As a knowledge repository, it functions as a living system. Data generated through audits, inspections, red-team exercises and institutional assessments supports continuous research-driven refinement. This design prevents BNRI from becoming a static checklist and ensures that it remains responsive to evolving hybrid threats. At the same time, it positions India within an international landscape shaped by standards such as ISO and IEC 27001:2022 for cyber resilience, the UNDRR Sendai Framework for disaster governance and NATO's 2022 Strategic Concept where infrastructure resilience entered collective security discussions[46]. Through this alignment, India strengthens domestic capability while contributing meaningfully to global resilience governance.

4.5 Prescriptive Value

Institutionalising BNRI addresses several structural gaps simultaneously. It introduces enforceability, shifting resilience from voluntary aspiration to legal requirement where non-compliance generates liability. It formalises prioritisation by assigning the highest protection obligations to Tier-A infrastructures due to their cascading risk potential, while Tier-B and Tier-C systems are governed proportionately to establish a national resilience floor. It also brings transparency through measurable benchmarking. India gains the ability to assess resilience capacity with quantifiable indicators and present readiness in international platforms. BNRI therefore becomes more than an administrative mechanism. It establishes a doctrinal base and positions India as a knowledge producer rather than a policy borrower in the global resilience landscape[47].

5. The Measurable Framework: Comprehensive Protection Programme

Operationalising the Critical Infrastructure Protection Programme (CIPP) requires measurement. Intent must translate into enforceable standards. Building on the Bharat National Resilience Index (BNRI), this framework introduces a layered evaluation structure across seven analytical perspectives. These include technological, cyber-geopolitical, economic, disaster-

Each perspective converts resilience from policy language into statutory obligation, ensuring that compliance becomes a daily operational requirement. These principles, outlined in Critical Infrastructure Protection in a Cyber-Physical World[48], are now structured as mandates for regulators, operators and policymakers.

5.1 Technological Priorities

India's technological exposure arises from legacy OT and SCADA systems that continue to operate without adequate segmentation across power, logistics, healthcare and transport networks[49] [50]. The RedEcho activity affecting Mumbai demonstrated this vulnerability. A digital intrusion moved rapidly because network segmentation was weak and MFA adoption remained inconsistent across operators[51] [52]. Evidence indicates that MFA reduces breach success by more than 90 percent, yet many Tier-B systems still treat it as optional[53].

BNRI formalises statutory requirements by mandating OT and SCADA segmentation across Tier-A and Tier-B systems so that a single failure cannot cascade across the network. Zero trust architecture with MFA becomes baseline access control. A national AI-enabled anomaly detection grid, aligned with predictive analytics models, provides early warning as a national capability rather than a localised practice[54]. A resilience levy supports retrofitting of legacy systems, acknowledging that cost cannot remain a justification for delayed implementation. This structure aligns India with the U.S. CISA OT and ICS performance objectives[55], while CIPA embeds enforceability across operators.

5.2 Cyber-Driven World Order

Strategic competition increasingly unfolds in cyberspace, where intrusions combine digital disruption with physical damage, narrative manipulation and proxy escalation. India's deterrence posture remains largely declaratory, and no statutory escalation scale currently exists to define thresholds for hybrid response[56]. Threat intelligence sharing among CERT-In, NCIIPC and sectoral regulators also remains uneven. The U.S. ISAC ecosystems and the EU NIS2 collaboration mechanisms demonstrate the operational advantage of real-time collective situational awareness and coordinated threat tracking [57] [58].

The measurable framework therefore requires a statutory doctrine of cyber deterrence that defines thresholds for hybrid escalation, mandatory ISAC-style intelligence exchange platforms to ensure adversarial tactics are detected and countered in real time, zero trust enforcement in designated critical sectors to reduce insider threat and lateral movement, and standardised SOC maturity at Tier-3 nationwide with state support for smaller operators. Once formalised in law, resilience enters doctrine and national security incorporates enforceable cyber readiness.

5.3 Economic and Business Technicalities

Economic structures supporting resilience remain underdeveloped. Australia's SOCI Act integrates resilience audits into cost calculation models and links investment decisions with measurable security requirements[59]. India does not follow this practice. Costed resilience planning is often missing, PPP contracts rarely enforce liability for non-compliance, and incident disclosure lacks transparency. Blockchain-based validation across logistics corridors has not yet been implemented even though it offers safeguards against tampering and counterfeit movement. These gaps sustain the perception of resilience as a burden rather than a long-term economic safeguard.

BNRI introduces measurable economic obligations that shift this trajectory. Costed resilience planning becomes a statutory requirement within capital expenditure decisions. Liability mandates in PPP frameworks penalise concealment or non-implementation of resilience measures. Public disclosure of critical infrastructure disruptions improves transparency and reinforces investor confidence. Blockchain-driven verification across logistics and customs networks counters counterfeit goods, reduces tampering and protects revenue channels. Such codification aligns with global trends that position resilience investment within core infrastructure planning rather than as an external or optional layer[60].

5.4 Disaster Management

India remains vulnerable to recurring cyclones, floods and seismic events, and these hazards amplify systemic fragility when combined with cyber intrusions[61]. Silos between NDMA, SDMAs, CERT-In and NCIIPC continue to limit integrated hazard intelligence. Multi-hazard playbooks exist but remain early stage, and joint exercises are limited despite established precedents such as the U.S. NIPP [62] and the obligations under the UNDRR Sendai Framework[63].

Prescriptive mandates therefore include statutory convergence between NDMA and NCIA to enable integrated disaster and cyber resilience drills, mandatory biennial joint exercises across energy, health, transport and logistics systems, and the integration of meteorological forecasting tools with CI monitoring platforms so predictive hazard data feeds directly into CI risk dashboards. This approach recognises disaster management as intrinsic to CIP rather than an external emergency response function.

5.5 Legal and Statutory Provisions

India's regulatory architecture still lacks statutory authority over physical and interdependent systems. Section 70A of the IT Act grants NCIIPC jurisdiction only over cyber assets and excludes cross-sector audits and physical infrastructure oversight[64]. Comparative frameworks highlight the value of legal enforcement. The EU NIS2 Directive imposes penalties for non-compliance. Australia's SOCI Act mandates resilience audits. U.S. federal directives authorise inspection authority and create enforceable duties for operators [65] [66] [67].

CIPA addresses this structural gap by establishing NCIA with statutory inspection and enforcement powers, mandating multi-sector audits with compulsory annual reporting and embedding ISO and IEC 27001:2022 requirements directly into law so that they function as enforceable obligations rather than voluntary standards[68]. This shift converts resilience from recommended practice into legal compliance.

5.6 Socio-Political Governance and Capacity

Governance fragmentation continues to slow CIP maturity. No single ministry holds statutory authority, centre–state coordination remains weak, and capacity pipelines across cyber, engineering and resilience disciplines remain inadequate for national demand[69]. Comparative frameworks demonstrate the value of coherence. The United Kingdom's Critical National Infrastructure Knowledge Base institutionalises cross-sector dependency visibility, while OECD guidance highlights the need for inter-ministerial alignment and structured communication channels[70] [71].

The framework therefore prescribes NCIA as an inter-ministerial statutory authority to centralise resilience governance, centre–state compacts for shared critical sectors including energy, health and water, continuity cells across all Tier-A infrastructures to ensure institutional fallback during disruption and multidisciplinary training pipelines that combine cyber, engineering and disaster risk expertise. These measures shift India from fragmented oversight toward institutionalised resilience capacity.

5.7 Comprehensive National Security

Critical infrastructure resilience must function as a core element of national security doctrine. Resilience and readiness shape the operational foundations of sovereignty and determine how effectively states absorb and respond to hybrid aggression[72] [73]. India currently lacks statutory thresholds defining the severity of hybrid attacks, remains outside structured incident-sharing treaties and has yet to align with UN GGE cyber norms or NIST maturity benchmarks[74].

The measurable framework requires codification of hybrid attack thresholds within national security doctrine, legal embedding of CIP obligations within defence and security structures, negotiation of incident-sharing treaties with strategic partners and alignment with NATO's 2022 Strategic Concept that recognises critical infrastructure resilience as a central determinant of security[75]. By placing CIP within comprehensive national security, resilience becomes part of deterrence, continuity and sovereign endurance.

6. Synthesis: From Fragmentation to Institutionalisation

India's Critical Infrastructure Protection (CIP) framework remains fragmented. Coverage under the IT Act is partial, reporting norms remain voluntary and sectoral silos continue to ignore cascading dependencies. As argued in Towards a Critical Infrastructure Protection Programme for India: Reconceptualising Sectoral Priorities for Strategic Resilience and National Security[76], imported models such as the U.S. NIPP or the EU NIS2 cannot be adopted wholesale. Their design assumes mature federal coordination, uniform compliance capacity and strong regulatory presence, conditions that do not align with India's socio-economic landscape. Institutionalisation must therefore arise from an indigenous design grounded in the Twin Pillars, One Foundation and One Measurable Framework. The outcome is layered governance with unified structure.

6.1 The First Pillar: Critical Infrastructure Protection Act (CIPA)

CIPA functions as the legal vehicle that converts resilience from voluntary commitment into enforceable obligation. The challenge lies not in conceptual clarity but in the absence of binding authority, a gap highlighted across multiple analyses[77]. By establishing the National Critical Infrastructure Protection Authority (NCIA) with inspection powers, penalties and emergency directive capacity, CIPA places systemic resilience on a statutory footing. It mandates audits with penalties for concealment, aligning India with NIS2 and the SOCI Act[78]. It institutionalises cross-sector resilience drills every twenty-four months, linking cyber preparedness with disaster readiness[79]. It requires the creation of sector-specific ISACs under statutory supervision so intelligence exchange becomes trusted and enforceable[80]. It clarifies roles across ministries, private operators and regulators, closing accountability gaps that voluntary systems have been unable to resolve. Through these mandates, CIPA builds legal certainty, operational accountability and institutional authority.

6.2 The Second Pillar: Bharat National Resilience Index (BNRI)

Measurable standards are essential for institutionalising resilience. Responding to earlier calls for resilience indices[81], BNRI serves as both compliance mechanism and knowledge system. It assigns baseline requirements to Tier-C operators, including MFA, reporting and audits. Tier-A systems must comply with advanced mandates such as digital twins, AI anomaly detection and red teaming. BNRI introduces comparability across states and sectors, guiding prioritisation based on evidence and reducing structural inequity where capacity remains uneven[82]. Beyond national application, BNRI positions India as a reference model for the Global South. It mirrors the function NIST performs for cyber maturity, but is calibrated to federal asymmetry and differentiated development.

6.3 The Foundation: Reimagining Sectoral Priorities

The Foundation of India's CIPP rests on sectoral reprioritisation, as argued in the FINS Journal analysis[83]. Imported taxonomies prioritise energy, ICT, finance and transport, which is insufficient for India. The expanded statutory taxonomy must include logistics, water systems, agriculture, public health, judiciary, maritime infrastructure and innovation clusters. Each represents a system-of-systems vulnerability whose disruption can fracture governance continuity, economic stability and public legitimacy. Maritime infrastructure underpins Indo-Pacific strategy, judiciary systems uphold constitutional continuity and innovation ecosystems represent sovereign capability. Excluding these sectors leaves structural gaps and exposes India to hybrid disruption. Codification ensures that the protection framework reflects operational reality rather than external templates.

6.4 The One Measurable Framework: Comprehensive Protection Evaluation

BNRI becomes functional only when embedded in the measurable framework. The seven analytical perspectives described in the previous FINS paper Critical Infrastructure Protection in a Cyber-Physical World[84] become statutory benchmarks across technological, cyber-geopolitical, economic, disaster-management, statutory, governance and national security dimensions.

They include SCADA segmentation, MFA and AI anomaly detection; deterrence doctrine, ISACs and zero trust; liability clauses, blockchain validation and resilience financing; NDMA–NCIA convergence, biennial drills and hazard fusion; NCIA authority, ISO and IEC 27001 alignment with penalties; inter-ministerial authority, state compacts and continuity cells; and hybrid attack thresholds, treaty alignment and doctrinal embedding. This framework makes resilience auditable, enforceable and continuously adaptive.

6.5 Convergence into Institutionalisation

Institutionalisation emerges through the synthesis of the Twin Pillars, the Foundation and the Measurable Framework. The Foundation determines what is critical. CIPA enforces protection. BNRI measures resilience across preparedness, mitigation, response and recovery. The Measurable Framework integrates these layers into operational evaluation. Through this architecture, India closes domestic protection gaps and positions itself globally. As NATO's 2022 Strategic Concept elevated infrastructure resilience as a security priority[85], India's statutory model locates resilience within national security while offering a replicable approach for federal, resource-constrained states confronting hybrid threat environments.

7. Implementation Roadmap: Parallelising Statutory, Institutional, and Operational Efforts

Institutionalising India's Critical Infrastructure Protection Programme (CIPP) cannot unfold as a slow linear sequence. Statutory enactment cannot wait for operational readiness, and capacity-building cannot wait for parliamentary approval. India's risk environment is immediate, institutional capacity remains uneven and hybrid threats are already active. Implementation must therefore progress in parallel across law, institutions, operators and society so resilience development begins before, during and after legislation.

7.1 Statutory and Policy Layer – Government of India and Legislature

The legal layer provides enforceability. Drafting and passing the Critical Infrastructure Protection Act (CIPA) establishes definitions, sectoral obligations and enforcement authority under the National Critical Infrastructure Protection Authority (NCIA)[86]. While legislation moves through parliamentary process, executive orders can impose minimum resilience baselines such as Mean Time to Recovery (MTTR), redundancy indices and mandatory cyber-drill intervals. These interim compliance requirements ensure operators do not delay action while awaiting the final statute. CIPA must also align directly with national security doctrine. Once linked, hybrid threat protection shifts from regulatory aspiration to statutory deterrence[87]. CIP then forms part of sovereignty and defence posture rather than a technical oversight function.

7.2 Institutional and Governance Layer – NCIA, Ministries, and State Cells

Institutions convert statutory intent into operational structure. Once established, NCIA becomes the national coordination node connecting the Ministry of Home Affairs, MeitY, Ministry of Power, Ministry of Defence, Ministry of Finance and Ministry of Health. Sectoral resilience cells must be embedded within each ministry, covering energy, logistics, water, agriculture, judiciary, maritime and innovation systems and reporting to NCIA. At the state level, CIP governance structures must operate under Chief Secretaries so national standards adjust to regional realities. This reduces centre–state fragmentation and ensures authority remains centralised while operations are distributed. The structural gap that has historically hindered both disaster response and cyber incident coordination is addressed through this alignment.

7.3 Measurement and Knowledge Layer – BNRI and Research Ecosystem

BNRI represents the measurement function. As a statutory tool, it evaluates resilience across preparedness, mitigation, response and recovery while operating as a dynamic knowledge system[88]. Its implementation requires academic–industry consortia. IITs, DRDO laboratories and corporate R and D units must collaborate on digital twin platforms, AI detection grids and blockchain-enabled logistics verification. This ensures measurement evolves with threat sophistication rather than remaining static.

Mandatory reporting becomes integral across tiers. Tier-A systems submit resilience updates every six months, while Tier-B and Tier-C systems report annually. This creates a continuous reporting loop to NCIA, enabling standardisation, benchmarking and compliance auditing.

7.4 Operational Layer – Sectoral Operators and PPP Ecosystems

Operators constitute the execution core. Critical Incident Response Units (CIRUs) must be installed in Tier-A and Tier-B infrastructures including ports, aviation hubs, hospitals and power grids. These units must maintain direct escalation routes to NCIA to prevent bureaucratic delay during crises. Public-private cooperation must shift from voluntary partnership to compliance-bound engagement. PPP contracts must include enforceable resilience clauses, mandatory incident disclosure and penalty provisions for non-compliance[89]. This changes operator behaviour from discretion to obligation. Preparedness must be exercised through annual national simulation cycles integrating cyberattacks, disaster hazards and terrorism scenarios. These multi-hazard drills should involve NDMA, NCIIPC, NSG and operators across critical sectors. Only rigorous testing converts cascading risk readiness from theoretical intent into operational capability.

7.5 International and Diplomatic Layer – External Partnerships

Critical infrastructure functions within global networks and transnational supply chains, which makes a diplomatic dimension essential. Agreements must advance through QUAD, BIMSTEC and BRICS focusing on incident-sharing frameworks, cyber-resilience drills and joint protection arrangements[90] [91]. India should align with international standards including ISO and IEC 27001:2022 while mirroring NIS2 compliance benchmarks to ensure interoperability with global resilience governance. These steps enhance credibility and support reciprocal recognition of protection maturity. Infrastructure diplomacy must also evolve. India can project its CIPP architecture as part of Indo-Pacific security and South–South cooperation so CIP becomes not only a domestic strategy but also a foreign policy instrument that strengthens regional influence through resilience leadership.

7.6 Capacity and Societal Layer – Citizens, Workforce, and Civil Society

Resilience requires societal embedding. A National CIP Training Academy under NCIA should build multidisciplinary capacity pipelines that include engineers, forensic analysts, red-team specialists and emergency responders, addressing the persistent skill deficit in resilience governance. Citizen-level inclusion requires integrating digital hygiene, CI awareness and preparedness into education systems, vocational programmes and national outreach initiatives so resilience behaviour becomes a norm. Civil society must also be included. NGOs, self-help groups and community networks should be incorporated into formal outreach, particularly in rural regions where institutional coverage remains limited. This prevents resilience from becoming urban and technocratic, ensuring that the framework is socially inclusive.

7.7 Implementation as a Parallel Ecosystem

India’s roadmap must develop as a parallel ecosystem rather than a sequential rollout. Multiple layers progress together. Statutory codification advances while interim executive orders introduce baseline norms. Institutions including NCIA, state cells and sectoral units begin functioning as BNRI initiates data reporting. Private operators implement PPP-driven compliance while international partnerships provide modelling and benchmarking. Public engagement evolves concurrently, embedding legitimacy and awareness. Through this parallel model, a multi-level protection shield emerges in which statutory, institutional, operational and societal elements evolve simultaneously rather than in delayed sequence.

Conclusion

This paper advances the discourse on India's Critical Infrastructure Protection (CIP) by moving beyond fragmented cyber-focused approaches toward an integrated statutory and evaluative architecture. The framework rests on the Critical Infrastructure Protection Act (CIPA) and the Bharat National Resilience Index (BNRI), supported by one reimagined foundation of sectoral priorities and reinforced through one comprehensive measurable framework. Together they convert resilience from discretionary practice into statutory obligation across preparedness, mitigation, response and recovery.

CIPA functions as the legal backbone and BNRI operates as the measurement mechanism. This pairing closes the enforcement gap that has limited India's ability to govern cascading dependencies. The statutory pillar establishes audit authority, penalties and integrated drills, while the measurement pillar embeds quantifiable indices across Tier-A, Tier-B and Tier-C infrastructures. This linkage unites legal enforceability with empirical evaluation so that governance operates coherently across juridical, operational and technical domains[92].

The reimagined foundation expands statutory protection beyond energy, ICT, finance and transport. Logistics, agriculture, health, judiciary, maritime routes and innovation ecosystems are included because these systems shape India's hybrid vulnerability landscape. Their inclusion reflects asymmetric federal capacity, demographic pressures and threat realities rather than assumptions drawn from industrialised states[93].

The measurable framework aligns seven analytical perspectives into enforceable requirements spanning technological, cyber-geopolitical, economic, disaster-management, statutory, governance and national security dimensions. Through these standards, resilience becomes doctrine, integrating drills, inspections, liability and deterrence into law, practice and security planning. CIP becomes a continuum rather than a set of disconnected activities.

Taken together, the proposed model offers a prescriptive blueprint for institutionalising resilience. By aligning statutory authority, sectoral reprioritisation and measurable enforcement, CIP evolves into a unified national security architecture. Resilience becomes a sovereign function shaped through an India-specific criticality lens that integrates governance, economy and security into a single system of national protection and strategic endurance.

End Notes

[1] NCIIPC. About NCIIPC...]

[2] Dash, P. (2024). Towards a CIPP for India...]

[3] NCIIPC. About NCIIPC...]

[4] Ghosh, S. (2022). Chinese state-backed actors and India's power grid...]

[5] Ouyang, M. (2019). Interdependent CI system modelling...]

[6] de Jong-Chen, C., & O'Brien, K. (2017). U.S. NIPP overview...]

[7] EU. (2022). NIS2 Directive...]

[8] Critical 5. (2024). Australia's SOCI Act...]

[9] Dash, P. (2025). Towards a CIPP for India...]

[10] Simion, C. P. et al. (2013). Threat analysis for CI protection...]

[11] Dash, P. (2025). Towards a CIPP for India...]

[12] Dash, P. (2025). Towards a CIPP for India...]

[13] World Bank. (2013). Building resilience report...]

[14] Dash, P. (2021). Protecting India's CI...]

[15] Dash, P. (2024). Hybrid dimension of CI security...]

[16] Ibid...]

[17] Dash, P. (2024). Compulsions of enacting CIPA...]

[18] Critical 5. (2024). SOCI Act summary...]

[19] UNDRR. (2019). Global assessment report...]

[20] NCIIPC. About NCIIPC...]

[21] Dash, P. (2021–2024). Series on CI security and CIPA...]

[22] Dash, P. (2024). Compulsions of enacting CIPA...]

[23] Dash, P. (2024). Safeguarding India's future...]

[24] CSIS; NATO. (2022). Nord Stream sabotage analysis...]

[25] Dash, P. (2024). Why CIPA is warranted...]

[26] Petit, F. et al. (2013); EU (2022). NIS2 provisions...]

[27] Dash, P. (2024). Safeguarding India's future...]

[28] USDHS. (2009). NIPP; Critical 5 (2024). SOCI Act...]

[29] Dash, P. (2024). Hybrid dimension of CI security...]

[30] Dash, P. (2024). Why CIPA is warranted...]

[31] Dash, P. (2025). Towards a CIPP for India...]

[32] Dash, P. (2024). Hybrid dimension of CI security...]

[33] Dash, P. (2024). Why CIPA is warranted...]

[34] OECD. (2021). Regulatory frameworks and investment...]

[35] Dash, P. (2021). Protecting India's CI...]

[36] Dash, P. (2024). CIPA analyses...]

[37] Kuipers, S. (2019). Disaster collaboration studies...]

[38] Petit, F. et al. (2013). Resilience Measurement Index...]

[39] Linkov, I. et al. (2018). Resilience approaches...]

[40] Dash, P. (2025). Towards a CIPP for India...]

[41] Sun, Y. et al. (2022). AI anomaly detection...]

[42] CISA. (2023). Cybersecurity performance goals...]

[43] Critical 5. (2024). SOCI Act...]

[44] Chatterjee, A. et al. (2024). Risk-informed investments...]

[45] Dash, P. (2024). Compulsions of enacting CIPA...]

[46] ISO (2022); UNDRR (2015); NATO (2022)...]

[47] Dash, P. (2025). Towards a CIPP for India...]

[48] Ibid...]

[49] Kelic, A. et al. (2008). SCADA vulnerabilities...]

[50] Ouyang, M. (2019). Interdependency modelling...]

[51] Ghosh, S. (2022). Intrusions into India's power grid...]

[52] NCIIPC. About NCIIPC...]

[53] Proofpoint. (2022). MFA breach reduction...]

[54] Sun, H. et al. (2022). AI detection for resilience...]

[55] CISA. (2023). CPGs for CI...]

[56] Dash, P. (2024). Compulsions of enacting CIPA...]

[57] CTU. (2018). ISAC best practices...]

[58] EU. (2022). NIS2 Directive...]

[59] Critical 5. (2024). SOCI Act...]

[60] IISD. (2019). World Bank resilient infrastructure...]

[61] Singh, A. et al. (2014). Disaster and CI risk in India...]

