INDIC RESEARCHERS FORUM

Civilisation • Security • Statesmanship

TWO-AND-A-HALF FRONT SECURITY REPORT

VOLUME 2 | ISSUE 1 | 2024-25

Foreword by Lt Gen CA Krishnan, PVSM, UYSM, AVSM (Retd.)

Published by:

Indic Researchers Forum

T-12 SMG-II, Ghaziabad, Uttar Pradesh – 201005

Website: www.indicrf.org

Email: indicrf@gmail.com

LinkedIn: Indic Researchers Forum

Twitter | YouTube | Instagram: **@indic_rf**

Disclaimer

This publication reflects the author's individual scholarly perspective. The author(s) certify that the work is original, unpublished, and not under review elsewhere. All data, facts, and figures have been referenced appropriately and are believed to be accurate to the best of the author's knowledge.

Where interviews are featured, the views expressed are solely those of the interviewee(s) and do not represent the official position of the Indic Researchers Forum. Interview content is published in transcript format without editorial modification, preserving the speaker's original intent.

In Memory of Late General Bipin Rawat

PVSM, UYSM, AVSM, YSM, SM, VSM, ADC

(Photo by Arvind Yadav/Hindustan Times via Getty Images)

First Chief of Defense Staff

16 March 1958 - 8 December 2021

INDEX

About Us

Indic Researchers Forum (IRF) is an independent think tank committed to advancing Bharat's strategic and civilizational interests through rigorous research in geopolitics, national security, and global affairs.

Established in 2021, IRF operates on the guiding pillars of Civilization, Security, and Statesmanship. We aim to address Bharat's complex and evolving security challenges both internal and external through a multidimensional lens rooted in cultural depth and strategic realism.

Our intellectual foundation draws inspiration from Late General Bipin Rawat's doctrine of the "Two-and-a-Half Front War," which aptly encapsulates the multifront threats Bharat faces from hostile neighbors to internal destabilization and asymmetric warfare. This framework continues to inform our research agenda as we assess the interconnected nature of military, cyber, ideological, and hybrid warfare domains.

In an era defined by the restructuring of the global order, rising non-state actors, economic volatility, technological disruption, and socio-cultural friction, IRF seeks to promote strategic autonomy, regional resilience, and international partnerships with like-minded partners.

Through a network of scholars, policymakers, domain experts, and military veterans, we publish original research, convene high-impact policy discussions, and develop actionable strategies aimed at protecting Bharat's cultural sovereignty and national security architecture.

IRF believes in cultivating a statesmanship mindset—one that balances civilizational continuity with modern strategic innovation to help shape Bharat's rightful role in the emerging global order.

Research Projects

Monitoring Extremism

Geo-politics & Geo-economics

Indic Bilateral Dialogues

Defense & Aerospace

AI & Cybersecurity

Climate Change & Sustainable Development

Our Team

Senior Board

Maj Gen GD Bakshi
Editor, Indian Military Review

Lt Gen Vinod Bhatia
Former, Director General Military Operations

Lt Gen Vinod Khandare
Principal Advisor
Ministry of Defense

Lt Gen Shokin Chauhan
Former Director General
Assam Rifles

Maj Gen Rajan Kochhar
Former MGAOC
Central Command

AV Marshal PK Shrivastava
Former Director,
Bharat Dynamics Ltd.

Cmde SL Deshmukh
Senior VP, SUN Group
(Aerospace & Defense)

Harjit Sandhu, IPS
M. Director, Canvass Investigations & Research,

Prof. John Nomikos
Director, RIEAS
Athens, Greece

Velina Tchakarova
Founder, FACE
Vienna, Austria

Dr Nanda Kishor M S
Associate Professor; HOD
Pondicherry University

Directors

Yashas Arya
Founder & Managing Director
Indic Researchers Forum

Prof. Srinivasan Balakrishnan
Director (Strategic Engagement &Partnership)
Indic Researchers Forum

Researchers

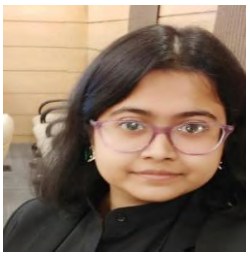
Sathya Pulukuri
Associate Editor
Indic Researchers Forum

Arghish Akolkar
Contributing Editor
Indic Researchers Forum

Mohit Gajbhiye
Senior Researcher
Indic Researchers Forum

Priyanshu Pandey
Researcher
Indic Researchers Forum

Rajas Purandare
Researcher
Indic Researchers Forum



Puloma Pal
Researcher
Indic Researchers Forum

Yubaraj Das
Researcher
Indic Researchers Forum

Evin K. Vinoy
Researcher
Indic Researchers Forum

Foreword

Indic Researchers Forum's "Two-and-a-Half Front Annual Security Report 2024 - 25" is a comprehensive analysis of the contemporary security challenges confronting India. The report addresses multifaceted threats that India confronts. It goes beyond traditional conventional military threats and explores the domains of civil society, controlling river systems, Cyber and Space, Non-State actors, Autonomous systems and India's intelligence culture. It cuts across civilisational, security and statesmanship domains and examines in-depth the ideological, geopolitical and institutional dynamics with focus on China and Pakistan, while also examining internal security issues.