[62] USDHS. (2009). NIPP...]

[63] UNDRR. (2015). Sendai Framework...]

[64] NCIIPC. About NCIIPC...]

[65] de Jong-Chen, C., & O'Brien, K. (2017). NIPP guidance...]

[66] EU. (2022). NIS2 Directive...]

[67] Critical 5. (2024). SOCI Act...]

[68] ISO. (2022). ISO/IEC 27001:2022...]

[69] Dash, P. (2024). Safeguarding India's future...]

[70] Critical 5. (2024). CNI Knowledge Base...]

[71] OECD. (2019). CI resilience governance...]

[72] Popovski, V. (2023). Resilience and sovereignty...]

[73] Vinson, J., & Brawley, M. (2024). Readiness studies...]

[74] Dash, P. (2024). Hybrid dimension of CI security...]

[75] NATO. (2022). Strategic Concept...]

[76] Dash, P. (2025). Towards a CIPP for India...]

[77] Dash, P. (2021–2024). CIPA necessity series...]

[78] EU (2022). NIS2; Critical 5 (2024). SOCI Act...]

[79] USDHS (2009). NIPP; UNDRR (2015). Sendai...]

[80] CTU. (2018). ISAC best practices...]

[81] Dash, P. (2025); Petit et al. (2013). Resilience Index...]

[82] Singh, A. et al. (2014); Sarkar, S. (2022). CI resilience equity...]

[83] Dash, P. (2025). Towards a CIPP for India...]

[84] Dash, P. (2025). CI protection analysis...]

[85] NATO. (2022). Strategic Concept...]

[86] Dash, P. (2024). CIPA legislative studies...]

[87] Dash, P. (2024). Hybrid dimension of CI security...]

[88] Dash, P. (2025). Towards a CIPP for India...]

[89] Dash, P. (2024). Why CIPA is warranted...]

[90] NATO. (2022). Strategic Concept...]

[91] EU. (2022). NIS2 Directive...]

[92] Dash, P. (2025); Dash, P. (2024). CI resilience analyses...]

[93] Dash, P. (2021). Protecting India’s CI...]

References

1. Capitol Technology University (CTU). (2018, November 14). The 16 sectors of critical infrastructure. https://www.captechu.edu/blog/cybersecurity-of-16-sectors-of-critical-infrastructure

2. Center for Strategic & International Studies (CSIS). (2022, September 29). Security implications of Nord Stream sabotage. https://www.csis.org/analysis/security-implications-nord-stream-sabotage

3. Chatterjee, A., Wadhawan, S., Carluccio, S., Gupta, N., Gurung, D. R., Dharani, S., & Naidoo, S. (2024, September). Accelerating risk-informed investments in climate-resilient urban infrastructure: A framework-based approach (T20 Policy Brief). Council on Energy, Environment and Water. https://www.ceew.in/publications/accelerating-risk-informed-investments-climate-resilient-urban-infrastructure-framework

4. CISA. (2023). Cross-Sector Cybersecurity Performance Goals for OT/ICS. Cybersecurity & Infrastructure Security Agency. https://www.cisa.gov/resources-tools/resources/cross-sector-cybersecurity-performance-goals

5. Critical 5. (2024). Critical Five Vision 2030: Protecting interdependent critical infrastructure systems. https://www.criticalfive.org

6. Dash, P. (2021, August 30). Protecting India’s critical infrastructure. Orissa Post. https://www.orissapost.com/protecting-indias-critical-infrastructure/

7. Dash, P. (2024, August 17). Why the Critical Infrastructure Protection Act is seriously warranted. India News Diary. https://indianewsdiary.com/why-the-critical-infrastructure-protection-act-is-seriously-warranted/#google_vignette

8. Dash, P. (2024, August 20). Safeguarding India’s future: The urgent need for a critical infrastructure protection act. The Daily Pioneer. https://www.dailypioneer.com/2024/columnists/safeguarding-india-s-future--the-urgent-need-for-a-critical-infrastructure-protection-act.html

9. Dash, P. (2024, February 8). Protecting critical infrastructure. Odisha Post. https://odishapostepaper.com/edition/4805/orissapost/page/6

10. Dash, P. (2024, November 18). Hybrid dimension of critical information infrastructure security: Why India needs a Critical Infrastructure Protection Act to attain cyber-physical resilience. Uday India. https://www.udayindia.in/news/hybrid-dimension-of-critical-information-infrastructure-security-why-india-needs-a-critical-infrastructure-protection-act-to-attain-cyber-physical-resilience

11. Dash, P. (2024, September 11). Compulsions of enacting: A “Critical Infrastructure Protection Act”. Uday India. https://www.udayindia.in/news/compulsions-of-enacting-a-critical-infrastructure-protection-act

12. Dash, P. (2025, April–June). Towards a critical infrastructure protection programme for India: Reconceptualising sectoral priorities for strategic resilience and national security. FINS Journal of Diplomacy & Strategy, 8(2). https://finsindia.org/April-June-2025-issue-2-vol-8.html

13. Dash, P. (2025, July 1). Towards a Critical Infrastructure Protection Programme for India: Reconceptualising sectoral priorities for strategic resilience and national security. FINS Journal of Diplomacy & Strategy. https://finsindia.org/towards-a-critical-infrastructure-protection-programme-for-india-dr-padmalochan-dash.html

14. de Jong-Chen, C., & O'Brien, K. (2017). The cybersecurity dilemma: U.S., EU and China approaches. Microsoft Policy Papers. https://www.microsoft.com/en-us/cybersecurity

15. European Union. (2022). Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS2 Directive). EUR-Lex. https://eur-lex.europa.eu/eli/dir/2022/2555/oj

16. Ghosh, S. (2022, March 1). Chinese hackers linked to Mumbai power outage. The Indian Express. https://indianexpress.com/article/technology/chinese-hackers-mumbai-power-outage-7783483/

17. International Institute for Sustainable Development (IISD). (2019, July 11). World Bank report illustrates benefits of resilient infrastructure. SDG Knowledge Hub. https://sdg.iisd.org/news/world-bank-report-illustrates-benefits-of-resilient-infrastructure-

18. ISO. (2022). ISO/IEC 27001:2022 – Information security, cybersecurity and privacy protection. International Organization for Standardization. https://www.iso.org/standard/82875.html

19. Kelic, A., Warren, D. E., & Phillips, L. R. (2008, September). Cyber and physical infrastructure interdependencies (SAND2008-6192, Unlimited Release). Sandia National Laboratories. https://www.osti.gov/servlets/purl/945905

20. Kuipers, S. (2019, March 11). Disaster consequences and collaboration. Risk, Hazards & Crisis in Public Policy, 10(2), 138–142. https://doi.org/10.1002/rhc3.12163

21. Linkov, I., Trump, B. D., & Fox-Lent, C. (2018, September). Resilience: Approaches to risk analysis and governance: An introduction to the IRGC resource guide on resilience. International Risk Governance Center (IRGC). https://irgc.org/wp-content/uploads/2018/09/Linkov-Trump-Fox-Lent-Resilience-Approaches-to-Risk-Analysis-and-Governance.pdf

22. NATO. (2022). Strategic Concept 2022. North Atlantic Treaty Organization. https://www.nato.int/strategic-concept

23. NCIIPC. (n.d.). National Critical Information Infrastructure Protection Centre – Mandate and responsibilities. Government of India. https://nciipc.gov.in

24. North Atlantic Council. (2022, September 29). Statement by the North Atlantic Council on the damage to the Nord Stream 1 and Nord Stream 2 pipelines [Press Release No. 129]. NATO. https://www.nato.int/cps/en/natohq/official_texts_207733.htm

25. OECD. (2021). OECD Recommendation on the Governance of Critical Risks. Organisation for Economic Co-operation and Development. https://www.oecd.org/gov/risk/recommendation-governance-critical-risks.htm

26. Organisation for Economic Co-operation and Development (OECD). (2019, April 17). Good governance for critical infrastructure resilience. OECD Publishing. https://www.oecd.org/en/publications/good-governance-for-critical-infrastructure-resilience_02f0e5a0-en.html

27. Ouyang, M. (1) (2019). Cyber-physical-social interdependencies and organizational resilience: A review of water, transportation, and cyber infrastructure systems and processes. National Science Foundation Public Access Repository. https://par.nsf.gov/servlets/purl/10167203

28. Ouyang, M. (2) (2019). Review on modeling and simulation of interdependent critical infrastructure systems. Reliability Engineering & System Safety, 121, 43–60. https://doi.org/10.1016/j.ress.2013.06.040

29. Petit, F., Bassett, G., Black, R., Buehring, W., Collins, M., Dickinson, D., Fisher, R., Haffenden, R., Huttenga, A., Klett, M., et al. (2013). Resilience Measurement Index: An Indicator of Critical Infrastructure Resilience. Argonne National Laboratory, Chicago, IL, USA.

30. Popovski, V. (2023, July 20). Critical infrastructure must be resilient… it's critical. UNDP Eurasia. https://www.undp.org/eurasia/blog/critical-infrastructure-must-be-resilientits-critical

31. Proofpoint. (n.d.). Critical infrastructure protection. https://www.proofpoint.com/uk/threat-reference/critical-infrastructure-protection-cip

32. Sarkar, D. (2022, August 18). Indian infrastructure: Leveraging past experiences for future growth. Observer Research Foundation. https://www.orfonline.org/expert-speak/indian-infrastructure

33. Simion, C. P., Bucovetchi, O., & Popescu, C. A. (2013, May). Critical infrastructures protection through threat analysis framework. Annals of the Oradea University: Fascicle of Management and Technological Engineering, XXII(1). https://www.researchgate.net/publication/307720857_CRITICAL_INFRASTRUCTURES_PROTECTION_THROUGH_THREAT_ANALYSIS_FRAMEWORK

34. Singh, A. N., Gupta, M. P., & Ojha, A. (2014). Identifying critical infrastructure sectors and their dependencies: An Indian scenario. International Journal of Critical Infrastructure Protection, 7(2), 71–85. https://doi.org/10.1016/j.ijcip.2014.04.003

35. Sun, W., Bocchini, P., & Davison, B. D. (2022). Overview of interdependency models of critical infrastructure for resilience assessment. Natural Hazards Review, 23(1), 04021058. https://www.cse.lehigh.edu/~brian/pubs/2022/naturalhazardsreview/ASCE_ReviewInterdependencyModel_V2.pdf

36. UNDRR. (2015). Sendai Framework for Disaster Risk Reduction 2015–2030. United Nations Office for Disaster Risk Reduction. https://www.undrr.org/implementing-sendai-framework/what-sendai-framework

37. United Nations Office for Disaster Risk Reduction (UNDRR). (2019, October 10). Global assessment report on disaster risk reduction 2019. UNDRR. https://gar.undrr.org

38. United States Department of Homeland Security (USDHS). (2009). Critical Infrastructure Resilience: Final Report and Recommendations. National Infrastructure Advisory Council, Washington, DC, USA. https://www.dhs.gov/xlibrary/assets/niac/niac_critical_infrastructure_resilience.pdf

39. Vinson, N., & Brawley, S. (2024, December 6). Critical infrastructure: Readiness, resilience, and security. UK Parliament POST. https://post.parliament.uk/critical-infrastructure-readiness-resilience-and-security/

40. World Bank. (2013, November). Building resilience: Integrating climate and disaster risk into development. https://www.worldbank.org/content/dam/Worldbank/document/SDN/Full_Report_Building_Resilience_Integrating_Climate_Disaster_Risk_Development.pdf

41. World Bank. (2023). Lifelines: The resilient infrastructure opportunity – Updated insights. World Bank. https://documents.worldbank.org/en/publication/documents-reports/documentdetail/775891600098079887/lifelines-the-resilient-infrastructure-opportunity

[This work has been funded by the Indian Council of Social Science Research (ICSSR), Ministry of Education, New Delhi, under the ―ICSSR Post-Doctoral Programme‖ 2019-20 on "Critical Infrastructure Protection Programme for India".]

About The Author

Dr. Padmalochan Dash, ICSSR Post-Doctoral Fellow, Central University of Gujarat.

White-Collar Terrorism: The Radicalization of Professionals and the Exploitation of Financial Infrastructure

Abstract

Purpose: This article brings together the research done on the ground and the analysis of the collected information to present a detailed study of white-collar terrorism. This is a case of the most ironic of the terrorists, the highly educated professionals who exploit their access to institutions to enable extremist violence. As part of the research, the authors read and analyzed secret case files, oversight reviews, intelligence on the financial sector, and academic literature and then combined all these into a single comprehensive framework to understand how this issue hampers the fight against terrorism most severely and in what way.

Design/Methodology/Approach: The research, which focuses on the Al-Falah University Delhi blast investigation, uses a qualitative case study methodology to create a framework for analysis via systematic literature review, sectoral vulnerability assessment, and policy framework development. It moves through different stages starting with conceptual definition, empirical profiling, pathway analysis, institutional examination, and finally, prescriptive recommendation, with each layer depending on the previous one to unfold the complexity of professional radicalization phenomena.

Findings: Essentially, one of the most revolutionary changes is the concept of white-collar terrorism, a change in which terrorist organizations intentionally hire highly qualified professionals in order to get specialized expertise instead of simply relying on marginalized operatives. These professionals use their occupational legitimacy, institutional access, and technical knowledge to exploit the vulnerabilities of the Banking, Financial Services, and Insurance (BFSI) sector. Failures in detection arise from cognitive biases that favor professional respectability, institutions being unprepared for ideologically-motivated insider threats, and fragmented intelligence architectures that are not capable of recognizing dispersed indicators.

Research Limitations/Implications: Secret limits on the gathering of classified intelligence, a detection bias that favors visible activities over those that are concealed, and ethical constraints that limit the study of the radicalization of people who are already active in this process, all of these factors limit the empirical depth. The findings, however, have an imperative to rekindle the conception of the counter-terrorism system as the one that should include educated professionals as the main sources of threat thus the need to have the cooperation between Public-Private Partnership to engage financial intelligence with the community to detect this kind of activities.

Originality/Value: This study merges the four previously isolated areas of theories of white-collar crimes, research on terrorist financing, psychology of radicalization, and analysis of institutional vulnerabilities, into one coherent framework. The suggested multi-level identification system and detailed PPP model offer practical plans to the police and intelligence agencies dealing with the hard-to-grasp existence of professional radicalization in operations.

Keywords: white-collar terrorism, professional radicalization, terrorism financing, BFSI exploitation, insider threats, public-private partnerships, financial intelligence, counter-terrorism strategy

Bottom Line Up Front (BLUF)

Terrorism has changed from only marginalized actors who commit it to a situation of the intentional recruitment of educated professionals, who then become the weaponisation of institutional access for the facilitation of extremist violence. The Al-Falah University case is an example of such a change: medical doctors took advantage of the educational institutional legitimacy and healthcare infrastructure to carry out terrorist operations. Present-day terrorist networks deliberately look for finance professionals to assist them in money laundering, IT specialists for cyber operations, engineers for creating weapons, and doctors to oversee the logistics of terrorist acts, in short, roles that need technical sophistication rather than a violent nature.

These terrorists from among the white-collar set use the "respectability shield" of professional credentials, at the same time, they exploit insider knowledge of compliance thresholds, and live their functional normalcy till the moment of operational activation, thus making conventional detection frameworks ineffective.

The existing counter-terrorism methods are inefficient because they consider the terrorists as external threats and overlook the fact that the terrorists are professionals who are internally operating, have legitimate system access, and create transaction patterns that are like routine business and therefore cannot be differentiated. The BFSI sector is severely vulnerable to such activities: radicalized bankers can manipulate KYC procedures, MSB operators can create a mix of hawala and formal banking, NPO managers can facilitate the diversion of charitable funds, and insurance agents can use legitimate products to layer illicit proceeds. The detection of such activities calls for a paradigm shift from a kinetic-focused counter-terrorism approach to an integrated financial intelligence approach, which among other things emphasizes: better employee vetting through the implementation of "Know Your Employee" standards; institutional risk assessment to uncover radicalization vulnerabilities; multi-agency data fusion to gain access to the different threat indicators that are scattered; and comprehensive Public-Private Partnership frameworks, which among other things allow for community reporting along with whistleblower protections.

If we fail to rightly conceive the notion that educated professionals might become vectors of threat and at the same time fail to put in place detection architectures that address the issues of insiders exploiting the situation, terrorist networks will keep on utilizing the financial infrastructure's legitimate operations to carry out their acts of terror, thereby not only jeopardizing security but also the economic integrity, while at the same time, conventional surveillance will remain blind to the threats that are hiding in professional respectability.

I. Introduction: Challenging the Disenfranchisement Paradigm

The revelation of a terrorist cell module involving medical doctors from Al-Falah University shook the core of the assumptions of the counter-terrorism doctrine[1]. These were operatives with advanced medical degrees, they held respected positions in institutions, and were socially integrated, traits which are contrary to the typical characteristics of terrorism as a refuge for the marginalized of society. Nevertheless, their arrest unveiled the cunning exploitation of the healthcare sector, the prestige of the institution, and the professional legitimacy to commit terrorist violence. This instance is a case of the frightening change, i.e. terrorism is turning to educated professionals more and more who in turn weaponize their occupational access instead of the disenfranchised youth who are vulnerable to ideological manipulation.

Traditional counter-terrorism frameworks rely on the assumption that poverty, political marginalization, and social exclusion are the main causes of radicalization[2]. The disenfranchisement paradigm of radicalization shapes the allocation of resources, methods of detection, and strategies for intervention that focus on economic development and social integration as measures to prevent the problem. Nevertheless, there is an increasing amount of empirical evidence which is in contradiction with this. Engineers radicalize and hence design sophisticated improvised explosive devices. Chartered accountants become radicalized and then create complex money laundering schemes. Banking professionals become radicalized and then exploit compliance systems. The medical personnel become the radicalized ones and are hence able to provide logistical support. These professionals did not radicalize due to economic hardships but rather thanks to their ideological commitment, identity crises, and psychological factors that operate even if the material situation is the same.

This article presents three interrelated arguments. Firstly, white-collar terrorism, where a terrorist act is a crime directly perpetrated or facilitated through the exploitation of professional credentials, institutional access, and technical expertise, is a distinct phenomenon that requires the development of new conceptual frameworks. Secondly, the radicalization of the educated professionals to terrorism is different radically from the one of the traditional extremists. The educated professionals get self-radicalized online in a sophisticated way, they get recruited in a targeted manner by organizations seeking specialized expertise, and they get deployed in roles that help them make technical contributions while exposing them operationally.

Third, the efficient detection of such cases requires the presence of Public-Private Partnership (PPP) bodies which should be manifest as a combined force of a more robust institutional oversight, financial intelligence capabilities, and community involvement rather than conventionally surveillance directed at kinetic threats.

Where its importance lies, is far beyond mere academic discourse. The Financial Action Task Force recorded that 69% of the territories are structurally so weak that they have a hard time investigating terrorism financing[3], partly due to the failure of recognizing the insider threats coming from credentialed professionals. Law enforcement officers have a hard time dealing with their enemies who at first glance seem like their colleagues and community leaders, the ones whose professional credentials give them a presumptive legitimacy, thus, conventional threat assessment models fail to spot them. After all, intelligence agencies aimed at spotting angry youths from ghettos who are likely to become terrorists, fail to notice successful professionals who keep up appearances of normality until the moment they are activated for operations.

This paper unfolds through ten interconnected segments that scope the matter fully and offer practical suggestions. Section II provides a comprehensive literature review that supports the theoretical framework. Section III offers the features of white-collar terrorism. Sections IV and V depict professional terrorists and their psychological mechanisms of indoctrination. Sections VI and VII discuss vulnerabilities in the BFSI sector and the failure of detection. Sections VIII and IX present multi-layered strategies and holistic PPP models. The concluding part gathers ideas for the implementation of the policy and highlights research areas for the future.

II. Literature Review: Theoretical Foundations and Empirical Gaps

The Disenfranchisement Paradigm and Emerging Contradictions

Initial terrorism research advocated mainly for structural explanations that focused on poverty, political oppression, and social marginalization as factors leading to radicalization[4]. A core concept of this model, which was prevalent in counter-terrorism research until the end of the 20th century, was that terrorists came from populations that suffered from absolute deprivation or systematic exclusion from political participation. Napoleoni's prominent study of terrorism financing was mainly based on the idea that diaspora networks and state sponsorship were the main agents through which the terrorists get their funds. These models assumed that external resources are flowing into the marginalized communities which are lack of access to formal financial systems[5]. In the same way, Basile's study of hawala networks described them as informal value transfer systems that were developed to serve the needs of the populations that were excluded from the conventional banking infrastructures[6].

On the other hand, thorough empirical studies are increasingly disputing the direct relationship between poverty and terrorism. The statistical analyses of Krueger and Malečková showed that there is no significant correlation between the poverty indicators and the participation in terrorism activities; moreover, the terrorists sometimes had better education and higher income than the average of the general population[7]. Their research, which has been repeated in many different situations, makes it necessary to have a different understanding. The Brookings Institution carried out an extensive and in-depth research that educated but unemployed or underemployed people were the ones that showed the highest risk of becoming radicalized[8]; and this, in turn, suggests that relative deprivation and not absolute poverty is what causes extremism. When the expectations of the educated individuals exceed the opportunities that are available to them, then the grievance narratives will find a way to reach them even if they are in an objectively comfortable material situation.

Radicalization Theory: Cognitive Versus Behavioral Dimensions

McCauley and Moskalenko's Two-Pyramid Model delineates the difference between cognitive radicalization (the adoption of extremist ideological frameworks) and behavioral radicalization (the violent manifestation of radical beliefs)[9]. This theoretical distinction is instrumental in grasp the professionals, who ideologically radicalize, but still function in their profession. For instance, a banker might ideologically side with the jihadist theology and watch extremist content, but still, perform his daily compliance duties in a proper manner. He is inactive until a transition of his cognitive radicalization to the behavioral one occurs due to recruitment at the organizational level or self-directed commitment.

Davies's relative deprivation theory supplies the psychological foundation for the same[10]. Revolutionary movements are not the result of absolute deprivation but of the differences between the expectations and the fulfillment, the feeling of frustration experienced when the anticipated outcomes turn out to be quite different from the reality. When Davies's theory is applied to the radicalization of professionals, it offers an explanation of how highly educated people might feel that their qualifications are undervalued, that they have reached a career plateau although they are experienced, or suffer an identity crisis despite being successful and hence become susceptible to the extremist narratives which provide existential meaning beyond the secular achievement. The anomie which defines the modern professional life, normlessness despite material success, is what creates the ideological vacuum that extremism fills.

White-Collar Crime Theory: Occupational Deviance Frameworks

Sutherland's concept of white-collar crime which was basic in nature, put the main focus on the idea that these were respectable people who commit crimes through their access to occupations in legitimate institutions[11]. This structure, which was groundbreaking when it was first introduced, went against the idea that crimes only came from the lower socioeconomic strata. Cressey's fraud triangle, which includes opportunity, rationalization, and pressure, serves as a basis for the understanding of the issue which goes far beyond just financial crimes[12]. Professionals have the opportunity due to their access to institutions, they rationalize their actions through their ideological commitment by changing the form of the criminal activity to be their religious obligation or political resistance, and they get the pressure from the operational side or from the peer group within the extremist networks.

Levi and Reuter have shown the role of financial professionals as "gatekeepers" whose knowledge is the key to the sophistication of money laundering that goes beyond simple cash smuggling[13]. Freeman has studied "terrorist financing facilitators" building elaborate corporate structures hiding the beneficial ownership and the flow of funds[14]. However, these studies merely consider the professional facilitation as of minor importance,'the criminals-for-hire' who provide services to terrorist organizations, and thus do not acknowledge credentialed insiders as the terrorist networks’ most valuable and purposely cultivated and deployed strategic assets.

Terrorism-Crime Convergence Literature

Schneider and Zeranski's convergence thesis documented blurring boundaries between terrorism and organized crime[15], noting how terrorist organizations adopt criminal enterprises (narcotics trafficking, kidnapping, extortion) for revenue generation, whereas criminal syndicates use terrorist tactics only occasionally. Nonetheless, this literature mainly discusses the funding of terrorism through crimes, ignoring the professionals in legitimate institutions who facilitate operations. Shelley's research on transnational crime networks named professional enablers, lawyers, accountants, bankers, as the main components of the critical infrastructure[16], but the field of terrorism studies is still far behind in integrating these insights systematically.

Levitt's comprehensive analysis of Hamas financing revealed the systematic exploitation of charitable networks[17], whereas Biersteker and Eckert documented the use of alternative remittance systems and informal value transfer mechanisms by terrorists[18]. There is still a lack of research that addresses the professional recruitment of terrorist groups, which is one of the most important issues that the terrorists target engineers for technical operations, finance graduates for sophisticated money laundering, medical personnel for logistics and treatment capabilities, and IT specialists for cyber operations and secure communications infrastructure. This recruitment constitutes the strategic behavior of the organization, not the opportunistic exploitation of the available resources.

Empirical Foundation: The Al-Falah Case

The Delhi blast probe is a significant case that helps to physically substantiate the concept of white-collar terrorism. The uncovering of the exploitation of an array of different institutional weaknesses by terrorists turned out to be a significant part of the investigation. One of these weaknesses was the very loose verification of the required security clearances that enabled the operatives to be in the positions at the same time they were radicalized.

Another way was the support of the one who was inside the handler facilitating the activities of the bomber through the resources of the institution, and the last was the professional or occupational status which was used as a cover to colleagues and security personnel not to suspect. Educational institutions have become the places for the radicalization of students. Secret academic study groups were the environments where the extremist ideologies were developed under the guise of scholarly inquiry, and the institution's prestige was used for operational legitimacy.

Research Gaps and Theoretical Integration Needs

Contemporary research on financing of terror shows three major drawbacks that are still not solved. First, research on terrorism financing keeps the separation between "legitimate" (operations of the financial sector) and "illegitimate" (terrorist exploitation), thus, it is underestimated how deeply terrorist networks are getting involved in formal economic systems. Second, the literature does not sufficiently address the change in the profiles of terrorist financiers, particularly the rise of financially-credentialed operatives who exploit sectoral vulnerabilities from within, rather than external infiltrators who penetrate organizational defenses. Third, enforcement-oriented studies are mostly about detection mechanisms and compliance regimes and do not give enough attention to theorizing white-collar terrorism as a different strategic threat that requires fundamentally new counter-measures, which combine financial crime investigation methodologies with national security imperatives.

The paper closes these gaps by integrating theory of white-collar crime, radicalization psychology, terrorism financing research, and institutional vulnerability analysis into one framework which sees professional radicalization as one consistent phenomenon where terrorist organizations borrow corporate crime methodologies, recruit and deploy financially literate personnel strategically, and exploit structurally vulnerable BFSI infrastructure systematically. Instead of treating sectoral abuse as merely opportunistic, the paper shows that financial sector exploitation has become central to terrorists' operational capacity in the contemporary threat landscape.

III. Conceptualizing White-Collar Terrorism

White-collar terrorism is a new and different type of crime that needs to be explained in a way that shows that it is totally different from the other related criminal activities in many ways. Here the authors of this paper consider white-collar terrorism as: terrorist action resulted from or helped by those characters who used their social recognition, professional qualifications, occupational knowledge, institutional and social access and pursued political goals by using the exploitation of the legitimate organizational infrastructure.

Our specification outlines the features of the metropolis in question along three main axes. Initially, the gender of the attackers differs from those of traditional terrorism: typically, the former are educated, professionally successful, and socially integrated. On the contrary, the latter are usually living on the edges of society, economically poor, politically excluded, or have suffered politically. Secondly, the break of influence from white-collar crime makes not give money for the reform of the poor, but rather it is the ideological commitment to the extremist causes. Thirdly, the transition from terrorist financiers to a traditional external resource flows approach with a focus on inside exploitation of institutional access that external actors cannot penetrate is a partial solution to the problem of terrorism financing.

White-collar terrorists display five characteristics that make them hazardously distinct. Professional knowledge is the main instrument of force; accountants comprehend and get around anti-money laundering regulations by structuring transactions in a way that is below detection limits without the knowledge of the officers, bankers get to know correspondent banking can be used to hide the transfer of money from one country to another thus the innocent party is the one with who the money is made, IT professionals grasp network security and establish encrypted communications infrastructure[20]. Institutional access is the main cause of transforming legitimate organizations into operational platforms; bank employees access customer accounts and compliance systems, hospital administrators control medical records and facility access, university faculty influence curriculum and student networks.

Social acceptability creates an original trust, the "respectability shield" through which professional qualifications deflect suspicion; chartered accountants setting up offshore companies look like conducting tax planning, doctors making trips internationally suggest professional mobility rather than operational coordination. Besides that, financial literacy takes the act of terrorism to a whole new level, which is quite sophisticated and unrecognizable from the legitimate industrial ones.

The point at which the terrorists keep everything outwardly normal until they strike might be their most lethal attribute. For instance, professionals through effective compartmentalization may not be able to disclose to their families, colleagues, and communities that they have split ideologies and have even drifted. These features, when mixed, create exceptional advantages for terrorist groups. They can make an otherwise illegal fund look like normal through totally routine transactions. Through the use of certain core banking systems, compliance databases, and customer data, they can execute their attacks in a very surgical way. They can surpass control if they follow insider knowledge closely and they are aware of the exact trades which will lead to scare someone off so they will not report the illegal moves they made.

One point of the credential professionals' ability is that they can indoctrinate or even recruit the same level of people internally within institutions thereby creating a pool which is capable of exploiting organizational oversight in the structures. With the feature of detection being delayed which is typical of insider threats, the period of time for their operations is prolonged up until the moment of finding out, thus their activities usually come to an end prior to a police investigation after which law enforcement usually figures out funding behind attacks[21].

IV. Profiles and Pathways: The Accomplished Radical

White-collar terrorists are often people who have achieved great success in their respective fields and are quite the contrary of what one might expect - those who have failed and gone down this path. For example, engineers with advanced degrees are responsible for designing sophisticated weapons systems. MBAs create the structure of business ventures that look legitimate on the surface but are, in fact, operational fronts. Medical doctors offer their expertise in healthcare to the logistics department. Lawyers use their knowledge of legal systems to protect the organization's assets. Accountants keep track of financial statements that are used to legitimize the flow of illegal money[22]. Evidence from all over the world confirms this trend: the 2006 transatlantic aircraft plot mostly involved pharmacy students and professionals[23], several ISIS operatives had engineering degrees from highly respected universities, and financial analysis of al-Qaeda uncovered the deliberate recruitment of finance professionals to gain expertise in money laundering[24].

One needs to go beyond the economic frameworks in order to understand the motivations of white-collar terrorists. According to Sageman's research on jihad networks around the world, the main source of the participants was the middle class and they were mostly radicalized not through peer groups but through economic hardships[25]. On the one hand, ideological commitment, identity crises, and psychological factors are the engines behind the process of radicalization; on the other hand, these concepts still remain a mystery to most people. Those who are well-educated have a greater political awareness and this very fact makes them identify the suffering of Muslim communities all over the world as the common problem requiring immediate action. Success in the professional world cannot provide existential meaning; some individuals feel anomie even though they have a successful career. What extremist ideologies do is to provide one with a set of moral values, a sense of purpose, and the feeling of being a part of a community which is lacking in the secular professional world.

The dynamics of radicalization were changed to a large extent by digital platforms, which now make it possible to take one's ideological journey self-directed and without the need to physically meet an extremist. Users of YouTube are led by its recommendation algorithms from mainstream Islamic content to progressively radical material. Telegram channels are full of extremism content which comes with a pseudo-intellectual veneer. Dark web forums are the places where one can find the most detailed operational guidance[26]. Professionals with a good educational background are more capable of conducting extensive research and thus, they can be more deeply involved in the study of extremist literature, online fatwas, and ideological texts which members of less literate groups are not able to access.

The ability to think critically, instead of being a shield against radicalization, allows one to comprehend complex theological and political frameworks and apparently, this is what a number of people interpret as providing scholarly legitimacy to violence.

Terrorist organizations specifically look for experts in their targeted recruitments. There student groups on university campuses where radical ideas are exchanged under the guise of cultural or religious identity. The case of Al-Falah is a perfect example of how educational institutions can become recruitment nodes, as in inside the house of Dr. Muzammil Shakeel Ganai[27]. Sometimes a few religious institutions might have preachers who are propagating extreme interpretations of the religion. Charitable organizations that operate in conflict zones are a perfect cover for the networking of extremists; professionals who are volunteering, doctors who are providing medical aid, accountants who are managing finances, engineers who are building the infrastructures, can come across operatives who are there to assess their suitability for getting more deeply involved[28]. One's professional networks such as LinkedIn and industry conferences can also turn out to be recruitment venues where gradually after trust has been established through professional discussions, the ideological content gets introduced.

Role-specific radicalization is a clear indication of the improvement in skills level of terrorist organizations. They attract financial specialists to engage in money laundering activities, cyber operatives to make communication secure, propaganda designers to create content that is not only attractive but also convincing, and medical personnel to take care of treatment as well as logistics. These professionals do not necessarily need to have a violent nature; just having the technical skill is enough. The organizations are quite intentional in how they deploy such professionals in locations where their skills have maximum impact but at the same time their personal weaknesses minimize the risk of them being able to compromise the operation.

V. Sectoral Vulnerabilities and Systemic Blind Spots

The BFSI sector is full of different problems when professionals become radicalized. For example, the bank employees who are in charge of customer onboarding create fake accounts with forged documents, re-activate old accounts without going through the verification process and hence, create pathways for terrorism financing[29]. Treasury and remittance staff perform international transfers through banks that do not have strong oversight in order to avoid being detected. Trade finance departments open letters of credit for fake shipments, and fully document transactions for non-existent goods in order to transfer value abroad[30]. Loan officers provide financing to shell companies; after the money has been given, the loans will be defaulted on while the funds are gradually disguised abroad.

MSBs are even more vulnerable to radicalization because of less stringent regulations. A radicalized MSB operator can connect hawala networks with the formal banking sector to turn an informal transfer into a wire transfer, thus gaining the confidentiality of hawala and the legitimacy of the bank[31]. At the same time, cash transactions taking place outside the banking system can be used to hide illicit money in an already large volume of legitimate transactions. In the early stages, fintech businesses may forego compliance for the sake of growth; A founder who has been radicalized may decide to incorporate features that facilitate illicit activities in the platform, for example by allowing minimal KYC, instant onboarding, high limits, and thus creating exploitation platforms during vulnerability windows before regulatory scrutiny intensifies[32].

NPOs offer an entirely different set of opportunities for exploitation. Financial managers can divert money from the charity account under the disguise of humanitarian work by using fake invoicing, inflated costing, and phantom projects[33]. Organizations that collect zakat can use this money to support extremist causes. Some NPOs are purely money laundering vehicles, i.e., fake charities that do not conduct any real activities but facilitate illegal fund transfers through their accounts, while their professional management helps them to avoid scrutiny.

Universities turn into environments for radicalization as academic departments host ideological debates which spread radical ideas[34]. Hospitals, on the other hand, can provide operational benefits, i.e. legitimate reasons for presence, medical supply access, the capacity to treat the injured operative without the need for reporting and also the creation of false medical documentation. Research institutions that work with dual-use technologies can be a source of proliferation risk if the insiders radicalize.

Systemic failures to a large extent white-collar terrorist operation despite sophisticated counter-terrorism infrastructure. The professional status is the main reason for presumptive trustworthiness, the "respectability shield" working unconsciously through cognitive heuristics where one’s credentials are taken as a sign of safety[35]. Intelligence analysts, specifically trained to recognize the radicalization of marginalized youth, are likely to overlook that of successful professionals. There is a cognitive dissonance between professional and terrorist roles, which causes the dissonance to be dismissed rather than investigated.

Institutional failures aggravate the problem of insufficient detection. The Al-Falah case showed that there were not only various lapses in the process of verifying credentials but also an absence of the monitoring of institutional integrity. The BFSI human resources, compliance officers, and management personnel who get fraud detection training through various programs also receive practically no training on identifying indicators of radicalization. FIUs, police, and regulatory bodies work with only a small fraction of the information that they could share between themselves; also, threat indicators that are scattered across various institutions are not combined to form actionable intelligence.

Love and ethical dilemmas result in detection-related paralysis. Employers are restricted when it comes to asking potential workers about their religious beliefs or ideological views during the interview process. The likelihood of discrimination against certain groups is heightened if screening of employees is further tightened. Constant behavioral monitoring may cause workers to feel that they are under surveillance. If the focus of counter-terrorism moves to educated professionals, especially from Muslim communities, then this may lead to the stigmatization of demographic groups. The existence of such tension makes organizations hesitant to implement detection measures, as they are afraid that doing so will result in being accused of bias.

The issue of them functioning normally until they get activated is, perhaps, the biggest one. Professionals are able to separate different aspects of their lives, thus they can be competent at work while at the same time having radical ideologies in their minds. Behavioral patterns, in most cases, are revealed outside of the workplace and in the private domain such as home internet usage, weekend study groups, evening religious gatherings, and so forth, thus, they are invisible to workplace observation. AML systems are rule-based and thus are good at catching crude money laundering through transaction monitoring but they have a hard time when it comes to sophisticated insider manipulation[36]. Professionals who have been radicalized organize their dealings in such a way that the amounts are below the thresholds, they transfer money from one place to another through non-sanctioned regions, and they manufacture documents that look like they come from legitimate businesses without the knowledge of these institutions, which lack conceptual frameworks and detection methodologies for ideologically motivated insider threats operating on different logic than financially motivated threats.

VI. Multi-Layered Detection and Public-Private Partnership Frameworks

Combating white-collar terrorism needs broad-ranging structures that function at micro (individual), meso (institutional), and macro (systemic) levels. Controls at the micro-level are done through more effective employee screening in which, besides a criminal background check, a pre-employment assessment is carried out to look at factors like social media (analysis is done only with consent), references (questions should be asked about extremism in the place of work), and structured interview techniques (judgment is evaluated). It is necessary to periodically carry out a reinvestigation of security-cleared positions. Behavioral continuous monitoring, through the adoption of privacy safeguards, is the best method to detect signs of radicalization, e.g., ideological rigidity, expressed support for terrorist organizations, recruitment attempts, or unauthorized system access. Insider threat detection tools monitoring an individual's behavior, login patterns, data access, and communication can be a source of great help in detecting the malicious intents of perpetrators of the abnormal activities.

The meso-level controls carry out the management of institutional risks. Banks put into practice risk-based monitoring systems where branches and departments are assigned risk scores depending on their geographic location, customer demographics, transaction patterns, employee turnover, and previous violations[37]. The most vulnerable units get increased supervision which also includes a more frequent audit.

Besides scheduled audits, the random compliance audits serve to unveil the possible manipulations of the audited entities; managers, who have been radicalized, get prepared for those announced audits but find it hard to hide the irregularities during unannounced reviews. The proactive anomaly review mainly focuses on the examination of specific functions' transactions, such as those of treasury, trade finance, and wire transfers, thereby allowing the identification of different patterns that are inconsistent with business rationales.

If we look at the macro-level, there has to be a coordination of multi-agency. Sharing platforms of integrated data which link banks, FIU, NIA, ATS, ED, CBI, and sectoral regulators are allowing information exchange in real-time[38]. Agencies that are in charge receive the news immediately when banks submit the suspicious activity reports related to the behavior of employees. Cross-sectoral intelligence fusion centers are places where financial analysts, law enforcement investigators, and counter-terrorism specialists physically meet and work together on finding the patterns that are going beyond the entities and sub-figures that are not aware of this. Moreover, the regulatory coordination that exists between financial regulators, educational accreditation bodies, professional licensing authorities, and law enforcement can facilitate the terrorism indicator referrals in a very smooth way.

The most effective detection method is a complete P-P-P (Public-Private Partnerships) framework that combines public awareness, institutional knowledge, and government intelligence capabilities. There are three groups that have the most critical information but lack the communication mechanisms, i.e. the general public who observe suspicious behavior but do not have trusted reporting channels, employees of institutions who see the radicalization of a colleague but do not have clear paths for the escalation to protect whistleblowers, and government agencies that have pieces of intelligence which make sense only when they are combined with observations from the ground[39].

It is a National Centralized Anonymous Terror Finance Reporting Portal open to the public, BFSI employees, NGO staff, educational personnel, and healthcare workers that offers secure and encrypted submission channels which ensure anonymity. The portal allows for reporting in the following categories, i.e. suspicious financial transactions, observed radicalization behavior, concerns about charitable organizations, security lapses in institutions, and unusual customer patterns. The severity, credibility, and urgency of the reports are automatically assessed by the triage. AI-powered systems also help find the submissions that support the existing intelligence, highlight the most important reports for quick human review, and identify the non-relevant reports.

An all-inclusive “Terror Finance Whistleblower Protection Act” ensures in good faith reports absolute immunity from any civil or criminal liabilities even if the report turns out to be false. The employers are warned of heavy fines in case they retaliate against the employee who reports[40]. Whistleblower secrecy is protected by law except in a case where the prosecution is absolutely necessary. There is also a financial incentive similar to the IRS whistleblower provisions that offer some financial rewards to the persons who provide information that leads to successful prosecutions or the prevention of attacks[41].

Different sectors have their own reporting nodes which provide guidance that is suitable for each sector. For instance, banking sector suspicious employee behavior desks, MSB AML red-flag hotlines, university radicalization risk cells, and healthcare professional integrity monitoring mechanisms are all there to address the concerns specific to their sectors. The Al-Falah case exemplifies the prioritization of the university sector vulnerability. High-severity reports are automatically sent to the NIA and the respective state ATS with a financial intelligence unit (FIU) assessment happening at the same time. The international coordination via Interpol, FATF, and bilateral intelligence sharing is there to facilitate the quick response to the issues that are of a transnational nature.

The community involvement is based on the public understanding of the terrorism financing indicators without the public discriminating against certain groups of people. Public awareness campaigns disclose how terrorism is financed, how to report legitimate concerns as opposed to discriminatory profiling, and how to access the reporting mechanisms. Professional training programs for BFSI employees, healthcare workers, and educators are aimed at enabling the participants to recognize radicalization, know the proper reporting procedures, and be aware of the legal protections.

Education through curriculum also helps to develop critical thinking when faced with extremist narratives, digital literacy enabling one to recognize online radicalization, and civic responsibility as a means of community security[42].

VII. Policy Recommendations and Research Imperatives

Mandatory white-collar radicalization risk assessments entail that all financial institutions, MSBs, NPOs receiving foreign contributions, and professional licensing bodies carry out annual evaluations of their institutional vulnerabilities, the adequacy of employee screening, effectiveness of detection mechanisms, and incident response preparedness. Risk-based regulatory oversight that is exercised through the allocation of examination resources is based on the assessed terrorist financing risk and not on uniform schedules.

The inclusion of employee vetting in AML/CFT effectively extends KYC principles to employees in sensitive positions through "Know Your Employee" standards. Comprehensive background investigations now also involve social media analysis and screening for ideological extremism for those with access to the system, transaction authority, or customer data. In order to avoid discriminatory profiling, the vetting process concentrates more on the behavioral indicators and support of violence rather than on the religious or political beliefs of a person. Oversight boards that are independent from the process and review procedures protecting civil liberties are in place.

The enhancement of the Foreign Contribution Regulation Act that governs foreign funds to Indian NGOs includes the provision for real-time reporting for high-risk organizations thus enabling authorities to monitor activities as they happen[43]. Beneficial ownership transparency requires that the non-profit sector discloses its control structures. Programmatic verification is the process through which an independent entity verifies that the charitable programs are actually being implemented by means of the site visits and interviews with the beneficiaries thereby ensuring that there are no shell charities that are simply acting as channels for funds to terrorism.

National databases that combine information about individuals, groups, and entities connected to extremism become the only sources against which people are screened. Financial institutions screen their customers, employees, and partners automatically; when a match is found, an enhanced due diligence procedure is initiated. Due process protections are in place to secure high standards of evidence, with mechanisms for appeal and independent judicial review.

Community awareness campaigns modify "See Something, Say Something" for the terrorism financing context, thereby informing communities so that they can recognize the financial side without promoting discrimination. Community-based interventions help the organizations that serve the vulnerable develop programs for intervention, counseling, mentoring, family engagement before the behavior reaches the level of criminality[44]. Professional associations include counter-radicalization in their ethics frameworks; codes of ethics explicitly prohibit facilitating terrorism, and disciplinary procedures are established for violations.

The next generation of research imperatives comprises longitudinal studies following the trajectories of professional radicalization thereby clarifying early signs and intervention possibilities. Comparative effectiveness research evaluating detection methods has the potential to be an efficient resource for answering the questions: Do the enhanced screening mechanisms actually detect radicalization? Are insider threat technologies as effective as human observers? Sectoral vulnerability assessments that look at industries beyond BFSI, healthcare, education, and technology, critical infrastructure will be able to provide sector-specific guidance. Research on the international level comparing different countries to find those that effectively fight white-collar terrorism is able to point to the best practices. The exploration of the role of technology as a radicalization enabler and a detection tool is necessary: In what way do social media algorithms facilitate radicalization? Is artificial intelligence capable of identifying radicalization reliably? What technologies that preserve privacy allow effective monitoring without mass surveillance[45]?

VIII. Conclusion: The Age of White-Collar Counter-Terrorism

White-collar terrorism is a major change from the concept where the evolution of fundamental understanding is that terrorist networks intentionally hire professionals with qualifications to provide specialized expertise instead of using marginalized operatives. The Al-Falah University scandal is an example of educational research institutions becoming nodes of the radicalization process where the professional qualifications serve as the operational cover.

An in-depth study of the BFSI sector's vulnerabilities reveals a pattern of bank insider manipulation for compliance, the blending of MSBs' hawala with traditional banking, misappropriation of charitable funds in the NPO sector, layering in the insurance industry, and securities round-tripping operations are all ongoing because the detection frameworks are designed for external threats whereas insiders exploit legitimate access without raising alarms.

Radicalization routes to well-educated professionals, individual radicalization via high-quality online content, highly selective organizational recruitment for specific expertise, religious network transformation into tight extremist cells, and the utilization of role-specific skills are all points on a different map compared to the traditional ones. The protective cloak of respect conferred by professional status, failures of institutional detection, limitations of employee screening imposed by the law, and the continuation of the normal functions until the activation moment make white-collar terrorists almost invisible to the eyes of conventional counter-terrorism structures.

Combating such a menace entails a shift in paradigms from a primarily kinetic-aware counter-terrorism strategy to a combination of integrated measures involving financial intelligence, regulatory oversight, institutional resilience, and community engagement. Financial intelligence is required to be on the same level as traditional intelligence disciplines. Tracking the money trail causes the exposure of the networks, the identification of the facilitators, and the enabling of the disruption by the authorities before the operations take place[46]. The regulation of the integration process changes the local, fragmented, and disjointed efforts into a comprehensive strategy. Community participation through PPP frameworks that facilitate reliable reporting channels, providing legal protections, and feedback mechanisms assists in the transformation of passive bystanders into active security partners, thus completing the circle.

The major feature of enhanced detection ought to be the upholding of people's fundamental rights. The procedures for screening, monitoring, and reporting that are in place should direct the efforts towards identifying behavioral changes and the support for violent actions that are clearly expressed, rather than focusing on the demographic characters, religious beliefs, or political opinions of the persons involved. To safeguard the community from discriminatory execution of security measures while at the same time, ensuring the efficiency of these measures, there should be independent oversight, judicial review, and a sound due process mechanism in place.