The Forum's specialised centres for China Studies, Pakistan Studies and Internal Security Studies makes it well placed to undertake such a study.

A confident and transformed India is emerging amidst intense global power struggle and the geopolitical turmoil. India's geographical extent and its rich human resource pool combined with a commanding geo-strategic location makes its rivals and the primary global powers view India's rise with apprehension and suspicion. India's rise will be resisted. The regional dynamics makes it easy for rivals to keep the regional environment simmering to tie down India to the region and therefore India's 'Two - And - A Half Front' threat will only gather greater momentum in the decade ahead.

This edition is a sequel to the inaugural Issue of 2023-24 and dwells further and deeper into India's 'Two - And - A - Half Front' threat. It provides a much needed, consolidated set of well-researched articles by distinguished authors, providing a refreshing, 360 degrees coverage of India's security and geopolitical challenges.

The report highlights the need for India to navigate hybrid threats in conjunction with threats along the country's borders, cyber warfare, space militarisation, and domestic ethnic insurgencies. Key themes include China's unrestricted warfare, Pakistan's internal instability and India's intelligence culture reforms.

The first chapter, titled *"Safeguarding India's Democracy & Civil Society: The China Threat"* features a conversation between Lt Gen PR Shankar and Cleo Paskal on China's 'Three Warfares' strategy comprising public opinion, psychological warfare and legal warfare. They discuss China's unrestricted warfare, ideological subversion and influence operations in India. The dialogue highlights India's resilience and contrasts India's democratic pluralism with China's authoritarian brittleness. Key takeaways include the need for comprehensive national security and viewing India-China rivalry as a "Cold War" and a contest of 'world-views' and not just as a competition of interests.

In the chapter *"Navigating the Dragon's Path: Assessing China's Infrastructural Projects on Brahmaputra and its Security Implications for India",* Yubaraj Das examines the issue of China's large scale water diversion projects, a topic which merits detailed analysis by India. The author examines China's South - North water transfer projects on the Brahmaputra (Yarlung Tsangpo), discusses its ecological impacts on Assam's economy, sediment disruption affecting agriculture and fisheries etc. The author highlights two major concerns of India regarding Chinese activity to control Brahmaputra water flow; one of too less water being released and the other of too much being released. The author also examines diplomatic efforts and MoUs for hydrological data sharing and points out China's reluctance for entering multilateral treaties. Yuvaraj Das recommends integrated assessment of downstream vulnerabilities and enhanced river diplomacy.

Puloma Pal explores China's cyber strategy, including military-civil fusion (MCF) and employment of APT groups like APT41 in the chapter *titled "Navigating the Murky Waters of State-Sponsored Cyber Warfare and Asymmetric Tactics in China".* The chapter analyses the cyberattack on Air India's cyber domain in 2021 and brings out the blurred lines between espionage and economy. The chapter further discusses cyber warfare in geopolitics, asymmetric tactics, and recommends use of AI/ML for threat detection, faster reaction to newer threats and the need for public-private partnerships to develop resilience.

China's Arctic and space ambitions as extensions of BRI is examined in the chapter *"Exploiting the Uncharted: China's Interest in Space Program and the Polar Silk Route"* by Priyanshu Pandey. The chapter examines China's investments in Yamal LNG and Polar Silk Road in pursuit of energy security and trade routes in the Arctic. The author also analyses China's space exploration, covering Tiangong Station and APSCO and draws implications for India. Priyanshu Pandey cautions that China's assertiveness in the Arctic and space are indicative of a transformative shift in the control of the global commons. China's assertion of being a "Near-Arctic State," a self-declared status for itself, is seen as part of China's strategy to redefine governance narratives and establish a claim through legal reinterpretation and strategic investments. These efforts blur the lines between peaceful development and strategic militarisation. China's actions provide a unique case study of a resilient and disruptive state power attempting to alter the status quo of the Global Commons. The author recommends global vigilance and appropriate response.