The advent of white-collar terrorism puts the basic security assumptions under question. The enemies might not have the appearance of enemies; rather they may look like colleagues, clients, and community leaders. This fact imposes the demand for a discreet and uncomfortable acknowledgment that professional achievement, education, and social integration do not guarantee the immunity of one from radicalization. On the contrary, these very features might make these persons more attractive to terrorist groups as they look for individuals with specialized knowledge and skills. However, the realization of this fact should not lead to the generalization that all professionals or specific demographic groups are to be distrusted. The overwhelming majority pose no danger to security and are, on the contrary, valuable associates in the fight against terrorism at the level of communities and institutions.

White-collar terrorism epitomizes the fusion of financial acumen with the desire to cause harm by a violent extremist. Tackling this menace calls for a similar convergence of capabilities - intelligence agencies collaborating with financial regulators, law enforcement working with private institutions, communities communicating with governments, and researchers crossing disciplinary boundaries. The intricateness of the contemporary terrorism financing network calls for an equally intricate and coordinated response. The stakes here are way beyond merely preventing individual attacks. When terrorists exploit the financial infrastructure designed to support their activities, they not only weaken the system, but also risk shaking public trust and causing economic instability.

Therefore, apart from security imperatives, preserving the financial system integrity against terrorism exploitation is also an economic imperative.

Eliminating white-collar terrorism necessitates a constant effort despite the difficulty in locating the perpetrators and the complexity of the intervention. Unlike physical threats, financial facilitation does not leave any visible signs of damage until the attacks are carried out. Hence, measuring the success of the prevention efforts is almost impossible because it results in 'nothing' happening, which in turn makes it hard to justify the sustained allocation of resources. However, the consequence of allowing people with the right knowledge to weaponize their institutional access without being detected is the threat of dire outcomes. The suggested framework serves as a starting point: mandatory risk assessments, upgraded employee vetting, better charitable oversight, integrated databases, and thorough PPP reporting mechanisms pave the way for hitherto non-existent detection architecture. The actualization of this vision demands legislative action, regulatory reform, institutional investment, and cultural change.

The Al-Falah case and innumerable other instances highlight the situation's urgency. White-collar terrorism is not a concern of the future, rather, it is a reality presently. Professionals with the required knowledge are the ones who are currently most responsible for the facilitation of terrorism financing, logistics, and operations, of whom some might be unaware, as they are being exploited by manipulative individuals who are cunning; on the other hand, some are knowingly, as their ideological commitment is stronger than their professional ethics. Detection and intervention are the first steps for both types. As terrorism evolves into a more distributed, technologically advanced, and deeply embedded in legitimate infrastructure type of activity, so should counter-terrorism evolve. Counter-terrorism in the era of white-collar terrorism should be of the same kind: financially savvy, institutionally integrated, community-engaged, and understanding that educated professionals can either be the greatest security assets or the most dangerous security threats. The challenge of this era in counter-terrorism is to establish systems which not only help to identify those professionals but also foster security tactics and strategies that leverage these professionals as security assets rather than threats.

Endnotes

1. "Delhi Blast: Jaish-e-Mohammed Module Busted, Doctors from Al-Falah University Arrested," India Today, May 2024.
2. John Horgan, The Psychology of Terrorism (London: Routledge, 2014), 45-67.
3. Financial Action Task Force, Fourth Round Mutual Evaluation Reports: Summary Analysis (Paris: FATF, 2025), 14-17.
4. Martha Crenshaw, "The Causes of Terrorism," Comparative Politics 13, no. 4 (1981): 379-399.
5. Loretta Napoleoni, Modern Jihad: Tracing the Dollars Behind the Terror Networks (London: Pluto Press, 2003), 45-67.
6. Mark Basile, "Going to the Source: Why Al Qaeda's Financial Network Is Likely to Withstand the Current War on Terrorist Financing," Studies in Conflict and Terrorism 27, no. 3 (2004): 169-185.
7. Alan B. Krueger and Jitka Malečková, "Education, Poverty and Terrorism: Is There a Causal Connection?" Journal of Economic Perspectives 17, no. 4 (2003): 119-144.
8. Brookings Institution, "Education, Employment and Radicalization: Findings from Field Research" (Washington: Brookings, 2021), 28-45.
9. Clark McCauley and Sophia Moskalenko, "Mechanisms of Political Radicalization: Pathways Toward Terrorism," Terrorism and Political Violence 20, no. 3 (2008): 415-433.

10. James C. Davies, "Toward a Theory of Revolution," American Sociological Review 27, no. 1 (1962): 5-19.

11. Edwin H. Sutherland, White Collar Crime: The Uncut Version (New Haven: Yale University Press, 1983), 7.

12. Donald R. Cressey, Other People's Money: A Study in the Social Psychology of Embezzlement (Glencoe: Free Press, 1953), 30-33.

13. Michael Levi and Peter Reuter, "Money Laundering," Crime and Justice 34, no. 1 (2006): 289-375.

14. Michael Freeman, "The Sources of Terrorist Financing: Theory and Typology," Studies in Conflict and Terrorism 34, no. 6 (2011): 461-475.

15. Friedrich Schneider and Ursula Zeranski, "The Relationship Between Terrorism and Organized Crime," in Terrorism and International Crime, ed. Hans-Jörg Albrecht et al. (Berlin: Duncker & Humblot, 2011), 89-107.

16. Louise I. Shelley, John Picarelli, and Chris Corpora, "Global Crime Inc.," in Beyond Sovereignty: Issues for a Global Agenda, ed. Maryann K. Cusimano (Boston: Bedford/St. Martin's, 2003), 143-166.

17. Matthew Levitt, Hamas: Politics, Charity, and Terrorism in the Service of Jihad (New Haven: Yale University Press, 2006), 112-145.

18. Thomas J. Biersteker and Sue E. Eckert, eds., Countering the Financing of Terrorism (London: Routledge, 2008), 134-156.

19. "Al-Falah University Terror Module: Inside the Medical Professional Network," Indian Express, June 2024.

20. Frank G. Madsen, Transnational Organized Crime (London: Routledge, 2009), 145-167.

21. Marc Sageman, "The Stagnation in Terrorism Research," Terrorism and Political Violence 26, no. 4 (2014): 565-580.

22. David C. Rapoport, "The Four Waves of Modern Terrorism," in Attacking Terrorism: Elements of a Grand Strategy, ed. Audrey Kurth Cronin and James M. Ludes (Washington: Georgetown University Press, 2004), 46-73.

23. "Transatlantic Aircraft Plot: The Educated Extremists," BBC News, September 2008.

24. Jimmy Gurulé, Unfunding Terror: The Legal Response to the Financing of Global Terrorism (Cheltenham: Edward Elgar, 2008), 67-89.

25. Marc Sageman, Understanding Terror Networks (Philadelphia: University of Pennsylvania Press, 2004), 61-90.

26. Maura Conway, "Determining the Role of the Internet in Violent Extremism and Terrorism: Six Suggestions for Progressing Research," Studies in Conflict and Terrorism 40, no. 1 (2017): 77-98.

27. "Al-Falah University Terror Module." Abhay Parashar, Abhay. n.d. “White Collar Terror: New Picture Shows Delhi Suicide Bomber Umar in Doctor’s Coat.” Edited by Ashish Verma. https://www.indiatvnews.com/news/india/delhi-blast-white-collar-terror-new-picture-shows-delhi-suicide-bomber-umar-in-doctor-s-coat-2025-11-15-1017592.

28. Matthew Levitt, "Hamas from Cradle to Grave," Middle East Quarterly 11, no. 1 (2004): 3-15.

29. John A. Cassara, Hide and Seek: Intelligence, Law Enforcement, and the Stalled War on Terrorist Finance (Washington: Potomac Books, 2006), 89-112.

30. John A. Cassara, Trade-Based Money Laundering: The Next Frontier in International Money Laundering Enforcement (Hoboken: Wiley, 2016), 78-102.

31. Mohammed El-Qorchi, Samuel Munzele Maimbo, and John F. Wilson, Informal Funds Transfer Systems: An Analysis of the Hawala System (Washington: International Monetary Fund, 2003), 12-28.

32. Ross S. Delston and Stephen C. Walls, "Reaching Beyond Banks: How to Target Trade-Based Money Laundering and Terrorist Financing Outside the Financial Sector," Case Western Reserve Journal of International Law 41, no. 1 (2009): 85-142.

33. Nikos Passas, "Informal Value Transfer Systems and Criminal Organizations: A Study into So-Called Underground Banking Networks," report for the Dutch Ministry of Justice (The Hague: WODC, 1999), 23-45.

34. "University Radicalization: The Academic Pipeline to Extremism," Intelligence and National Security 29, no. 3 (2014): 498-520.

35. Daniel Kahneman, Thinking, Fast and Slow (New York: Farrar, Straus and Giroux, 2011), 199-217.

36. Brigitte Unger and John Walker, "Measuring Global Money Laundering: The Walker Gravity Model," Review of Law and Economics 5, no. 2 (2009): 821-853.

37. Peter Reuter and Edwin M. Truman, Chasing Dirty Money: The Fight Against Money Laundering (Washington: Peterson Institute for International Economics, 2004), 112-134.

38. Financial Crimes Enforcement Network, The SAR Activity Review: Trends, Tips & Issues, Issue 19 (Washington: FinCEN, 2011), 34-52.

39. START Consortium, "Public-Private Partnerships in Countering Violent Extremism: Field Principles and Best Practices" (College Park: University of Maryland, 2018), 12-45.

40. Sue E. Eckert, "The US Regulatory Approach to Terrorist Financing," in Terrorismusfinanzierung, ed. Ulrich Sieber and Karl von der Heydt (Berlin: Duncker & Humblot, 2004), 211-234.

41. William F. Wechsler, "Follow the Money," Foreign Affairs 80, no. 4 (2001): 40-57.

42. UNESCO, "Education for Justice: Counter-Terrorism Module Series" (Paris: UNESCO, 2020), 23-56.

43. Government of India, Ministry of Home Affairs, "Foreign Contribution (Regulation) Act, 2010: Implementation Guidelines" (New Delhi: MHA, 2020).

44. Daniel Koehler, Understanding Deradicalization: Methods, Tools and Programs for Countering Violent Extremism (London: Routledge, 2017), 78-104.

45. Jonathan M. Winer and Trifin J. Roule, "Fighting Terrorist Finance," Survival 44, no. 3 (2002): 87-104.

46. R.T. Naylor, Wages of Crime: Black Markets, Illegal Finance, and the Underworld Economy (Ithaca: Cornell University Press, 2002), 234-256.

About The Author:

Shri. Vipul Tamhane is an anti-money Laundering and combating terrorist financing specialist and provides legal and commercial advice to businesses, governments, and law enforcement organisations. He is a visiting faculty member at Pune University's Department of Defence and Strategic Studies. He is the Founder and Editor-in-Chief of Diplomacy Direct, a public interest Think Tank (and YouTube Channel) based in India that deals with topics on counter terrorism, international relations and geopolitics.

Emerging Biological Warfare Threats in the Era of Synthetic Biology and Genetic Engineering: Implications for India’s National Security

Abstract

The changing dynamics of warfare today has been a vulnerable matter of concern. The rapid advancements in technology such as synthetic biology and genetic engineering is changing the global landscape. Use of AI enables design, modification and production of novel pathogens. Even though biotechnology holds immense promises, it’s dual use also proposes potential threats by producing more antimicrobial resistant pathogens as well as the complete new form of deadliest viruses using synthetic biotechnology. This poses significant national biosecurity concerns. This paper examines how synthetic biology and genetic engineering with the addition of AI concerning the development of potential bioweapons. This paper also analyses current global norms and India’s capabilities, vulnerabilities and technological infrastructure that could be exploited in a high-impact biological incident along with policy framework suggestions which aim at strengthening national biodefence. In doing so, it underscores the urgent need for India to modernise its biosecurity architecture to safeguard its public health, economic stability and national security in the age of advanced biotechnology.

Key Words: Biotechnology, Synthetic Biology, Genetic Engineering, Global Biosecurity, Bioweapons

Overview of Genetic Engineering and Synthetic Biology

Genetic engineering and synthetic biology represent the most transformative development in the life sciences which enables precise manipulation, design and accurate construction of biological systems. While these technologies have generated significant benefits in medicine, agriculture and industry, they also possess significant threat due to their dual use for the development of potential bioweapons which leads to emergence of national biosecurity concerns.

Genetic Engineering refers to the deliberate modification of an organism's genetic material using biotechnological tools to alter specific traits or functions. Traditional techniques involved recombinant DNA technology, where genes from one organism were inserted into another to express desired characteristics. Over time, advancements such as site-directed mutagenesis[i] and, more recently, CRISPR-Cas systems have made genetic modification faster, cheaper, and far more precise. These developments allow scientists to edit genes with high accuracy, raising both the therapeutic potential and the risk of misuse.

Synthetic biology extends beyond genetic engineering by aiming to design and construct new biological components, pathways, or entire organisms that may not exist in nature. It applies engineering principles such as standardization, modularity, and predictability to biology. Synthetic biology enables the de novo synthesis of genetic sequences, redesign of microbial genomes, and creation of novel biological functions. The convergence of synthetic biology with artificial intelligence, automation, and high-throughput DNA synthesis has accelerated innovation while simultaneously lowering barriers to entry. (National Human Genome Research Institute, 2019)

The dual-use nature of both fields lies in the fact that the same tools used for beneficial purposes such as vaccine development, disease diagnostics, and sustainable bio-manufacturing can also be repurposed to enhance pathogenicity, transmissibility, or resistance to medical countermeasures. As access to genetic engineering tools and synthetic biology platforms expands globally, the distinction between legitimate research and potential misuse becomes increasingly difficult to regulate.

In the context of biological warfare, these technologies have altered the threat landscape by enabling the possibility of engineered or modified biological agents that may evade traditional detection and response mechanisms. Consequently, genetic engineering and synthetic biology now occupy a central position in contemporary biosecurity and biodefense discourse, necessitating robust governance, ethical oversight, and international cooperation particularly for countries like India that are rapidly expanding their biotechnology capabilities.

Applications of These Technologies in the Development of Potential Biological Weapons

As mentioned earlier, Genetic Engineering and Synthetic Biology is actually developed for beneficial purposes like in medicine, agriculture and industry, but their significant dual use risk makes us worried about the development of novel bioweapons. New emerging technologies lower the technical barriers, increase precision and expand the range of biological agents that could be deliberately manipulated for hostile purposes.

Genetic Modification of Existing Pathogens- This is one of the major areas of concern as, advances in gene editing allows the alterations that may enhance the virulence, transmissibility, environmental stability and resistance to medical countermeasures. Such modifications could undermine established public health defences, including vaccines and therapeutics thereby, complicating detection, diagnosis and responses. Many labs conduct gain of function[ii] research. The idea is to study how dangerous viruses evolve so that the vaccines and defenses can be prepared.

De Novo Synthesis of Biological Agents- The generation of complete novel viruses is now possible by synthetic biotechnology. This technology eliminates access to naturally occurring pathogens. This technology enables the chemical synthesis of genetic sequences and it is theoretically possible to recreate known pathogenic organisms and design complete novel biological entities with unpredictable characteristics which leads to lack of medicinal production and supply to strong resistant viruses as their source is not known[iii].

Manipulation of Host-Pathogen Interaction- Genetic tools can be used to study and alter how pathogen interacts with the human immune system. It results in enabling immune evasion and prolonged infection. In a hostile context, this knowledge could be exploited to design agents that delay immune recognition[iv] or reduce the effectiveness of standard treatments.

Targeted or Population Specific Effects- Synthetic Biology also introduces risk related to targeted or population specific effects, although highly speculative and ethically condemned, research into genetic variability across populations raises concerns that biological agents can be engineered to exploit specific biological susceptibilities. Even the perception of such possibilities has strategic and psychological implications for national and international security.

Agro-Biological Warfare- Beyond human health, these technologies can be misused in agriculture which will be commonly called Agro-Biowarfare. It will target crops or livestock critical to food security and economic stability. Genetically engineered plant or animal pathogens could cause widespread destruction without immediate detection, blurring the line between natural outbreaks and deliberate attacks. (Biosecurity in the Age of Synthetic Biology: Safeguarding against Emerging Risks | Taylor's University, 2024)

Most importantly many of these applications do not require state level resources. The democratization of biotechnology, including reduced costs, open access scientific information and the proliferation of private and academic laboratories increases the risk of misuse by non-state actors. This evolving threat landscape challenges existing regulatory and surveillance mechanisms. Overall, while genetic engineering and synthetic biology are transformative fields, their potential application in the development of biological weapons underscores the urgent need for robust biosecurity frameworks, ethical oversight and international cooperation to prevent misuse while preserving scientific progress.

Global Trends in the Advancement and Use of Genetic Engineering and Synthetic Biology

1. **Rapid Market Growth and Technological Expansion**- The global synthetic biological sector is expanding quickly and reducing the cost of DNA sequencing[v] and synthesis, rising adoption across industries like health, agriculture, and environmental applications, and the integration of advanced tools such as AI and machine learning. (Research and Markets, 2025)

2. **Emerging Dual- Use Biosecurity Concerns-** while as mentioned above, synthetic biology and genetic engineering holds immense promise, they also introduce potential dual-use risks. There is increasing international emphasis on managing the potential misuse of these technologies, including unintended or intended consequences and deliberate weaponisation.

(Biosecurity in the Age of Synthetic Biology: Safeguarding against Emerging Risks | Taylor's University, 2024) There was a small example of how the government can control the experiments and research if they find a possible danger. Between 2011-2014, some American labs modified H5N1 influenza virus to make them more transmissible. In 2014, the US government announced a moratorium on funding of various 'Gain of Function' experiments involving Influenza, SARS and MERS. The importance of this case is

- Scientific freedom is not absolute.
- A democracy can pause its own research when risk outweighs benefits.
- Ethical oversight and public accountability can influence national biosecurity policy.

3. **Increased accessibility and democratization of tools**- The technology is becoming more accessible due to the growth of DIY biology movements, low-cost gene editing tools, and widespread distribution of genetic data, raising concerns about governance gaps and uneven safety practices across borders.
4. **Policy and Regulatory Debates Worldwide**- Governments and international bodies are actively discussing frameworks for biosecurity, biosafety, and governance of synthetic biology research. These discussions aim to balance innovation with risk mitigation while addressing ethical, legal, and social implications.
5. **Regional Research and Collaboration Dynamics**- Countries like the United States, China, Japan, Australia, and India are increasing their research output in synthetic biology and related technologies. Collaborative research and strategic partnerships between nations are becoming more common, highlighting both competitive and cooperative dimensions in global biotechnology development. (Asia, 2025)

Assessment of India's Current Capabilities, Vulnerabilities, and Preparedness

India has taken several steps toward strengthening its capacity to respond to biological threats, including those arising from misuse of genetic engineering and synthetic biology. However, preparedness remains uneven and fragmented due to institutional, infrastructural, and strategic gaps.

Current Capabilities

- India operates a nationwide surveillance system, the Integrated Disease Surveillance Programme (IDSP) covering most districts and facilitating early detection of infectious disease patterns.
- India has multiple Biosafety Level (BSL) laboratories, including BSL-3 facilities and at least one BSL-4 facility at the National Institute of Virology in Pune. Plans are underway to upgrade other institutes to BSL-4 standards, such as NIHSAD in Bhopal. (TNN, 2025)
- The National Disaster Response Force (NDRF) has received training specifically for biological disasters, guided by NDMA protocols, and workshops have been conducted to improve interdisciplinary response. (National Workshop on Enhancing Response Capabilities in Biological Disasters | NDRF - National Disaster Response Force, 2015)

Vulnerabilities

- Multiple ministries and agencies (e.g., DBT, DRDO, ICMR, MoHFW) manage different aspects of biosafety and biodefense without a central coordinating authority, leading to siloed decision-making and delayed responses. (Goswami, 2025)
- India lacks a dedicated, updated legal framework specifically targeting modern biothreats and dual-use risks posed by advanced biotechnology. Existing laws were created before recent leaps in synthetic biology and may not adequately govern their misuse.
- Although India has some high-containment labs, their distribution is uneven, and overall capacity for advanced pathogen research, containment, and rapid analysis remains limited compared to needs for deliberate or engineered threats.

- Large population density, particularly in rural areas, combined with variable healthcare capacity, means that disease outbreaks whether natural or engineered can spread rapidly and overwhelm local systems. India's urban and rural health infrastructure is uneven, posing a challenge for rapid, coordinated response.

Preparedness Efforts

- The National Disaster Management Authority (NDMA) has published guidelines for biological disasters, and state governments are developing emergency action plans and simulations to improve readiness.
- India is a signatory to the Biological Weapons Convention (BWC) and participates in export control regimes like the Australia Group. Senior leaders have advocated for modernizing global biosecurity frameworks and stronger compliance mechanisms.
- Experts and policymakers have underscored the need for a national biosecurity strategy with unified governance, enhanced surveillance systems, rapid response teams, and investment in advanced diagnostic technologies to bridge current preparedness gaps.

India's Emerging Security Challenges in the Context of Advanced Biotechnologies

The rapid advancement of genetic engineering and synthetic biology presents a complex set of emerging security challenges for India. While these technologies are essential for innovation in healthcare, agriculture, and industry, their dual-use nature introduces new risks that extend beyond traditional biological threats.

One of the foremost challenges is the increased accessibility of advanced biotechnological tools. The declining cost of DNA synthesis, gene-editing platforms, and bioinformatics software has lowered barriers to entry, making it possible for non-state actors or poorly regulated entities to misuse these technologies. This diffusion of capability complicates attribution and detection of deliberate biological misuse.

India also faces institutional and governance challenges. Oversight of biotechnology research and applications is distributed across multiple ministries and regulatory bodies, often resulting in fragmented governance. Existing biosafety and biosecurity regulations were largely designed for conventional biological risks and may not be fully equipped to address threats arising from synthetic biology, such as engineered pathogens or novel biological constructs. (Emerging Challenges to Biological Security | National Institute of Advanced Studies, 2025)

Another significant concern is public health system vulnerability. High population density, rapid urbanization, and disparities in healthcare infrastructure can amplify the impact of a deliberate or accidental biological release. An engineered pathogen with enhanced transmissibility or resistance could overwhelm surveillance, diagnostic, and response mechanisms before effective containment measures are implemented.

Agro-biosecurity represents an additional and often underestimated challenge. India's dependence on agriculture and livestock for food security and livelihoods makes it vulnerable to biological threats targeting crops or animals. Advances in biotechnology could enable the development of agents designed to selectively damage agricultural systems, causing economic disruption without immediate human casualties. (Emerging Challenges to Biological Security | National Institute of Advanced Studies, 2025)

Finally, strategic and geopolitical dimensions add to India's security concerns. Global competition in advanced biotechnologies, uneven regulatory standards across countries, and the absence of robust international verification mechanisms under existing treaties increase uncertainty. India must navigate a landscape where rapid scientific progress is occurring alongside weak global enforcement against biological weaponization. (Emerging Challenges to Biological Security | National Institute of Advanced Studies, 2025)

Collectively, these challenges highlight the need for India to view advanced biotechnologies not only as drivers of growth but also as critical components of national security, requiring integrated policy responses, strengthened governance, and sustained investment in preparedness and resilience.

Recommended Policy and Regulatory Frameworks for Strengthening National Biosecurity

1. Strengthening Biological Weapons Convention(BWC) would be one of the most crucial steps as BWC prohibits development, production and stockpiling of bioweapons and is the cornerstone of global biosecurity. India supports modernizing BWC with stronger compliance and verification mechanisms to address emerging biosecurity challenges. But the main concern is that even though BWC was established but due to lack of verification and implementation it merely remained on the papers it seems. It needs strong verification as well as implementation.

2. Looking at India, there is a strong need to form a 'National Biosecurity Framework' or 'National Biosecurity Policy' as we should not ignore the biological threats in the age of non-conventional warfare. India has already proposed the 'National Implementation Framework' that included oversight of dual-use research, reporting mechanisms, and incident management which are keys to regulate advanced biotechnologies domestically. (Strengthening Global Biosecurity and Modernising the Biological Weapons Convention (BWC), 2025)

3. Contemporary biosecurity scholarship emphasizes that traditional, static regulatory approaches are insufficient to manage the rapidly evolving risks associated with synthetic biology and advanced genetic engineering. Experts advocate adaptive governance systems that can evolve alongside technological advancements, allowing policies to be periodically revised in response to new scientific capabilities and threat perceptions. A tiered risk-assessment framework is recommended, wherein biological research and applications are classified based on their potential for misuse, scale of impact, and reversibility. Such an approach enables regulators to allocate oversight resources proportionately, rather than applying uniform restrictions that may hinder legitimate research. (Frontiers, 2024)

4. India's Draft National Biotechnology Development Strategy 2020–25 reflects an effort to align scientific innovation with national priorities, including safety, sustainability, and security. The strategy emphasizes the development of robust biotechnology infrastructure networks, enhanced research capacity, and improved coordination between academic, industrial, and governmental actors. Importantly, the policy highlights the need for responsible data sharing and governance of biological information, acknowledging the growing role of genomic data and digital platforms in biotechnology research. Provisions related to molecular surveillance and translational research[vi] are particularly relevant from a biosecurity perspective, as they can strengthen early detection of biological threats while supporting public-health preparedness.

5. The Cartagena Protocol on biosafety represents a precautionary international approach to managing risks associated with modern biotechnology, particularly genetically modified organisms. Its core objective is to ensure the safe handling, transfer, and use of living modified organisms that may have adverse effects on biodiversity and human health. While the protocol is primarily environmental in focus, its principles are indirectly relevant to biosecurity governance. The emphasis on risk assessment, prior informed consent, transparency, and international cooperation provides valuable normative guidance for regulating emerging biotechnologies.

6. Multi-stakeholder dialogue platforms play a critical role in bridging gaps between scientific innovation and security governance. Initiatives such as the Biosecurity Dialogues facilitate structured engagement among governments, scientific communities, industry leaders, and civil society actors. These forums help build shared norms, promote transparency, and encourage responsible conduct in life-science research. They also enable early identification of emerging risks and support coordinated responses across sectors and borders. Such platforms are particularly valuable in addressing the transnational nature of biosecurity threats.(Biosecurity Dialogues, 2025)

7. Australia's Biosecurity Act 2015 represents a comprehensive, risk-based legislative approach to managing biological threats affecting human, animal, and plant health. The law integrates prevention, preparedness, detection, and response under a single statutory framework. It emphasizes proportional risk assessment, inter-agency coordination, and emergency powers during biological incidents. For countries like India, the Act offers useful lessons on unified governance, legal clarity, and adaptive regulatory mechanisms suitable for evolving biotechnological risks.

Conclusion

The convergence of genetic engineering and synthetic biology has fundamentally altered the nature of biological threats, expanding both the scale and sophistication of potential biowarfare. While these technologies hold immense promise for healthcare, agriculture, and sustainable development, their dual-use nature poses serious challenges to national and global security. For India, a rapidly advancing biotechnology ecosystem combined with demographic, infrastructural, and governance complexities increases vulnerability to deliberate or accidental biological incidents.

India has demonstrated important capabilities through disease surveillance systems, laboratory networks, and international commitments such as the Biological Weapons Convention. However, gaps persist in unified biosecurity governance, regulatory oversight of emerging technologies, and preparedness for highly engineered biological threats. Addressing these challenges requires moving beyond reactive public-health responses toward a proactive, security-oriented biosecurity framework.

Strengthening national biosecurity will depend on adaptive regulatory systems, coordinated civil-military mechanisms, sustained investment in scientific infrastructure, and continuous risk assessment of dual-use research. Equally important is India’s engagement in international dialogue and norm-building efforts to modernize global biosecurity governance. Ultimately, safeguarding India against future biological threats will require balancing innovation with responsibility, ensuring that advances in biotechnology contribute to national resilience rather than strategic vulnerability.

Endnotes

i. Site directed mutagenesis is a powerful molecular biological technique to create specific, intentional changes (mutations) in DNA sequence like single base pair substitutions, insertions or deletions using custom synthesized primers in Polymerase Chain Reaction (PCR). This method allows researchers to precisely alter genes to study protein function, understand genetic diseases and engineer proteins with improved or novel properties becoming a cornerstone of modern genetics and biotechnology.

ii. Gain of Function is intentional enhancement of viruses and modifying their existing genetic material to make them more transmissible, more potent and more resistant to many strong antiviral drugs which ultimately make them more deadly.

iii. Vaccines are medicines prepared from the virus strains to prevent disease. Methods involve using the whole virus, part of the virus or the genetic material of the virus. So the complete new strain produced using synthetic biotechnology makes it difficult for scientists to detect and make antiviral drugs.

iv. Immune recognition is a fundamental process where your body identifies what’s self (your own cells) versus non-self (foreign invaders like bacterias, viruses, toxins) using specialized molecules, triggering a defence response to neutralize threats while avoiding attacking healthy tissues.

v. DNA sequencing is the lab process of reading the exact order of the four chemical (Nitrogen) bases i.e. A,T,G,C(Adenine, Thymine, Guanine, Cytocine) in a DNA molecule, revealing the genetic instructions that tell cells how to function and grow which is crucial for understanding genetics.

vi. Molecular Surveillance is the use of molecular biology techniques such as DNA sequencing and gene expression analysis to study and monitor diseases particularly pathogens and cancers. This approach aims to understand the molecular mechanism underlying disease, identify specific subtype or mutations

References

Asia. (2025, February 19). Synthetic Biology in Australia, China, and India: Insights from Asia and Pacific Research Center, Japan Science and Technology Agency. Prnewswire.com; Cision PR Newswire. https://www.prnewswire.com/news-releases/synthetic-biology-in-australia-china-and-india-insights-from-asia-and-pacific-research-center-japan-science-and-technology-agency-302378929.html

Biosecurity Dialogues. (2025, November 5). The Nuclear Threat Initiative. https://www.nti.org/about/programs-projects/project/global-biosecurity-dialogue

Biosecurity in the Age of Synthetic Biology: Safeguarding Against Emerging Risks | Taylor's University. (2024). Taylor's University. https://university.taylors.edu.my/en/student-life/news/2024/biosecurity-in-the-age-of-synthetic-biology-safeguarding-against-emerging-risks.html

Emerging Challenges to Biological Security | National Institute of Advanced Studies. (2025). Nias.res.in. https://cms.nias.res.in/events/emerging-challenges-to-biological-security

Frontiers. (2024). Frontiers | Peer Reviewed Articles - Open Access Journals. Frontiers. https://www.frontiersin.org/

Genetic Engineering. (2025). Genome.gov. https://www.genome.gov/genetics-glossary/Genetic-Engineering

Goswami, A. (2025, August 23). Bioterrorism and India's Security Framework: Aligning National Law with Global Norms - Defence Research and Studies. Defence Research and Studies. https://dras.in/bioterrorism-and-indias-security-framework-aligning-national-law-with-global-norms/

https://www, & book.com/unep. (2019). Risks and potential rewards of synthetic biology. UNEP. https://www.unep.org/index.php/news-and-stories/story/risks-and-potential-rewards-synthetic-biology

National Human Genome Research Institute. (2019, August 14). Synthetic Biology. Genome.gov; National Human Genome Research Institute. https://www.genome.gov/about-genomics/policy-issues/Synthetic-Biology

National Workshop on Enhancing Response Capabilities in Biological Disasters | NDRF - National Disaster Response Force. (2015). Ndrf.gov.in. https://www.ndrf.gov.in/en/pressrelease/national-workshop-enhancing-response-capabilities-biological-disasters

Office, U. S. G. A. (2023, April 17). Science & Tech Spotlight: Synthetic Biology | U.S. GAO. Www.gao.gov. https://www.gao.gov/products/gao-23-106648

Research and Markets. (2025, July 18). Global Synthetic Biology Market Research 2026-2036 | Technology Roadmap Highlights Future of Space Biotech, AI Convergence, and Global Market Democratization. GlobeNewswire News Room; GlobeNewswire. https://www.globenewswire.com/news-release/2025/07/18/3117805/28124/en/Global-Synthetic-Biology-Market-Research-2026-2036-Technology-Roadmap-Highlights-Future-of-Space-Biotech-AI-Convergence-and-Global-Market-Democratization.html

Rugnetta, M. (2016, April 20). Synthetic biology. Encyclopedia Britannica. https://www.britannica.com/science/synthetic-biology

Srinivas, K. (n.d.). Synthetic Biology in India: Issues in Risk, Power and Governance. Retrieved December 18, 2025, from https://www.ris.org.in/sites/default/files/Publication/DP%20194%20Ravi%20Srinivas.pdf

Strengthening Global Biosecurity and Modernising the Biological Weapons Convention (BWC). (2025, December 2). Current Affairs - next IAS. https://www.nextias.com/ca/current-affairs/02-12-2025/global-biosecurity-modernising-bwc

The. (1998, July 20). Genetic engineering | Definition, Process, Uses, Examples, Techniques, & Facts. Encyclopedia Britannica. https://www.britannica.com/science/genetic-engineering

TNN. (2025, June 23). NIHSAD to be upgraded to BSL-4 lab for testing deadly pathogens. The Times of India; The Times Of India. https://timesofindia.indiatimes.com/city/bhopal/nihsad-to-be-upgraded-to-bsl-4-lab-for-testing-deadly-pathogens/articleshow/122032582.cms

About The Author

Harshada Deshpande-Kondlekar (MSc. Defence and Strategic Studies-University of Pune)

Artificial Intelligence and National Security in the Global South: A Critical Appraisal of Its Role as a Strategic Force Multiplier

Abstract:

Artificial Intelligence (AI) has been responsible for reshaping not only the global security architecture but also the national security architecture of individual actors i.e. states. AI has inevitably become a decisive force multiplier across military, intelligence and all other domains of strategic significance. Global South, situated in a complex geopolitical environment, faces multidimensional security challenges. To mitigate these contemporary challenges, integrating AI into national security framework is not only an opportunity but also a necessity, for actors within the region. This paper presents a critical overview of AI's inescapable role in the national security of a country and examines its transformative potential, operational applications, institutional readiness, strategic limitations and the emerging nature of security dilemma, significantly posing a major security challenge for developing countries in the Global South, which are at a higher risk of being "passengers in flight" in the emerging Global AI Ecosystem. This paper further provides a comparative analysis of the degree of AI integration in their National Security Strategy, as compared to that of Global North. The paper, here, attempts to comprehend how a new "Algorithmic Empire" is evolving and how AI can be a key determinant in the emerging dynamics between the Global North and the Global South.

The study, here, critically evaluates the impact of AI on defense modernization, autonomous systems, surveillance, intelligence fusion, cyber defense and border security management of actors within the region. To provide a holistic view, this study attempts to enlist the doctrinal changes, essential for the Global South countries, to transform their national security architectures. The study further focuses on identifying the capability gaps, data-infrastructure constraints, ethical concerns, data sovereignty concerns and the interaction between Civil-Military Domain of the developing countries, with respect to AI adoption, specifically for accommodating the same alongside existing developmental priorities. The paper attempts to provide a number of policy recommendations for strengthening national security frameworks of the Global South actors, providing a robust regulatory mechanism and accelerating their indigenous innovation, in the digital age.

Keywords: Artificial Intelligence, National Security, Strategic Force Multiplier, Data Sovereignty, Regulatory Mechanism, Global South

Introduction:

Artificial Intelligence (AI) has emerged as a critical element fundamentally transforming global and national security architectures. Major global powers have already witnessed AI acting as a potent force multiplier across key domains, including defence, intelligence operations, cybersecurity, and border management. They are using AI as a core technological enabler to maintain strategic edge in national security. The global AI in defence market size was valued at USD 12.55 billion last year[i] and is expected to be worth around USD 178.14 billion by 2034[ii].

The expansion of the global market is driven by several factors such as increased defense spending, technological advancements, demand for autonomous systems, cybersecurity[iii] needs and enhanced situational awareness as well. Global South, situated in a complex geopolitical environment, faces multidimensional security challenges.

To mitigate the contemporary challenges, integrating AI into national security framework is not only an opportunity but also a necessity, for actors within the region. This paper presents a critical overview of AI's inescapable role in the national security of a country and examines its transformative potential, operational applications, institutional readiness, strategic limitations and the emerging nature of security dilemma, significantly posing a major security challenge for developing countries in the Global South region, which are at a higher risk of being "passengers in flight" in the emerging Global AI Ecosystem.

This paper critically evaluates the impact of AI on defense modernization, autonomous systems, surveillance, intelligence fusion, cyber defense and border security management of actors within the region. To provide a holistic view, an attempt is made to enlist the doctrinal changes, essential for the Global South countries, to transform their national security architectures. The study further focuses on identifying the capability gaps, data-infrastructure constraints, ethical concerns, data sovereignty concerns and the interaction between Civil-Military Domain of the developing countries, with respect to AI adoption, specifically for accommodating the same alongside existing developmental priorities. In the last section, a few policy recommendations are provided for strengthening national security frameworks of the Global South actors, providing a robust regulatory mechanism and accelerating their indigenous innovation, in the digital age.

How AI Can Act as A Strategic Force Multiplier?

AI serves as a powerful and effective force multiplier, significantly augmenting operational capabilities and efficiency across multiple security sectors. The applications of AI provide substantial benefits that extend far beyond conventional military domains, creating asymmetric advantages and boosting national resilience.

- **Enhanced Intelligence, Surveillance, and Reconnaissance (ISR):**

One of the primary ways AI acts as a force multiplier is through the dramatic enhancement of Intelligence, Surveillance, and Reconnaissance (ISR) capabilities. AI systems possess the ability to rapidly process vast quantities of heterogeneous data derived from diverse sources, such as satellites, drones (SIGNIT and GEOINT) and social media feeds, performing this analysis faster, more efficiently and accurately than human analysts. This expedited processing capability delivers real-time battlefield awareness and significantly improves the identification of threats. The tangible impact of this application is demonstrated by specific instances, such as the Indian Army’s “Operation Sindoor,” which successfully leveraged AI-based tools for sophisticated enhanced surveillance and precision targeting[iv].

- **Asymmetric Warfare and Predictive Capabilities:**

The adoption of AI-enabled technologies provides crucial strategic advantages in scenarios of asymmetric warfare. Developing nations and even non-state actors can deploy inexpensive, yet highly effective, AI-enabled tools, such as kamikaze drones, offering a strategic counter against adversaries who may possess conventionally superior military power. Beyond the tactical level, AI contributes substantially to strategic planning through predictive analytics and decision support systems. AI allows for the creation of predictive modelling capabilities designed to anticipate patterns of attacks, forecast the movements of adversaries and optimize the deployment of vital resources. This results in faster, data-driven decisions crucial for effective security responses.

- **Cybersecurity and Counterterrorism**

In the vital areas of cybersecurity and counterterrorism, AI capabilities are indispensable. AI aids counterterrorism efforts by identifying suspicious financial transactions, detecting irregular communication patterns, and analysing extremist content. Furthermore, AI strengthens cyber defence posture by automating the detection of vulnerabilities and providing real-time threat response systems.

- **Logistics:**

AI-led predictive maintenance tools such as IBM Maximo Predict, Microsoft Azure Iot Predictive Maintenance or C3 AI Reliability (by US Department of Defense) help forecast equipment failures before they happen and ensure higher level of operational readiness[v] improves the efficiency of supply chains, particularly in contested or challenging environments. For training purposes, AI facilitates the creation of highly realistic, personalized training simulations utilizing virtual and augmented reality. This technological advancement in training is particularly valuable for nations that operate with limited financial and material resources.

- **Civilian Applications and National Resilience**

AI applications in the Global South extend beyond direct military and strategic utility, playing a vital role in civilian sectors which ultimately bolster national resilience and stability.

AI is actively being applied to address pressing developmental challenges within critical societal sectors like healthcare, agriculture, and education. For example, the World Food Program's SKAI model utilizes AI to accurately assess disaster damage, substantially speeding up emergency response operations[vi]. These civilian applications reinforce the overall national fabric, contributing indirectly to security outcomes.

Strategic Limitations to Integration of AI as A Strategic Force Multiplier

Despite the overwhelming strategic benefits, the path to successful AI integration for national security in the Global South seems fraught with significant structural and conceptual challenges. The inherent complexity of geopolitical and developmental hurdles mandates AI integration, yet the region faces a major gap as compared to the Global North in technology, research and development (R&D) capacity as well as in strategic framework development[vii].

A core challenge is the widespread lack of institutional and infrastructural readiness across many developing countries. Many nations lack robust data infrastructure, suffer from a shortage of a skilled workforce capable of developing and managing advanced AI systems and have not yet established coordinated civil-military frameworks necessary for unified strategic development. Furthermore, the absence of robust AI governance models and a heavy reliance on foreign technology providers severely limits indigenous capacity and security autonomy. These deficiencies increase the risk that the Global South actors may become "passengers in flight" in the global AI ecosystem, who are only passively accepting outcomes of AI innovation and regulation rather than shaping them.

The Global South faces a range of multidimensional security threats, including internal conflicts, persistent border tensions, terrorism and increasing cyber vulnerabilities. In this environment, the pressure to adopt AI technologies is intense, leading to a phenomenon that can be described as the "Fear of Missing Out" (FOMO). This inherent urge to rapidly catch up to the AI revolution often bypasses a thorough evaluation of the cost-benefit analysis and the specific suitability of adopted AI policies for their own peculiar national interests. The focus, therefore, must shift from mere emulation of the Global North's policies to strategic regulation aligned with national priorities.

The global asymmetry in AI development means that the Global South frequently bears significant risks associated with the un-audited or potentially biased deployment of AI systems. When core technologies like Machine Learning, Deep Learning, Natural Language Processing, Computer Vision and Generative AI Models especially LLMs[viii] are developed externally, without conducting a proper need-gap analysis, the resultant systems can introduce biases that undermine fairness, efficiency, and security operations within the adopting nation, posing a further dissipation of resources when the Global South already opt for parsimonious developmental initiatives.

Recommendations For Enhancing Digital Sovereignty and Resilience

To navigate the complex challenges and mitigate the risks associated with the Algorithmic Empire[ix], the Global South requires a balanced, strategic and cooperative approach, prioritizing sovereignty and internal development. One of the key challenges to national sovereignty comes from the non-state actors. with the emergence of Cryptocurrency, a new mode of terror funding has emerged where a covert means to move funds across the borders from solicited donations is used posing a challenge to the use of conventional monitoring and tracking mechanisms used by a country's security forces. AI-powered Blockchain Intelligence Tools[x] can facilitate the authorities to map suspicious crypto transactions and directly linked crypto wallets used for carrying out illicit transborder activities.

- **Fostering Indigenous Capacity and Infrastructure**

A crucial step is fostering indigenous capacity through Government Funded Multimodal Large Language Model (LLM) Initiatives, for example, India's BharatGen . Developing localized models tailored to regional languages and contexts is essential for reducing reliance on foreign foundational models.

Equally important is developing Digital Public Infrastructure (DPI) to serve as a global template suitable to the needs of the developing economies and their limited capacity for developing state-of-the-art AI-driven infrastructure and investment in R&D of defence technologies, from scratch. This investment ensures that essential data and digital services are built on sovereign, accessible foundations.

Additionally, embedding Techno-legal compliance directly into the AI development lifecycle (MLOps[xii]) is necessary. An act similar to that of adopted within EU's AI Act[xiii] where Policy-as-a-Code (PaC) directly supports EU regulations, a multilateral cooperative mechanism In the form of a risk management system, that fits the conditions within the Global South AI Adoption framework, can be developed for identifying high-risk AI systems.

This ensures that ethical considerations, governance standards and legal requirements are addressed proactively during development, rather than retrospectively. Automated tools and processes should be implemented for labour-intensive tasks within the security apparatus to maximize efficiency and resource allocation.

- **Governance, Cooperation and Regulation**

The Global South must move promptly to address the regulatory vacuum that currently exists. Instead of traditional, centralized models, establishing a polycentric Governance Commons in the digital domain will not only ensure decentralisation of AI capabilities but also build a more democratic international order in this domain. This decentralized, networked model is designed to facilitate global cooperation on AI standards and practices without compromising individual national sovereignty for any country, developed or underdeveloped.

Here, the diplomatic efforts are vital for securing the interests of the Global South. This requires enhanced Diplomatic Negotiation and Consular Services, supported by data-backed effective and innovative negotiation strategies. Furthermore, in order to avail the timely benefits of emerging technologies, it becomes essential for Global South actors to engage bilaterally and multilaterally, at both regional and global levels. This engagement must focus on developing comprehensive security frameworks covering crucial areas, including:

1. Establishing robust standards for data sovereignty.
2. Securing critical AI supply chains.
3. Developing cutting-edge cyber security and defence collaborations.
4. Creating regulatory frameworks specifically addressing dual-use AI technologies.

Way Ahead:

The Global South stands at a critical juncture where bilateral and multilateral engagement, characterized by high-stakes and nuanced relationship building, is the need of the hour. There is a dire need for a balanced and well-curated approach to AI adoption within the region, moving away from uncritical emulation of existing frameworks and towards focused regulation.

A robust AI policy framework must be implemented, consciously combining four core pillars viz., Innovation, Regulation, Sovereignty, and Cooperation. By focusing on filling the regulatory vacuum and strategically investing in sovereign technological foundations like national LLMs and DPI, the Global South can leverage AI's force multiplying effects while mitigating the profound risks posed by the rising Algorithmic Empire and effectively manoeuvre its strategic interests within the emerging AI-led global order. Not to forget, the failure to adopt this balanced and strategic approach poses an undeniable risk of forfeiting their strategic autonomy and locking developing nations into a perpetual state of technological dependency, hence making the future security and stability of the Global South depend critically on transforming AI from a source of geopolitical vulnerability into a pillar of national resilience.

Endnotes

i. Google. (n.d.). What is MLOps? | google cloud. Google. https://cloud.google.com/discover/what-is-mlops#

ii. Ibid.

iii. Cybersecurity market size, share, Analysis: Global Report 2032. Cybersecurity Market Size, Share, Analysis | Global Report 2032. (2025, December 1). https://www.fortunebusinessinsights.com/industry-reports/cyber-security-market-101165#:~:text=CYBERSECURITY%20MARKET%20SIZE%20AND%20FUTURE%20OUTLOOK&text=The%20global%20cybersecurity%20market%20size,14.40%25%20during%20the%20forecast%20period

iv. Philip, S. A. (2025, October 7). Op Sindoor is India's first AI-enabled operation. how "heavy use" of Modern Tech by Army played out. ThePrint. https://theprint.in/defence/op-sindoor-is-indias-first-ai-enabled-operation-how-heavy-use-of-modern-tech-by-army-played-out/2758797/#:~:text=Representational%20image:%20File%20photo%20of,military%20movement%2C%20enabling%20pinpoint%20targeting

v. Nguyen, N. (2025, September 10). Ai in military: Top use cases you need to know. SmartDev. https://smartdev.com/ai-use-cases-in-military/#:~:text=2.,well%2Dequipped%20for%20their%20missions

vi. Baha, A., & Morrell, H. (2023, July 3). Revolutionizing disaster response with Skai | by WFP Innovation Accelerator | Medium. MEDIUM. https://wfpinnovation.medium.com/revolutionizing-disaster-response-with-skai-1ae9e02e87e5

vii. Yu, D., Gupta, A., & Rosenfeld, H. (2023, January 16). The "Ai divide" between the Global North and Global South. World Economic Forum. https://www.weforum.org/stories/2023/01/davos23-ai-divide-global-north-global-south/

viii. Takyar, A. (2025, October 16). A guide to key AI Technologies. LeewayHertz. https://www.leewayhertz.com/key-ai-technologies/

ix. Appleton, B. (2025). Algorithmic empire and the new digital colonialism: The legal struggle for technological self-determination in the age of ai. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.5389292

x. Ziv, G. B. (2025, October 17). AI and National Security: Promise and peril. Cognyte. https://www.cognyte.com/blog/ai-national-security/#:~:text=It's%20rapidly%20revolutionizing%20the%20way,insights%20and%20make%20smarter%20decisions

xi. Ministry of Electronics and Information Technology, Government of India. (2024, October 1). BharatGen: World's first government-funded multimodal LLM Initiative launched in India. IndiaAI. https://indiaai.gov.in/article/bharatgen-world-s-first-government-funded-multimodal-llm-initiative-launched-in-india

xii. Google. (n.d.-a). What is MLOps? | google cloud. Google. https://cloud.google.com/discover/what-is-mlops

xiii. Article 9: Risk Management System. EU Artificial Intelligence Act. (n.d.). https://artificialintelligenceact.eu/article/9/#:~:text=Summary,shall%20comprise%20the%20following%20steps

About The Author

Utkarsha Mahajan - Full-Time PhD Research Scholar (SIU-Junior Research Fellow), Symbiosis School of International Studies, Symbiosis International University, Pune

Pakistan's Nuclear Programme and the AQ Khan Proliferation Network

Abstract

While most nuclear weaponisation initiatives dealt only with the nuclear programme, the Pakistani one led to a nuclear proliferation network contrived by members of the same programme. This scenario consisted of a stunningly intricate and painstakingly concocted transnational network led by notorious non-state actors with occasional albeit tacit approval of the State (Abbas, 2018). This episode is unique not only for the scale and magnitude of the proliferation network but also the motivations which drove dozens of individuals, operating innumerable organisations, institutions, front companies, myriad middlemen, intemperate profiteers and above all numerous scintillating nuclear scientists and physicists to engage in this unprecedented exercise. It involved an alleged role of State actors, specifically the omnipotent military establishment which brought immense ignominy to the Pakistani State. In light of the recently concluded four-day conflict between India and Pakistan where India's Operation Sindoor decimated numerous Pakistani military assets, debates surrounding the Pakistani nuclear programme, its security or the lack of it thereof, and the decision making processes which drive Pakistan's nuclear policy have gained paramountcy in the Indian psyche. There is, thus, a need for a timely reminder of the dangers of nuclear proliferation and of the inherent fecklessness of, what academicians like Kenneth Walz call, 'nuclear mythmakers' (Walz, 1990).

Keywords: Pakistan, AQ Khan, proliferation, nuclear, network, Libya, Iran, North Korea.

Origins

The Pakistani nuclear programme finds its origins in the 'Atoms for Peace' Initiative introduced by the administration of US President Dwight D Eisenhower in 1953. Pakistan was one of its earliest beneficiaries (Abid, 2021). With this the Pakistan Atomic Energy Commission was founded in the year 1956 with Dr. Nazir Ahmed as its first Chairman (Ahmed, 2011). Munir Khan, also known as 'Reactor Khan' who joined the organization in 1972 as its chairman, remained in office till 1991 (CIA, Declassified document, 1999; Abbas, 2018). Till the 1960s, Pakistan had developed little by way of breakthroughs in nuclear technology with the PAEC, bureaucrats and the Foreign and Finance Offices often at loggerheads with each other especially when it came to mastering the nuclear fuel cycle and establishing reprocessing facilities for the same (EBSCO, 2023). This is seen through the conflicts surrounding the deal between Pakistan and Canada over the Karachi Nuclear Power Plant [KANUPP] (Donohue, 2014). Things came to a head in May 1974 with India's Operation Smiling Buddha, which declared her as the sixth nuclear power of the world after the five permanent members of the United Nations Security Council. This coupled with the defeats she had inflicted on Pakistan in both the 1965 and 1971 wars led to grave introspection in Pakistan. Zulfiqar Bhutto's declaration in an interview in 1965 that "Pakistan would eat grass to build the bomb" had amounted to little (Rajiv S.S.C., 2013). Bhutto was arguably the most vociferous proponent of the programme and General Ayub was its biggest hurdle (Abbas, 2018).

Dr. A. Q. Khan: All of this was set to change with the arrival of Dr. Abdul Qadeer Khan on the Pakistani nuclear landscape. Like Munir Khan, who was employed in the IAEA till 1972, Dr. A.Q. Khan was working as a metallurgist for the European Uranium Enrichment Centrifuge Corporation (URENCO), based in the Netherlands (Abbas, 2018). Here he began his career as a nuclear smuggler in the 1970s (Correra, 2006). Born in Bhopal in 1936, he'd raised suspicions among his colleagues with his frequent strolls into areas of the facility unrelated to his line of work and more importantly, without the consent of his employers (Laufer, 2005). Conjecture continued to grow as Khan was observed asking 'suspicious questions' (Laufer, 2005). Many colleagues claim to have seen him 'roaming the facility, taking notes on the uranium enrichment process in a foreign script' (Singh, 2009). Dutch intelligence had grown far too suspicious of Khan by this point and was on the verge of arresting him, only to be stopped by the CIA in both 1975 and 1986 (Singh, 2009).

Upon his return to his homeland in 1976, Dr. Khan began working for the PAEC under Munir Khan but a schism soon emerged between the two men. His dissatisfaction led Bhutto to create a new organization for him to lead, independent of the PAEC and Munir Khan and focusing on the centrifuge project to build a uranium enrichment facility, as opposed to the plutonium route being employed by the PAEC (MacCalman, 2016). Thus in July 1976, Khan founded the Engineering Research Laboratories later renamed the Khan Research Laboratories in May 1981 in recognition of his contributions by the Zia ul Haq government (MacCalman, 2016). The gradual separation of the KRL from the PAEC and the autonomy bestowed upon it in terms of management, control, and procurement led to the genesis of an illicit export network (Ahmed, 2011). The overthrow of the Bhutto government and the assassination of Zulfiqar Ali Bhutto himself in 1979, paved the way for the rise of a military dictatorship under the leadership of Zia ul Haq. Khan then acquired the Chinese design for a bomb used in their tests (Ahmed, 2011). Dr. Khan's role in the programme and the proliferation network it engendered was so perilous that former CIA director George Tenet once referred to him as being “at least as dangerous as Osama bin Laden.” (Leaver & Parsi, 2009). These episodes describe masterfully the conflicts between the civilian authority and the military which rules the roost in Pakistan. While drawing out the dichotomy between the words and actions of the Pakistani nuclear mythmakers in their quest to find the bomb, it's paramount to examine the internecine power plays which plagued the nation especially in the 1990s. This reveals the travails of the Pakistani political landscape and how seekers of power manipulate their way to the zenith in the Islamic Republic.

Pakistan acquires the bomb: In the 1980s both the PAEC and the KRL conducted nuclear cold tests (Atomic Heritage Foundation, 2018). A.Q. Khan thus informed Zia that Pakistan was ready for a nuclear test at short notice (Aftergood, 2009). A.Q. Khan also claimed in a late 1987 interview given to veteran Indian journalist Kuldip Nayyar that Pakistan possessed nuclear weapons which could be used to defend it against an Indian attack. He further stated that “America knows it. What the CIA has been saying about our possessing the bomb is correct.” (Chari, 2013).

Western reactions: The West, specifically the Americans had prevaricated when it came to the Pakistani nuclear programme. While the stated position of the USA was in stark opposition to the program, it had to make significant amendments to its nonproliferation policy to accommodate its broader security interests. In the 1970s, Congress through the Symington and Glenn amendments to the Foreign Assistance Act cut off aid to Pakistan though it was restored in 1979 (Weiss, 2005). The reason behind this restoration is illustrated best in a note sent by then US National Security Adviser Zbigniew Brzezinski to then President Ronald Reagan highlighting the Soviet Invasion of Afghanistan as being, from then on, the primary driver of the USA's Pakistan policy (Weiss, 2005). Thus, significant and decisive legislations like the Glenn and Symington amendments, passed by Congress to halt the Pakistani nuclear program were rendered ineffective by the Presidency (Pandey, 2023).

Proliferation networks: Iran, North Korea and Libya

Iran: Iran, having attained its nascent nuclear capabilities from the Atoms for Peace initiative of President Eisenhower, further developed its capabilities with the assistance of the A.Q. Khan network from 1987 onwards (Rowberry, 2013). An IAEA report states that it received a set of technical drawings for a P1 centrifuge and some samples of centrifuge components in 1987 (Laufer, 2005). According to further IAEA reports, AQ Khan gave Iran components for 500 centrifuges and designs for P2 centrifuges. Khan reportedly would order twice the amount of material required for the nuclear programme and would sell the surplus to his clients (Laufer, 2005).

The first contact with Iran in this regard was established in 1987 though relations between the two states were cordial for decades till then. There have been reports of Iranian scientists training at the Pakistan Institute of Nuclear Science and Technology (PINSTECH) (Janardhan, 2025). Khan himself is said to have visited the Bushehr reactor which had been built with Chinese assistance (Laufer, 2005). He's said to have offered a deal to help Iran create a cascade of about 50000 P1 centrifuges (Broad & Sanger, 2004). The alleged transfer of P1 and P2 centrifuges reveals a daring operation which couldn't have been undertaken without the approval of those in the highest echelons of the government. This aligns with the larger pro Iran tilt of the then Army Chief M.A. Beg, himself a Shia. This ties in perfectly with Khan's own admissions of Beg's complicity as also statements by former American diplomats like Henry Rowen (Rowen H. S., 2004)

Iran not only bought nuclear components off the shelf from Khan but also used his list as shopping guidelines to purchase those items from other sources (Clary, 2005). This also points to how unsuccessful western export controls proved to be. Iran developed its nuclear program based on the technology provided by Pakistan. The far-reaching consequences of that particular deal have become clearer with the passage of time. There are independent claims stating that the arrangement with Iran was a quid pro quo. This claim doesn't sound far-fetched since the Pakistanis were undergoing a forex crunch themselves in the mid to late 1990s. The conversations and meetings between high-ranking officials of both states prove state knowledge and complicity in the matter (Abbas, 2018)

North Korea: While Pakistan and the DPRK enjoyed strategic relations from the times of Z.A. Bhutto, the cooperation strengthened under Benazir Bhutto's premiership (Abbas, 2018). A.Q. Khan himself undertook several trips to the nation which serve as circumstantial evidence to the close nuclear cooperation between the two powers (Tertrais, 2008). The deal between the two was essentially a barter with Pakistan accepting the liquid fuelled missile technology in exchange for providing nuclear technology to the DPRK (Clary, 2005). The Pakistani Ghauri missiles were a result of the designs of the No Dong missiles provided by the North Koreans (Abbas, 2018). Since it was necessary for Pakistan to come up with a missile delivery system for its nuclear warheads, they are believed to have engaged in this egregious trade off. Khan, according to Musharraf, could have helped the North Koreans with uranium enrichment and uranium hexafluoride production (Clary, 2005). A lot of uranium containers were apparently from Pakistan thus proving its complicity. General Jahangir Karamat's visit to the DPRK in 1997 points to the same (Singh, 2009).

Libya: It's believed that Gaddafi's Libya was one of the key financiers of the Pakistani nuclear programme alongside Saudi Arabia (The Hindu, 2025; Kazi, 2004). This was in exchange of ‘certain nuclear cooperation’ namely the transfer of 20 complete L1 centrifuges, 2 used L2 centrifuges and 2 small cylinders of UF6 besides weapons designs provided originally by the Chinese to the Pakistanis (Perkovich, 2008). While other instances have more concrete incidents of State involvement, the Libya case seems more of a gambit by A.Q. Khan and his accomplices in order to enrich themselves than an outcome of deliberate state policy. This demonstrates that the Libya deal was far more a product of Dr. Khan’s greed and an inveterate pan-Islamism than a thoroughly calculated move approved by the Pakistani state. This though is contradicted by Benazir Bhutto who alleges Musharraf's involvement in the deal (Abbas, 2018).

Other clients: There have been instances of collusion between Pakistan and Iraq as also Syria though it rarely came to fruition (Laufer, 2005). It's been reported that the Saudis having invested significantly in the Pakistani programme may buy a few bombs off the shelf if the need arises (Urban, 2013).

Network's exposure and its ramifications: The shipment of the A.Q.Khan network's nuclear materials to Libya was exposed in the incident involving the seizure of components on the BBC China leading to international outrage (Singh, 2009). By this time, pressure from the Americans had grown on the Pakistanis to rein in Khan. Thus, the State began to gradually curb his activities. The formation of the National Command Authority and the Strategic Plans Division were aspects of the same strategy (Luongo and Salik, n.d.). With the hierarchy changed and Khan denied direct access to the country's Chief Executive, he was gently eased out of his role in 2001 over concerns of corruption and proliferation related activities (Ahmed, 2011). With the revelations by Libya to the IAEA and sanctions placed by the State department against KRL, the noose began tightening around Khan's neck. The final blow came the following year when he was arrested and sentenced to house arrest after his admission of guilt (Laufer, 2005). Various members of the infamous network have been subsequently arrested including the Tinners, Gotthard Lerch and B.S.A. Tahir (MacCalman, 2016).

Analysis: While analysing the motivations of various members of the infamous network, it's important to take a very academic and critical view of the incidents and guard against any sort of dogma. This is achieved not only by analysing the particulars of the programme but also by delving into how numerous factors play a role in the rise of such perilous transnational networks run primarily by non-state actors.

Political instability, tepid civil- military relations, the preponderance of the security establishment in the decision-making processes of that nation, institutional rivalries and bureaucratic inefficiency led to the rise of this proliferation network. However, there are a number of causal factors which may also have played a crucial role in what transpired in the State of Pakistan. Primary among them might be an errant weakening of civil society and the silencing of an enlightened and informed citizenry. While India stands out as a State with a vibrant and fearless civil society, Pakistani policy makers having successfully decimated their own in pursuit of a "hard state" have suffered the consequences of their megalomania. Another key reason behind the formation of this network was the financial gain which accrued to its members. Khan himself was said to have been the proud owner of numerous expensive properties in Dubai and is believed to have invested immensely in a hotel in Timbuktu (Times of India, 2004). This stands in good stead when one looks at allegations stating that the Iranians paid Khan over 3 million US Dollars in cash for his assistance. His net worth is said to have peaked at 400 million dollars, a handsome amount by any measure (Powell & McGirk, 2005).

It's also necessary to acknowledge what might often be termed as 'psychological factors' affecting these nuclear mythmakers. While financial gain was certainly a driving factor behind this endeavour for A.Q. Khan and his gaggle of conspirators, more important was perhaps the megalomania which had taken hold of Khan's mind. His placing a portrait of himself beside the Afghan Sultan Ghauri, while financing the renovation of his tomb is a case in point (Powell & McGirk, 2005). His commissioning of his own biographies displays another more sinister side of Khan (Abbas, 2018). This depicts his rather cold, manipulative nature as his propaganda efforts created a self-fulfilling prophecy of sorts. His power projection lent him greater heft which translated into financial and political autonomy. This further enhanced his standing amidst his peers, helped him contrive a veneer of impregnability and thus made him more capable of influencing national and political affairs. This emboldened him to operate his network with greater impunity thus fulfilling the cycle.

Another important aspect of this psychological causation is religious fanaticism coupled with a radically anti-Western world view. Khan progressively became more religious as time passed eventually developing some sort of a Messianic complex. This, of course, would fit perfectly into his megalomania and generic superciliousness seen through his constant bickering with PAEC Chairman Munir Ahmad Khan (Abbas, 2018).

"We Muslims have to be strong and equal to any other country, and therefore I want to help some countries be strong," Khan allegedly said once. Time reports ex-colleagues stating that following the U.S. attacks on Afghanistan and Iraq, he railed against the West and 'its operations against the Muslim community.' (Powell & McGirk, 2005).

It's clear through the choice of Khan's clients and potential clients that he viewed himself and his work as a bulwark against Western imperialist hegemony. He perhaps believed that the West and the US in particular were anathema to the Islamic world in general, driving his rhetoric behind the 'Islamic bomb'. His outreach to Saddam's Iraq, the Islamic Revolutionary Iran, Gaddafi's radically anti-Western Libyan regime and purported offers to harshly anti-Western erstwhile Syrian dictator Bashar al Assad support this argument (Hinderstein & Albright, 2004). This reflexive contempt for the West in general and the Americans in particular ties well into the generic anti-occidentalism of Pakistani society. The Pakistani masses have the utmost reverence for anyone ostensibly opposing the imperialist hegemony of the West. The naming of a cricket stadium in Lahore after the erstwhile Libyan leader Muammar Gaddafi is a case in point (Razvi, 2011). So only, one witnesses a strange phenomenon among the Pakistani masses who evidently believe wholeheartedly in the spirit of Samuel Huntington's Clash of Civilizations not unlike their conservative Western brethren. This ideological parallelism between Western cultural nationalists and Pakistani Islamists is disconcerting to say the least.

While dealing with the history and the present, it behoves one to project a possible future trajectory for that nation's nuclear domain. Financial greed on the part of European financiers and companies, lax export control regimes and an incapacity to regulate dual use technologies all contributed to the A.Q. Khan saga. Political compulsions and intelligence lapses drove Western countries to turn a blind eye to this festering wound for which the world is paying a heavy price even today. Pakistan, which benefits from these black markets to expand its nuclear capabilities, has little reason to work towards ending them (Kimball, 2009).

What can be done:

The UNSC Resolution 1540 adopted in 2004 focuses on nonproliferation efforts and addressing the concerns over non-state actors gaining nuclear capabilities (Arnold and Dolzikova, 2021). Implementing a strict sanctions regime, putting in place measures to prevent illicit trade in nuclear components, dismantling existing proliferation networks, enforcing strict export control measures especially for dual use materials, freezing assets of rogue actors, intelligence sharing among law enforcement agencies globally are a few steps which must be considered. Cracking down on criminal networks, terror financing and money laundering through international law enforcement bodies like the FATF and Interpol can help in globalising best practices.

Conclusion:

Thus it can be demonstrated that an intricate interplay of factors resulted in a rogue militaristic state like Pakistan getting hold of the bomb. From insidious institutional rivalry to obdurate bureaucrats, profligate politicking, and an egomaniacal praetorian guard, the Pakistani nuclear programme has been impacted by each of these factors. While looking into the temporal aspects of it, one ought to brood over those intemperate states of the mind which compel a litany of individuals to engage in such deleterious practices. This narrative surrounding the programme and the proliferation network which arose as a result of it, weaves together religious fanaticism, radicalisation and an anti-Western outlook with the sheer lack of civilian oversight, feeble governments, and the hubris of the military class which led to one of the gravest threats the world has ever faced.

References:

1. Abbas, H. (2018). Pakistan's Nuclear Bomb: A Story of Defiance, Deterrence and Deviance: Penguin India.
2. Abid, A. A. (2021, May 21). Pakistan’s peaceful application of nuclear technology. Strategic Vision Institute. https://thesvi.org/pakistans-peaceful-application-of-nuclear-technology/
3. Aftergood, S. (2009, September 8). A.Q. Khan discusses Pakistan's nuclear program. Federation of American Scientists. https://fas.org/publication/aq_khan/?hl=en-IN
4. Ahmed, M. (2011). Pakistan's Nuclear Odyssey: An organizational and bureaucratic-politics perspective. Journal of Political and Military Sociology, Vol. 39, pp. 61-83. https://www.jstor.org/stable/45408282?searchText=%28AQ+Khan+network%29+organization+bureaucratic+politics&searchUri=%2Faction%2FdoBasicSearch%3FQuery%3D%2528AQ%2BKhan%2Bnetwork%2529%2Borganization%2Bbureaucratic%2Bpolitics%26so%3Drel&ab_segments=0%2Fbasic_search_gsv2%2Fcontrol&refreqid=fastly-default%3A5e0cb9bb26ef5fc639ec8614d8094817&seq=1
5. Albright, D. & Hinderstein C. (2004, February 4). Documents indicate A.Q.Khan offered nuclear weapon designs to Iraq in 1990. Institute for Science and International Security. https://isis-online.org/isis-reports/documents-indicate-a.q.-khan-offered-nuclear-weapon-designs-to-iraq-in-1990
6. Arnold, A. & Dolzikova D.(2021, October 15). A.Q. Khan is dead: Long live the proliferation network. Royal United Services Institute. https://www.rusi.org/explore-our-research/publications/commentary/aq-khan-dead-long-live-proliferation-network
7. Atomic Heritage Foundation. (August 23, 2018). Pakistani nuclear program. https://ahf.nuclearmuseum.org/ahf/history/pakistani-nuclear-program/?hl=en-IN#:~:text=It%20conducted%20over%2020%20additional,invited%20Pakistani%20scientists%20to%20Beijing.
8. Broad W. and Sanger D. (2004, February 12). A tale of nuclear proliferation: How Pakistan built its network. New York Times https://www.nytimes.com/2004/02/12/world/a-tale-of-nuclear-proliferation-how-pakistani-built-his-network.html

9. Central Intelligence Agency. (1999). Pakistan: Nuclear Decision makers – Unanimous opinion. [Declassified document]. https://www.cia.gov/readingroom/docs/DOC_0000252645.pdf

10. Chari, P.R. (2013, November 14). Nuclear signaling in South Asia: Revisiting A. Q. Khan's 1987 threat. Carnegie Endowment for International Peace. https://carnegieendowment.org/research/2013/11/nuclear-signaling-in-south-asia-revisiting-a-q-khans-1987-threat?lang=en

11. Clary, C. (2005). The A.Q. Khan Network: Causes and Implications. (Master's thesis, Naval Postgraduate School). Defense Technical Information Centre. https://apps.dtic.mil/sti/pdfs/ADA443142.pdf

12. Correra G. (2006) Shopping for bombs: Nuclear proliferation, global insecurity, and the rise and fall of the A.Q. Khan network. Oxford University Press

13. Donohue, M. (2014, March 15). Pakistan's nuclear program. Stanford University. http://large.stanford.edu/courses/2014/ph241/donohue2/?hl=en-IN#:~:text=%5B1%5D%20The%20initial%20focus%20of,1955%20at%20Argonne%20National%20Laboratory.

14. EBSCO. (2023). Pakistan nuclear weapons program. https://www.ebsco.com/research-starters/power-and-energy/pakistan-nuclear-weapons-program?hl=en-IN

15. Janardhan, V. (2025, June 2023). When Pakistani A.Q. Khan network helped Iran's tomic programme and possibly its quest for a nuclear weapon. Wion news. https://www.wionews.com/world/iran-israel-war-when-pakistani-aq-khan-network-helped-iran-s-atomic-programme-and-possibly-helped-its-quest-for-a-nuclear-weapon-1750679523812?hl=e2005

16. Kazi, R. (2004, February 11). Halting the nuclear trade. Institute of Peace and Conflict Studies.

https://www.ipcs.org/comm_select.php?articleNo=1300&hl=en-IN

17. Kimball, D.G. (2009). Focus: Learning from the A.Q. Khan Affair. Arms Control Today, Vol. 39, No. 2, p. 3. https://www.jstor.org/stable/23628642?read-now=1&seq=1

18. Laufer, M. (2005, September 7). A. Q. Khan nuclear chronology. Carnegie Endowment for International Peace. https://carnegieendowment.org/research/2005/09/a-q-khan-nuclear-chronology?lang=en

19. Leaver E. & Parsi D. (2009). Foreign Policy in Focus. Review: Shopping for bombs: Nuclear proliferation, global insecurity, and the rise and fall of the A.Q. Khan network. Oxford University Press https://fpif.org/review_shopping_for_bombs_nuclear_proliferation_global_insecurity_and_the_rise_and_fall_of_the_aq_khan_network/

20. Luongo, K.N. and Salik N. (n.d.). Building confidence in Pakistan's nuclear security. Arms Control Today. https://www.armscontrol.org/act/2007-12/features/building-confidence-pakistans-nuclear-security?hl=en-IN

21. MacCalman, M. (2016). A.Q. Khan Nuclear Smuggling Network. Journal of Strategic Security, Vol.9, No.1, pp.104-118. https://digitalcommons.usf.edu/cgi/viewcontent.cgi?article=1506&context=jss

22. Pandey, S. (2023, August 21). US sanctions on Pakistan and their failure as a strategic deterrent. Observer Research Foundation. https://www.orfonline.org/research/us-sanctions-on-pakistan-and-their-failure-as-strategic-deterrent

23. Perkovich, G. (2008). Pakistan's nuclear future: Worries beyond war. Could anything be done to stop them? Strategic Studies Institute, US Army War College, pp. 59-84. https://www.jstor.org/stable/pdf/resrep12046.6.pdf?refreqid=fastly-default%3A393e37261bd793b412f6b29ab6241dde&ab_segments=&initiator=recommender&acceptTC=1

24. Powell, B. & McGirk, T. (2005, February 6). The man who sold the bomb. Time. https://time.com/archive/6596571/the-man-who-sold-the-bomb/

25. Rajiv, S. S. C. (2014). [Review of the book Eating grass: The making of the Pakistani bomb, by F.H. Khan]. Journal of Defence Studies, Vol. 8, No. 1, pp. 119-126. https://www.idsa.in/system/files/8_1_2014_BookReview_SSamuelCRajiv.pdf

26. Razvi, M. (2011, February 25). A stadium called Gaddafi. The Indian Express https://share.google/KRABiNtoxjKNZoHoT

27. Rowberry A. (2013, December 18) Sixty years of "Atoms for Peace" and Iran's nuclear program. Brookings Institute. https://www.brookings.edu/articles/sixty-years-of-atoms-for-peace-and-irans-nuclear-program/

28. Rowen H.S. (2004, March 30). Pakistan threatened to give nukes to Iran, ex- officials say. Stanford University. https://aparc.fsi.stanford.edu/news/pakistan_threatened_to_give_nukes_to_iran_exofficials_say_20040330#:~:text=The%20clearest%20evidence%20of%20the,t%20know%2C%22%20Rowen%20said.

29. Singh, N. (2009). The Khan Proliferation Network: Intelligence failure or Realpolitik. World Affairs: The Journal of International Issues, Vol. 13, No. 4, pp. 112-123. https://www.jstor.org/stable/48505219

30. Tertrais, B. (2008). Pakistan's nuclear future: Worries beyond war. Khan's nuclear exports. Strategic Studies Institute, US Army War College, pp. 11-57. https://www.jstor.org/stable/pdf/resrep12046.5.pdf

31. Times of India. (2004, February 1). Khan built hotel in Timbuktu. https://share.google/pMolei6xP6btosJMh

32. The Hindu. (2025, September, 19). Pakistan says its nuclear programme can be made available to Saudi Arabia under the defence pact. https://www.thehindu.com/news/international/pakistan-saudi-arabia-defence-pact-nuclear-capabilities-weapons-israel-gaza-war/article70069417.ece?hl=en-IN

33. Urban, M. (2013, November 6). Saudi nuclear weapons 'on order' from Pakistan. BBC News. https://www.bbc.com/news/world-middle-east-24823846

34. Walz, K. (1990). Nuclear Myths and Political Realities. The American Political Science Review, Vol. 84, No. 3, pp. 731-745. https://www.jstor.org/stable/1962764?read-now=1&seq=1

35. Weiss, L. (2005). Turning a Blind Eye Again? The Khan network's history and lessons for U.S. policy. Arms Control Today, Vol. 35, No. 2, pp. 12-18. https://www.jstor.org/stable/23627335?read-now=1&seq=1

About The Author

Yash Swar is a student of FYBA Political Science at St. Xavier's College, Mumbai

Global Trade at Crossroads – Need for an Overhaul

Abstract

The Rising Protectionism and Unilateral tariffs imposed by the sovereign nation states are undermining the authority and credibility. of the World Trade Organisation (WTO) and creating a turmoil in the Global Trade Order. The non-operative status of the WTO’s Dispute Settlement Body ((DSB) is leading to a lot of uncertainty in the Global trade landscape. This paper examines the implications of nonfunctioning of the WTO’s Dispute Settlement Mechanism (DSM), rising protectionism, frequent Most Favoured Nation (MFN) principle violations and the proliferation of bilateral and regional trade agreements (RTA’s) on the post-world-war II multilateral global trade order. The paper deals with an analysis of the WTO agreements to suggest reforms to restore the WTO's Dispute Settlement Mechanism, to ensure impartiality of the global trade body. The paper highlights India’s diplomatic maneuvering to navigates the uncertainty and inconsistency in global trade norms and geopolitical shifts, balancing national interests and domestic priorities while pushing for reforms beneficial to the Global South.

This paper is divided into different parts, beginning with European trade diplomacy with peace of Westphalia, then identifying the efforts of the international community to establish a multilateral trade order with global trade norms under the GATT and WTO, moving to discussing the strategic shifts in trade relations amidst geopolitical tensions and suggesting measures to revive the WTO system and India’s diplomatic maneuvering to navigate the complex and changing global landscape.

Keywords

Multilateral Global Trade Order, Protectionism, Unilateralism, WTO, Dispute Settlement Mechanism (DSM), Dispute Settlement Body (DSB), Free Trade Agreements (FTA).

Introduction

In the contemporary world, Global Trade is in the midst of rapid transformations due to increased geopolitical and economic tensions. The rise of protectionism- fuelled by prioritising national interest, greater scrutiny of investment and economic sanctions, increased trade disputes between nation- states, all lead to a more restrictive trade environment and practices. Unilateralism, independent actions by many states - imposing reciprocal and punitive tariffs, has raised concerns about the effectiveness of the WTO, undermining WTO rules and multilateral cooperation.

Against this background, the paper proposes to examine the relevance of the multilateral trading system with the WTO as the pivot. The paper further addresses the challenges to the global rule-based trading system in the face of economic nationalism and protectionist policies adopted by major contracting parties. A part of the paper discusses India’s strategy to regain trade advantages, including measures adopted to offset the unilateral tariffs.

Beginning of Trade Diplomacy

For international lawyers and international Relations scholars, the Treaty of Westphalia (1648) laid the foundation for the development of the modern Nation-State model of equal territorial sovereign states, as the primary focus of international relations, a model that exists to this day. The Peace of Westphalia ended the most hostile and conflicting period of European history ending both the Eighty Years’ War (1568–1648) and the Thirty Years’ War (1618–48). These wars were fought for a variety of reasons, including religious, dynastic, political and territorial ambitions, and most importantly, commercial rivalries.

By establishing a system of mutually sovereign and equal states, the Peace of Westphalia, among other impactful results, significantly marked the beginning of Diplomacy including trade diplomacy, State -driven trade, with absolute supremacy of the ensuing Trade Negotiations and Contracts, free from all external imperial control.

The territorial states, who are equal sovereigns, were given internal supremacy and economic autonomy with the right to manage their economies and engage in foreign trade independently, including entering into treaties and trade agreements. In essence, the Peace of Westphalia facilitated a more stable European political order removing obstacles on access to trade routes within Europe, crucial for merchants and traders to operate without constant fear of conflict, which in turn fostered a more conducive environment for commerce to flourish[1]. This eventually resulted in shifting the focus of international relations and trade from religious or imperial authority to secular, state-driven (national interest) objectives.

The conduct of negotiations and signing of treaties between and among the independent and equal sovereign states fostered a new environment for building relationships and engaging in trade. The state-led trade started revolving around national interest- promoting, preserving and protecting national interest in trade. To this day, trade and commerce is viewed by many powerful states more as a zero-sum game that could enhance National power.

That is ironically the reality of today's world, where the imposition of unilateral trade tariffs, often referred to as punitive tariffs, seems to be the order of the day. In August this year, the US President Donald Trump imposed an additional 25 per cent trade tariff on India, raising the overall levy to 50 per cent on goods coming from India. The additional 25 per cent tariff is a penalty for New Delhi's continued purchase of Russian oil and thus allegedly funding the Ukraine war[2]. The EU and the USA have imposed economic sanctions on Russia for the latter's invasion of Ukraine. Interestingly, however, certain sectors - pharmaceuticals, electronics, and energy- are exempted from the above punitive tariffs, protecting India's generic drug industry, which supplies nearly 50% of the US pharmaceutical market[3]. This act of the USA once again affirms the fact that Nation States manoeuvre trade negotiations keeping in mind the three "P" of National interest, i.e., Protection, Promotion and Preservation of National Interest.

On her part, India has decried the so-called punitive tariffs as unfair, unjustified and unreasonable and has continued keep sourcing Russian crude oil via alternative non sanctioned suppliers and shadow fleets. This decision is also driven by energy security needs and discounted oil prices offered by Russia, as well as a policy decision to maintain diplomatic relations with an old, trusted ally, sharing a friendship and partnership built during the soviet era. The commitment to maintain strategic energy ties also appears to be reciprocal. Reportedly, at the recently concluded Russia-India annual bilateral summit in New Delhi, the Russian President Putin has said famously,

"Russia is ready for uninterrupted shipments of fuel to India," saying their ties were "resilient to external pressure"[4].

Trade and refining sources estimate that this December shipment will top 1 million barrels per day (bpd), notwithstanding mounting pressure from the American side[5]. The sustained flow is aided by non-sanctioned Russian entities offering deep discounts, and by state-owned refiners such as Indian Oil Corporation, Bharat Petroleum, and Hindustan Petroleum resuming purchases in line with pre-sanctions levels. At the same time the Ministry added that India's buying of American oil is increasing[6]. The hypocrisy is that the USA has been buying significant amounts of enriched uranium fuel from Russia, making Russia a top supplier and allowing for waivers through 2028 due to national interest and limited alternatives[7].

WTO - a Centre for Trade Liberalisation

At the global level, the WTO, established as a core part of the rule-based international order, as a member driven organization, establishes and enforces the global rules of trade to ensure that trade flows smoothly, predictably, and freely[8]. The primary purpose of the WTO is to open trade for the benefit of all and is committed to the principles of transparency, non-discrimination, and binding dispute settlement. WTO agreements, negotiated and signed by the bulk of the world's trading nations are ratified in their legislatures.

However, the influence of WTO as the watchdog of global trade is slowly eroding. After ten years of intense discussions, the Doha Round of trade negotiations among the WTO members, concluded in November, 2011 without achieving the desired goal of multilateral trade liberalisation. The impact of this failure is surely visible on the WTO's rule-making authority and its dispute-settlement mechanism.

Undoubtedly, binding tariffs and applying them equally to all trading partners (most-favoured-nation treatment, or MFN) are key to the smooth flow of trade in goods. In the past, preferential trade agreements (PTAs) among small groups of countries co-existed with multilateral, non-discriminatory trade liberalisation pacts. For instance, the rules that govern anti-dumping duties and countervailing duties to offset illegal subsidies, were in the domain of both the WTO and the PTAs.

As per Article 1 of the WTO Agreements, Agreement on implementation of Article VI of the GATT, 1994, an anti-dumping measure shall be applied only under the circumstances provided for in Article VI of GATT 1994 and pursuant to investigations initiated and conducted in accordance with the provisions of this Agreement[9]**.**

Most importantly, in case of a conflict, the WTO rules prevailed, because the WTO rules conferred enforceable rights that applied uniformly to all WTO members. Whereas PTA-defined rights were applicable only to the PTA members. However, over the years, a variety of developments, like economic nationalism and trade wars, such as the US-China tariff dispute, are creating challenges to the WTO's efficiency and authority as a centre for rule-based global trade governance.

Weakening influence of the Dispute Settlement Body (DSB)

Dispute settlement is the central pillar of the multilateral trading system. The Uruguay Round and the creation of the WTO and DSM (Dispute Settlement Mechanism) resulted in transforming the global trading system to be more rule-based, inclusive, and capable of enforcing trade obligations. WTO'S procedures governing the settlement of disputes, enabled the member nations to resolve trade disputes transparently and efficiently[10].

The commitment was given by member states that the multilateral system of settling disputes under the WTO will be used instead of taking action unilaterally. This amounted to the obligation to abide by the agreed procedures, and accept judgements. Every sovereign member state has a sovereign right to frame rules and regulations to regulate its international trade. This is permissible as long as the rules and regulations, so made, are not in conflict with its obligations and the rights of the other member states. The Uruguay Round agreement introduced a more structured and detailed process of dispute settlement along with a timetable to be followed in resolving disputes (DSB). Most notably, decisions of and reports by the DSB are enforced by the Uruguay Round Understanding on Rules and Procedures Governing the Settlement of Disputes (DSU).

Flexible deadlines were provided at various stages of the procedure, filling the loopholes of the earlier dispute settlement mechanism of GATT. The GATT procedure provided for rulings to be adopted by consensus. Under the current WTO system, rulings are automatically adopted unless there is a consensus to reject a ruling. Any disputant state wanting to block a ruling must rally the support of all other WTO members (including its adversary in the case) to share its view.

With member states increasingly giving primacy to national interests, the dispute-settlement mechanism of WTO is slowly appearing to be less effective. On its own, the WTO has no authority to unilaterally impose resolutions of international trade disputes. While the decisions of the WTO are binding on its members, the WTO decisions are enforced by consensus by member nations. This has enabled member states to escape WTO decisions, in case of a perceived threat to national interests

The WTO dispute settlement process starts with bilateral consultations between the disputant parties (Article 4 of the DSU), providing the disputant parties an opportunity to discuss the matter and to find a satisfactory solution without resorting to litigation (Article 4.5 of the DSU)[11]. This mandatory, non-judicial, diplomatic provision, a party-controlled and without third-party involvement and supervision provision was made aiming for a quick, negotiated and mutually agreed and WTO-consistent solution. Between the entry into force of the WTO on 1 January 1995 and 31 December 2024, a total of 631 requests for consultations were circulated to the WTO membership. According to WTO statistics, disputes raised in WTO forum during the period 1995- 2024 have involved claims under a broad range of WTO agreements, with the majority of disputes related to anti –dumping, subsidiaries and agriculture[12].

Unfortunately, the highest dispute settlement body of the WTO - the Appellate Body, which is composed of seven Members (As per Article 17 of the DSU). and are appointed by the Dispute Settlement Body (DSB) of WTO, is currently inoperative[13]. The Appellate body is facing an existential crisis, the term of the last sitting member expiring on 30 November 2020., has made the Appellate Body a court without judges. This is because of the blockage of appointment by the USA, the appointment (or reappointment) of Appellate Body members. All WTO members, who are exoffcio members of DSB, must agree with the appointment of new members and the USA has used its veto. The United States has systematically blocked the appointment of new judges since late 2017. Because of this blockage, the Appellate Body, ordinarily composed of seven members, had on 11 December 2019 was left with only one member and from that date, no longer be able to hear and decide any new appeals filed.

The US is especially dissatisfied with the WTO’s rulings in anti-dumping cases, on matters relating to subsidies, countervailing measures, safeguard measures and technical barriers to trade, terming WTO decisions as judicial overreach. The non-functioning of the Appellate Body has enabled large trading blocs to have the upper hand to settle international trade disputes over smaller ones and dictate decisions, mostly favouring their interest.

A lot of appeals including an appeal from India in dispute regarding Indian Tech tariffs initiated by the EU is unresolved, as currently the Appellate Body Division status is non – operational. Ironically, the United States has also notified the Dispute Settlement Body of its decision to appeal the panel reports in the cases brought by China, Norway, Switzerland and Türkiye in “United States— Certain Measures on Steel and Aluminium Products” (DS544, DS552, DS556 and DS564)[14]. With the non-operational status of the highest DSB of the WTO, member states are exploring alternative solutions like bilateral negotiations and bilateral trade agreements and also regional trade agreements.

The Fallout of the Breakdown of the DSB

The WTO was established with the intention to promote free trade, ensure non-discrimination, to create and sustain an uniform rule- based system for resolving trade disputes. Member states increasingly resorting to alternative mechanisms runs the possibility of creating a fragmented trade landscape. Unilateral trade interpretations carry the risk of creating uncertainty, of transforming the multilateral rule-based trading system into a system of power play. This leads to compelling the smaller nations to toe the line of the bigger players.

A most serious challenge undermining the credibility and authority of WTO as a global trade body relates to the economic nationalism stands and anti-globalism populist unilateralism, namely trade restrictive measures allegedly taken by member states in the pretext of protection of national security. The use of the national security exception under Article XXI of the General Agreement on Tariffs and Trade 1994, has proliferated in recent years[15].

The GATT national security exception was always available to GATT Contracting Parties, however members seldom invoked this provision, exercising and showing self-restraint. Trade restrictive measures allegedly taken for the protection of national security by the USA appear to have made the reverse trend, from self-restraint to proliferation of use of this provision for protection of domestic industries.

The protectionist stands, America First policy, under Trump's presidency involving a wide range of measures like unilateral increase in tariffs without prior consultation and quotas on imported goods, along with subsidies and other means poses a serious challenge to the non-discrimination and equal treatment for all members that the MFN clause represents.

Article I (a) of GATT upholds that

Each contracting party shall accord to the commerce of the other contracting parties treatment no less favourable than that provided for in the appropriate Part of the appropriate Schedule annexed to this Agreement[16]**.**

Under MFN, countries levy the same level of tariff for the product. USA has criticized the basic most-favoured nation (MFN) treatment, arguing that this provision prevents member states from optimising individual trade relationships. Unilateral actions like discriminatory application of trade preferences or penalties erodes the principles of predictability and transparency, lead to a divided international system for trade with parallel sets of rules, underpinning the multilateral trading system.

At the home front Mexico's sudden protectionist turn, announcing the imposition of additional tariffs of up to 50% on select Indian imports starting January 1, 2026 appears to be closely tied to the effort of Mexico to align trade policy to USMCA (United States-Mexico-Canada Agreement) priorities[17]. The announcement is coming from Mexico at a time when the regional trade deal- USMCA, is due for review. After the United States, Mexico becomes the second North American nation to impose a 50% additional tariff on certain goods exported from India.

Rightly to protect trade interests, GOI is negotiating several trade deals in a bid to offset the effect of the US tariffs. This strategy of India showed tangible results with the signing of the Comprehensive Economic and Trade Agreement (CETA), with the UK[18]. Most importantly, the UK-India Free Trade Agreement (FTA) includes deliverables, including duty-free access for 99% of Indian exports to the UK and the reduction of UK tariffs on 90% of Indian goods. Other deliverables include enhanced professional mobility for skilled workers and easy access for Indian professionals to sectors like IT and finance. Also an increased access to UK public procurement for Indian firms is another significant deliverable. This has prompted many commentators to describe this trade deal as a win–win deal for both partners. The India- UK FTA 2025 with clear deliverables may be taken as a reference - as a template for concluding further trade deals by India with other nation states.

At the same time, we need to be aware of the possibility that Bilateral trade deal may expose Indian farmers and small-scale industries to intense global competition, particularly in agricultural and labour-intensive sectors. President Trump has made the reduction of US tariffs conditional on the opening of the Indian market to US agricultural products. India has long used protectionist means to shield its vital farming sector, which employs 40 per cent of the country's workforce[19].

As a leading member state of organisations like ASEAN and BRICS plus, focus must be made on continuing efforts for diversifying markets, building resilient supply chains, and leveraging collective bargaining power. In this context the recent signing of the Comprehensive Economic Partnership Agreement (CEPA) with Oman, is a strategic trade strategy and well-timed[20]. In a global trade environment of protectionism and uncertainty , most nation-states are seeking an export destination closer to home, making nearshoring and friend shoring the norm .

A functioning, rule-based multilateral trade system is crucial for global economic stability. Urgent reform of the WTO is required for removal of power imbalance and protectionism, and to ensure that the global trade remains the medium for inclusive growth, job creation, and sustainable development for all nations, irrespective of the size in terms of population, area or wealth.

The current Director-General of the WTO, Ngozi Okonjo-Iweala, has recently reiterated that the multilateral trading system is bent, not broken[21]. She has made an appeal for using the current challenges as a golden opportunity for urgent and meaningful reform. Speaking in the capacity as Chair of the Trade Negotiations Committee (TNC), the WTO Director-General told a meeting of the (TNC) on 15 July, 2025.

The world is looking to the WTO to respond to issues that impact lives, livelihoods and the future prospects of the businesses that drive trade.

A major concern of developing states is that the WTO's Dispute Settlement Body (DSB) is becoming more legalistic, making the process more expensive and complex, shifting away from its original diplomatic approach. The exorbitant financial cost and lack of specialised expertise to navigate complex legal framework, is allegedly resulting in power imbalance in the DSB. Decisions are given on precedents of past cases making the system predictable and more formal, reducing theoriginally intended diplomatic element. To counter fragmentation and to build resilience, the Director General has also advocates for an alternative strategy -diversifying and deconcentrating supply chains to include more countries in the Global South, thereby fostering inclusivity and resilience without excessive

The Director General has further urged member nations to utilize the upcoming 14th Ministerial Conference (MC14) in March 2026 to show a "genuine shift in negotiations and a change in mind- set and political will to deliver results that address these concerns[22].

The DG further underscored the importance of delivering a manageable and meaningful agenda for MC14[23].

Way Forward- Measures for Overhaul

Global trade is indeed currently at a critical stage, national interest appears to be influencing trade decisions, trade agreements are becoming more like a win –win situation, making it often harder for nation states to arrive at mutually beneficial trade agreements. Rising protectionism is negatively impacting the credibility of the WTO as a global trade watchdog and also undermines the main objects of the WTO to ensure smooth, predictable, and free trade by lowering barriers, creating a platform for trade negotiations, and establishing rules for global trade and commerce.

Apart from dispute settlement, another main function of the WTO is to act as a forum for the negotiation and adoption of new trade rules. The failure of the Doha Round, the latest phase of multilateral trade negotiations among the WTO members is a major setback to the legislative effort of the world body to achieve major reform of the international trading system, through the introduction of lower trade barriers and revised trade rules. The inability of WTO to act effectively as a forum for devising global rules has been paralysed by the fact that all decisions need to be taken by consensus. This appears to be a difficult task with vast economic diversity among the 166-member state, members ranging from high-income and middle-income to Least-Developed Countries (LDCs).

Equally challenging is making the WTO's Appellate Body functional again, to make the body more relevant and less legalistic, address US concerns about alleged judicial overreach of the Appellate body, balancing developing countries interests with US concerns. An opt –out provision, allowing members to opt out of appellate process may be explored, encouraging Mediation as an alternative medium of dispute settlement (Article 5 -DSU). Greater use of ADR will definitely make the DSB process less legalistic and more flexible and diplomatic.

WTO Reforms is to be directed to restore stability and cooperation among nation states. The Appellate body composition and functioning is to be revisited, adopting and applying reforms to make the body less legalistic and more flexible. Currently observer status in the WTO is given only to INGO's (International Intergovernmental Organisations). Engagement with civil society groups is to be explored to strengthen the involvement of NGOs to get diverse perspective in trade negotiations and decisions[24]. A collaborative approach, emphasising on creating multi stakeholder dialogues among governments, business and civil society is to be encouraged to understand the concerns of diverse economic groups. This will ensure the adoption of trade rules that are more market friendly and community rooted, thereby assisting to balance market -driven growth with community and environmental concerns, leading to effective implementation of trade rules.

Article 17 of the WTO's Dispute Settlement Understanding (DSU) , by which provision the Appellate Body was established, provides a timeframe, that appeals shall be decided within 90 days and that an appeal shall be limited to issues of law covered in the panel report and legal interpretations developed by the panel[25]. US has criticized the Appellate body for not following WTO rules, like the 90 day time frame, resulting delays and uncertainty[26]. As and when the USA lift the blocking of the appointment of new members. the 90 -day time frame for issuing Appellate Body reports is to be strictly followed. This will restore the credibility of the DSB. Of the World Trade Organisation. Another contentious issue, that needs urgent attention is the alleged judicial overreach of the Appellate body. The Dispute Settlement Body ("DSB") was established by the WTO member states to administer the WTO dispute settlement system in accordance with the DSU.

In Article 3.7, of The DSU, the WTO Members agreed:

"The aim of the dispute settlement mechanism is to secure a positive solution to a dispute", the aim of the dispute settlement system is not to produce interpretations or "make law"[27].

In light of this provision, a WTO adjudicator's findings must therefore be limited to those findings necessary to resolve a given dispute. This will limit the Appellate Body's interpretation, leading to preserving the sovereignty of the member states. This is important for in Article IX:2 of the WTO Agreement, WTO Members reserved for themselves acting in the Ministerial Conference or General Council "the exclusive authority to adopt interpretations" of the WTO agreements[28].

The USA and some other members are particularly vocal about the interpretation of trade agreements by the Appellate body. USA, for instance has questioned decisions given by the Appellate body on national security exceptions. The Appellate Body must confine it's role only to the original intention of the DSU, to operate within its mandate, refraining from issuing advisory opinions, abstain from addressing issues unrelated to resolve a dispute. The Appellate Body Members must discontinue serving beyond their terms without WTO members approval. All these measures, are suggested to mitigate allegations about the Appellate Body's fairness and legitimacy.

To address the concern of the developing states, Special and Differential Treatment (S&D) provisions are to be made more effective and operational. At the same time, provisions for S&D treatment are to be revisited as some states once considered to be developing are now major economies. The world's second largest economy, PRC recently announced that China will no longer seek Special Differential Treatment (SDT) benefits under future WTO trade agreements, will not claim less stringent obligations in future WTO agreements[29]. This move of PRC, if followed by some other current major economies, still categorised as developing nations in the WTO system will help to make the WTO trading system more balanced. However, graduating from Developing Country status is a complex issue, States concerned must be allowed to have a pragmatic sovereign decision. Only then the shift in status will be beneficial for all, ensuring speedier implementation. A comprehensive approach to WTO reforms including transparency and inclusive agenda setting - addressing the diverse needs of the member states, the greater involvement of the Global South in the negotiating processes would restore faith in the neutrality of the global trade body.

For India, the increased tariffs are to be converted into opportunities for India by powerfully and meaningfully accelerating the 'Aatmanirbhar Bharat'(Self-Reliant India) mission. Indian exporters must be given incentives to sell more to the world, reducing roadblocks at home. The new support from the government to expand trade could include steps like easily accessible loans by relaxing bank lending rules, fewer compliance hurdles, a review of strict quality checks that have been slowing down supply chains, thereby enabling India to integrate with global value chains from a position of strength rather than dependence. In this context the Director General of WTO inviting India to take a proactive role in shaping Global trade reforms is significant[30]. This is surely a "path-breaking moment" giving India a space and opportunity to be the voice of the Global South in making the present global trade order fairer and transparent.

End Notes

1. Zreik, M.(2020): The Westphalia Peace and Its Impact on The Modern European State Available on: https://media.neliti.com/media/publications/348773-the-westphalia-peace-and-its-impact-on-t- 2457df08.pdf

2. US imposes additional tariffs on India for buying oil from Russia (6th august, 2025):

   Available on https://www.ey.com/en_gl/technical/tax-alerts/us-imposes-additional-tariffs-on-india-for-buying- oil-from-russia

3. Industry experts weigh in on US tariff exemption for Indian pharma amid section 232 review: EP News Bureau (August 8,2025) Available on: https://www.expresspharma.in/industry-experts-weigh-in-on-us-tariff-exemption- for-indian-pharma-amid-section-232-review/

4. Joint Statement following the 23rd India - Russia Annual Summit (December 05, 2025), Media Centre, Ministry of External Affairs: Ministry of External Affairs Available on : https://www.mea.gov.in/bilateral-documents.htm?dtl/40410

5. Felicity Bradstock: India Deepens Russian Oil Ties Despite U.S. Tariff Pressure in 2025 (December 14th, 2025) Available on: https://oilprice.com/Energy/Energy-General/India-Deepens-Russian-Oil-Ties- Despite-US-Tariff-Pressure-in-2025.html

6. Team Angel One:India Crude Oil Imports from US Surge Amid Trade Tensions and Russian

Oil Diversification (28 Oct 2025) Available on: https://www.angelone.in/news/market-updates/india-crude-oil-imports-from-us- surge-amid-trade-tensions-and-russian-oil-diversification

7. Russia 'ready to keep supplying enriched uranium to USA'(23rd May, 2025) https://www.world-nuclear-news.org/articles/russia-happy-to-keep-supplying-enriched-uranium- to-usa

8. About the WTO Available on: https://www.wto.org/english/thewto_e/thewto_e.html

9. WTO Analytical Index Anti-Dumping Agreement – Article 1 (DS reports): Text of Article 1

Available:https://www.wto.org/english/res_e/publications_e/ai17_e/anti_dumping_art1_jur.pdf

10. Understanding on rules and procedures governing the settlement of disputes: Annex 2 of the WTO Agreement Available on: https://www.wto.org/english/docs_e/legal_e/dsu_e.htm

11. WTO Analytical Index DSU – Article 4 (DS reports) Available on: https://www.wto.org/english/res_e/publications_e/ai17_e/dsu_art4_jur.pdf

12. Dispute settlement activity — some figures Available on: https://www.wto.org/english/tratop_e/dispu_e/dispustats_e.html

13. WTO Dispute Settlement Body — Developments in 2018 Ambassador Sunanta Kangvalkulkij (Thailand),2018 DSB Chair and 2019 GC Chair 10 th April 2019: Available on https://www.wto.org/english/tratop_e/dispu_e/sunata_19_e.htm

14. DS: 544 United States — Certain Measures on Steel and Aluminium Products: Panel Report under Appeal on 26 January 2023 Available on: https://www.wto.org/english/tratop_e/dispu_e/cases_e/ds544_e.htm United States appeals panel reports regarding US duties on steel and aluminium products: Available on: https://www.wto.org/english/news_e/news23_e/ds544_552_556_564apl_30jan23_e.html

15. The National Security Exception in WTO Law: Emerging Jurisprudence and future Directon: Jacob Gladysz: Available on: https://www.law.georgetown.edu/international-law-journal/wp-content/uploads/sites/21/2021/12/GT-GJIL210007.pdf

16. Understanding the WTO Basis :Principles of the trading system: Available on: https://www.wto.org/english/thewto_e/whatis_e/tif_e/tif_e.htm

17. Mexico Hits India With 50% Tariffs. This Will Be Most Impacted Sector: NDTV World : December 12, 2025: Available on: https://www.ndtv.com/world-news/mexico-slaps-50-tariffs-on-indian-goods-this-will-be-most-impacted-sector-9795503

18. India – United Kingdom Comprehensive Economic and Trade Agreement (CETA): Ministry of Commerce and Industry, Department of Commerce, GOI: Available on: https://www.commerce.gov.in/international-trade/trade-agreements/india-united-kingdom-comprehensive-economic-and-trade-agreement/

19. India–US trade deal talks move forward, but Delhi refuses to open agriculture market:India Today, Dec, 12, 2025: Available on : https://www.indiatoday.in/business/story/india-us-trade-deal-talks-agriculture-market-refuse-to-open-defence-energy-okay-piyush-goyal-trump-tariff-2835007-2025-12-12

20. India and Oman sign CEPA to deepen trade, services and labour mobility Agreement grants near-complete duty-free access for Indian exports, boosts services, MSMEs and worker movement, and positions Oman as a gateway to wider regions: Ministry of External Affairs, GOI December 19, 2025: Available on https://indbiz.gov.in/india-and-oman-sign-cepa-to-deepen- trade-services-and-labour-mobility/

21. Facebook - World Trade Organization - WTO's post (17th September, 2025) https://www.facebook.com/worldtradeorganization/posts/the-global-trade-system-is-bent-not-broken-said-director-general-ngozi-okonjo-iw/1198524098975757/

22. 14th WTO Ministerial Conference. 8th Dec. 2025 WTO Reform Week concludes with "constructive and positive exchanges" among members: Available on: https://www.wto.org/english/news_e/news25_e/mc14_08dec25_239_e.htm

23. DG Okonjo-Iweala: “More than ever all eyes are on us”: 15 th july, 2025, Trade Negotiations Committee news archive: Available on https://www.wto.org/english/news_e/archive_e/tnc_arc_e.htm

24. NGOs and the WTO: Available on : https://www.wto.org/english/forums_e/ngo_e/ngo_e.htm

25. Article 17 of the WTO's Dispute Settlement Understanding (DSU) : Available on : https://www.wto.org/english/res_e/publications_e/ai17_e/dsu_art17_jur.pdf Article 17.5 of the DSU has made it mandatory for the Appellate Body to issue a report, in principle, within 60 days of filing of an appeal to the Appellate Body, and at the most, within 90 days

26. US claims victory in tyre dispute with China The panel was composed by the DG on 12 March 2010, decision given on 18th December, 2010. Available on: https://www.twn.my/title2/wto.info/2010/twninfo101212.htm

27. Article 3-DSU Reports Available on: https://www.wto.org/english/res_e/publications_e/ai17_e/dsu_art3_jur.pdf

28. Article IX:2 of the WTO Agreement Available on: https://www.wto.org/english/res_e/publications_e/ai17_e/wto_agree_art9_jur.pdf

29. China gives up WTO developing-country status as tariff tensions linger – EURO NEWS- 24th september, 2025 Available on: https://www.euronews.com/business/2025/09/24/china-gives-up-wto-developing- country-status-as-tariff-tensions-linger

30. WTO chief urges India to lead global trade reforms WTO chief urges India to lead global trade reforms (The Economic Times- ET online, November 14, 2025) Available on: https://economictimes.indiatimes.com/news/economy/foreign-trade/wto-chief- urges-india-to-lead-global-trade-reforms/articleshow/125322433.cms?from=mdr

About The Author

Dr. Navashikha Duara - Associate Professor, Incharge Principal of SVKM'S Pravin Gandhi College of Law, Mumbai.

Baloch Problem of Nationalism

Abstract

The Baloch problem of nationalism is rooted in the artificial drawing of boundaries and state formation. The Baloch is a distinct ethno-linguistic community and had developed their own tribal structures. British colonial intervention in the nineteenth century fundamentally altered the established tribal structure by fragmenting Baloch-inhabited regions across British India, Iran, and Afghanistan. Colonial policies prioritised strategic and frontier management over socio-economic development, creating enduring patterns of underdevelopment and political marginalisation.

Following decolonisation, and integration of British Baluchistan into Pakistan under military pressure led to the emergence of Baloch nationalist consciousness. In Pakistan, Baloch nationalism has largely taken the form of resistance to centralisation, demands for provincial autonomy, and control over natural resources. However, Baloch nationalism is internally fragmented due to tribal divisions, class differences, and the presence of other ethnic communities.

In Iran, the Baloch experience is shaped primarily by religious marginalisation as a Sunni minority in a Shia-majority state, resulting in limited political representation and the emergence of resistance framed more in religious than ethnic-nationalist terms. In Afghanistan, the Baloch remain weakly politicised, with identity subordinated to tribal and local survival concerns. The paper argues that while language and historical memory provide a shared sense of Baloch identity across borders, divergent state structures and political contexts have prevented the emergence of a unified transnational Baloch nationalist movement.

Keywords

Baloch nationalism; Ethnicity and language; Pakistan; Iran; Afghanistan; Tribal politics; Marginalisation

The Pre-Colonial Baluchistan

From a sociological perspective, language has an important role in tracing community’s historical origins, collective identity, and cultural continuity. It reflects how a community understands itself and preserves its shared heritage over time. In the case of the Baloch, linguistic evidence provides crucial insights into their origins, migrations, and the formation of a distinct ethno-cultural identity. Balochi belongs to the northwestern branch of the Indo-Iranian language family and links the Baloch to the broader Iranian cultural world. Linguistic and historical evidence suggests that the Baloch originally lived near the Caspian Sea region on the Iranian plateau (Bansal 2008; Khan 2009). Political pressures and ecological constraints forced them to migrate eastward within Iran, particularly toward Kerman and Sistan. During this period, they came to be identified as the Baloch, and their language acquired a distinct cultural identity.

In the medieval period, further migration brought the Baloch into the region later known as Baluchistan, a vast semi-desert area stretching from northeastern Iran to southwestern Punjab, and from Khorasan to the Indian Ocean. Despite harsh ecological conditions, the Baloch developed adaptive tribal structures based on agriculture and related activities. Baloch tribal groups moving across harsh terrains also served as links in the ancient trade routes.

The Baloch maintained well-defined political structures before colonial intervention. Authority was organized through a loose confederation of tribes under the Khanate of Kalat. Power rested on negotiated relationships between the Khan and tribal chiefs rather than centralized administration. This system ensured relative autonomy and internal self-regulation and engagement in formal trade and political arrangements.

Baluchistan and British colonialism

British intervention in Baluchistan began in 1839 and was driven primarily by strategic considerations. Baluchistan served as an important trade corridor linking South Asia with the Middle East. Rather than the historical, tribal and cultural continuities, administrative convenience and frontier management were more important concerts for the British. Rather than direct annexation, the British relied on treaties to establish control. In 1854, Kalat was made an associate state, and the Treaty of 1876 formally recognized its independence while effectively placing it under British influence. This treaty allowed Britishers to station their troops, control foreign relations and manage key trade routes.

Baluchistan occupied a critical position as a buffer zone between British India and Russian expansion in Central Asia (Ahmad 2013; Wirsing 2008). In the late 19th Century, the British demarcated boundaries to prevent Russian expansionism. The Baloch inhabited areas were divided into different administrative jurisdictions. British Baluchistan was organized in 1887 as a separate administrative unit and was governed directly by British officials and other territories remained under the indirect rule of Khan of Kalat. Simultaneously the British entered into boundary agreements with Iran and Afghanistan disregarding the tribal networks and movements and divided the Baloch territory across Iran, Afghanistan, and British India.

The British governed Baluchistan from a strategic perspective and were least interested in the development of the region. They did not invest for development in education, economy, and politics of the region and the region remained underdeveloped compared to the other parts of British India.

British colonial rule ended in 1947, but Baluchistan remained fragmented. Pakistan inherited the British Baluchistan and other territories under the indirect rule of the British, Iran retained Eastern Baloch territories and Afghanistan continued to control Baloch areas in the South. Consequently, Baloch became a minority in all the three states. Despite being divided by international borders across Pakistan, Iran, and Afghanistan, the Baloch continue to share a strong sense of common identity rooted in language, tribal structures, and historical memory (Harrison 1981; Titus & Swidler 2000), but the same does not contribute to the development of nationalism among Baloch. Also, their problems in each State very because each state governs them within different political, economic, and ideological frameworks.

Baloch in Pakistan

At the time of the partition of India, the Khan of Kalat argued that Kalat was a sovereign entity with treaty-based relations with the British Crown rather than a princely state under British India. On this basis, Kalat declared independence in August 1947, simultaneously with Pakistan. (Khan 2009; Bansal 2008). Pakistan rejected Kalat’s claim to sovereign equality and viewed accession as essential to its territorial integrity. In March 1948, Kalat was incorporated into Pakistan under military pressure. For many Baloch, this event marked the beginning of political subjugation and continues to shape nationalist consciousness. Resistance to Pakistani rule emerged soon after accession. Early unrest included attacks on civilian targets and demands for the release of imprisoned Baloch leaders. The state’s response relied heavily on military force rather than political negotiation, a pattern that has persisted over decades.

Several waves of insurgency have occurred since 1948, with a renewed phase of low-intensity conflict beginning around 2004. This phase coincided with increased federal control over natural resources and large-scale development projects implemented without meaningful local participation (Wirsing 2008; Ahmad 2013).

Economic exploitation is central to the Baloch grievance. Baluchistan is rich in natural resources, including gas, minerals, and hydropower potential, yet remains one of the most underdeveloped regions of Pakistan. Centralized control over resources and unequal revenue distribution have produced limited benefits for the local population. Peripheral regions such as Baluchistan, Khyber Pakhtunkhwa, and Gilgit-Baltistan host major hydropower projects due to their geography. However, the energy generated is largely diverted to industrial and urban centres, particularly Punjab, reinforcing perceptions of internal colonialism. Poor infrastructure limited educational opportunities, and unemployment further deepen discontent. Internal divisions among Baloch tribes and tensions between Baloch and Pashtun communities complicate collective political action and sometimes lead to localized conflicts.

Tribal factions in Baluchistan and the lack of unanimity

The Baloch are the largest ethnic group in Pakistani Baluchistan, comprising roughly 55–60 percent of the population. Despite being the indigenous population, the Baloch have experienced long-standing political marginalisation and economic neglect, which has given rise to Baloch nationalism. This movement seeks greater autonomy, control over natural resources, and complete independence from the Pakistani state. However, even among the Baloch this demand is not unanimous. Tribal elites, middle classes and those Baloch living in the urban areas have different political and economic interests. They fear that armed insurgencies may increase violence and disturb social economic stability. Hence, they support constitutional reforms for autonomy and not separation.

The Pashtuns, constitute about 30–35 percent of the population and are concentrated mainly in northern Baluchistan, including Quetta, Zhob, and Pishin. They maintain close cultural and political ties with Pashtuns in Khyber Pakhtunkhwa and Afghanistan. Politically, they are opposed to Baloch separatism. Their demands align with the demands of Pashtuns in Khyber Pakhtunkhwa for provincial autonomy and recognition for the Pashtun-speaking population, democratic rights, and protection from militarisation. Thus, their demand is for political inclusion and not for separatism.

The Brahui, although linguistically distinct due to their Dravidian language, identify themselves as Baloch and are therefore integrated into Baloch political movements despite their separate ethnic origins.

The Hazara community is a Shi’a minority concentrated largely in Quetta, which is a conflict prone predominantly Sunni region near the Afghan border. Being a Shi’a minority, the Hazaras have been systematically targeted by Sunni extremist groups and faced severe sectarian violence and social exclusion. So Hazaras prioritise security and survival over participation in Baloch nationalist politics. As a result, they remain largely outside the nationalist movement and pursue different political goals.

Baluchistan also includes Punjabi and Urdu-speaking settlers, primarily in urban areas. As most of them work in the Government services or in the Military, they are viewed as the representatives of the government and anti-Baloch.

Baloch representation

Pakistan has a religious identity, whereas Baloch struggle is based on their ethnic identity and has a sense of being distinct from Pakistan and Baloch nationalism has a strong anti-Pakistan tone. Baloch organisations in Pakistan have different perspectives of Baloch politics. Baluchistan National Party (BNP–Mengal) and the National Party (NP) seek greater provincial autonomy, control over natural resources, and an end to military operations within the federal framework. They support a constitutional solution. In contrast, armed organisations including the Baloch Liberation Army (BLA), Baloch Liberation Front (BLF), and Baloch Republican Army (BRA) reject parliamentary politics and support separatist strand. Baloch Students Organization (BSO) is fragmented, some factions supporting parliamentary measures while others supporting separatism. But its significance lies in being a mobilizational platform for Baloch youth.

Baloch nationalism and insurgency is labelled as terrorism by the Government of Pakistan, and it uses the instrument of suppression against political dissent and demands for autonomy deepening mistrust between the Baloch population and state institutions.

Baloch in Iran and Afghanistan

In Iran, around two million Baloch live mainly in the province of Sistan–Baluchistan. They constitute a Sunni minority in a Shia-majority state, and their primary grievance is religious discrimination, political marginalisation and consequent economic underdevelopment. They are often viewed as politically suspect. Their armed resistance is driven more by religious ideology and not ethnic nationalism. The Iranian state responds with strong centralisation and harsh security measures, leaving little space for ethnic mobilisation. In Iran Baloch political representation has extremely limited scope. No legal ethnic or nationalist Baloch political parties are allowed to operate openly.

Hence there exist informal networks, religious leaders, and sporadic militancy by Islamist groups such as Jundallah and later Jaish al-Adl have emerged rather than formal political organisations (Harrison 1981; International Crisis Group 2009). Thus, the resistance is primarily in religious terms rather than ethnic self-determination (Alfoneh 2013). Their activities do not represent a unified Baloch nationalist agenda.

In Afghanistan, the Baloch constitute a small minority. They are concentrated in Nimruz and parts of Helmand, retaining their tribal structure and local loyalties. Afghanistan's fragmented tribal communities and history of conflicts between them mandates Baloch to be concerned about their survival and local accommodation and not struggle for collective political mobilisation or form a nationalist or the separatist movement. In Afghanistan, Baloch representative organisations are even weaker. Political participation occurs mainly through local tribal leadership and provincial structures, with little emphasis on ethnic nationalism (Titus & Swidler 2000). There is no significant history of organised Baloch separatism or militant mobilisation, and Baloch identity remains secondary to tribal and regional affiliations.

To Conclude

The Baloch question is rooted in historical patterns of migration, colonial intervention, and postcolonial centralization. Language and ethnicity form the core of Baloch identity, shaping a nationalism that challenges state narratives in every state. Although divided by international borders, the Baloch across Pakistan, Iran, and Afghanistan share common experiences of marginalization and underdevelopment. In Pakistan, Baloch grievances largely take the form of political demands for autonomy, control over natural resources, and resistance to centralisation. In Iran, the Baloch face issues of economic marginalisation combined with religious discrimination, as a Sunni minority in a Shia-majority state. In Afghanistan, where state control has historically been weak, Baloch identity is less politicised, and their concerns are shaped more by local insecurity and limited political representation. Thus, while a shared identity unites the Baloch across borders, distinct state systems and socio-economic conditions shape diverse forms of marginalisation and resistance, preventing the emergence of a single, unified political movement.

References:

1. Ahmad, S. (2013). Balochistan: Postcolonialism and the State. Lahore: Vanguard.
2. Alfoneh, A. (2013). “Iran’s Baluch Insurgency.” Middle East Quarterly, 20(3)
3. Bansal, A. (2008). Balochistan in Turmoil: Pakistan at Crossroads. New Delhi: Manas Publications.
4. Harrison, S. (1981). In Afghanistan’s Shadow: Baluch Nationalism and Soviet Temptations. Washington, DC: Carnegie Endowment.
5. International Crisis Group. (2009). Iran: The Rising Cost of Confrontation. Middle East Report No. 87.
6. Khan, M. (2009). The Problem of Balochistan. Karachi: Oxford University Press,
7. Titus, P., & Swidler, N. (2000). “Knights, Not Pawns: Ethno-Nationalism and Regional Dynamics in Post-Colonial Balochistan.” International Journal of Middle East Studies, 32(1), 47–69.
8. Wirsing, R. (2008). Baloch Nationalism and the Geopolitics of Energy Resources. Strategic Studies Institute. Ahmad, S. (2013). Balochistan: Postcolonialism and the State. Lahore: Vanguard.

About The Author

Prof (Dr) Vaibhavi Palsule - Ramnarain Ruia Autonomous College, Matunga, Mumbai

Disclaimer: The opinions expressed in this publication are those of the authors. They do not purport to reflect the opinions or views of the FINS or its members.