The Chapter on *"Inaugural Pashtun Security Dialogue"* transcribed by Sathya Pulukuri, features dialogues with Levsa Bayankhail, Tilak Devasher, Fazal Ur Rehman Afridi, and Zia Ullah Hamdard, covering the systematic oppression of ethnic groups in Pakistan and Pakistan-Afghanistan relations. The dialogues point to the overwhelming Punjabi domination of Pakistan and the systematic suppression of ethnic minorities like the Pashtuns, Baloch, and even the Sindhis. The situation is described as a form of internal colonialism, where Punjab acts as the metropole and the rest as subjugated peripheries. As per the dialogue participants, well-established lobbying network that presents Pakistan as a victim of terrorism, bigger crises like Palestine hogging the spotlight and Pakistan's control over its domestic media are the reasons for lack of global recognition of the rampant suppression of ethnic groups within Pakistan. There are signs of coming together of oppressed ethnic groups. The Pakistan state fears this as it would challenge the military-dominated structure of Pakistan. Pakistan also exploits the ethnic divisions in Afghanistan to justify deeper interference in Afghanistan. The dialogue participants recall the deep civilisational bonds that Pakhtuns share with India and point out the need for India to push for Pashtun human rights at international forums.

In the chapter on *"Revisiting FATA (Federally Administered Tribal Areas): An Amalgamation of Internal and External Instability for Pakistan"*, Priyanshu Pandey traces the legacy socio-economic issues and governance void in the erstwhile FATA. The author further goes on to evaluate the status of the area after well over five years of merger with Khyber Pakhtunkhwa. The chapter highlights issues of economic stagnation, smuggling, Talibanisation, and Pashtun unrest which plague the region.

Arghish Akolkar's conversation with Dr. Dheeraj Paramesha Chaya examines the Kautilyan roots, post-colonial evolution and India's intelligence failures such as 1962 and Kargil in the Chapter *"India's Intelligence Culture and the Challenge of Reforms"*. Dheeraj Paramesha points out that the threats India faces are far more immediate and diverse in nature than what Western democracies deal with and so India needs a model tailored to meet its own unique requirements. He highlights transparency to be a missing factor and argues for better declassification policies to let researchers examine our past for historical understanding.

He brings out the need for systemic reform across bureaucratic, political and cultural domains and underscores the point that Intelligence apparatus of a country should serve its national security and not be based on political convenience.

In the *Chapter "Examining External Support for ULFA: Implications for Security in Northeast India",* Evin K Vinoy traces the historical background of formation and growth of United Liberation Front of Assam (ULFA), their operational strategies, Funding and external support and implications for National Security and governance of Assam. The author recommends a combined military, economic and diplomatic strategy spread across strengthening border security & intelligence apparatus, addressing socio-economic, illegal immigration, human rights and developmental dimensions as well as diplomatic measures.

The chapter titled *"Adaptations and Evolution in Violent Non-State Actors' Tactical and Strategic Behaviours and Decision-Making"* by Mohit Gajbhiye explores the evolution of such non-state actors and analyses their behaviour and support networks to understand their modus operandi and decision-making process. The author also throws light on state sponsorship and the protection that such sponsorships provide to terrorist organisations. Mohit Gajbhiye also explores how technology, social media and digital platforms are being extensively exploited by violent non-state actors and the way forward to counter the threat through a well thoughtout multidimensional approach.

Rajas Ashish Purandare evaluates risks emanating from Lethal Autonomous Weapon Systems, including the ethics and escalation dimension of their use in the chapter *"Evaluating the Role and Risks of Lethal Autonomous Weapons Systems in Modern Warfare: Ethical, Technical, and Strategic Perspectives"*. The author uses the varying degrees of autonomy of these weapon systems to classify them. He points out the risks associated with autonomous weapon systems such as dangers of unintended escalation and collateral damages, highlights the need to factor in human rights concerns and argues that human oversight should always remain. Rajas Ashish concludes by emphasising the need for regulatory frameworks laying down appropriate legal and moral standards.

The report alerts India's strategic community and policy makers to the need for urgent proactive strategies to counter multi-front threats from China and Pakistan by adopting reforms in intelligence structures, diplomacy and security measures while addressing internal vulnerabilities.

Bangalore, India

October 2025

Lt Gen CA Krishnan, PVSM, UYSM, AVSM (Retd)
Director, Asia Centre Bangalore.
Former Deputy chief of Army Staff & Member Armed Forces Tribunal.
Former Member, Board of Directors Bharat Electronics Ltd & Bharat Dynamics Ltd

=====

ABBREVIATIONS

Abbreviation	Definition
AASU	All Assam Students' Union
ADB	Asian Development Bank
AGP	Asom Gana Parishad
AI	Artificial Intelligence
Al Badr	Militant group active in Kashmir
APHC	All-Party Hurriyat Conference
APSCO	Asia Pacific Space Cooperation Organization
APT	Advanced Persistent Threat
Aqua Tech	Publication on water infrastructure
AR/VR	Augmented/Virtual Reality
BRI	Belt and Road Initiative
C&SO	Cordon and Search Operations
CASIC	China Aerospace Science and Industry Corporation
CCCC	China Communications Construction Company
CCW	Convention on Certain Conventional Weapons

CGTN	China Global Television Network
CII	Critical Information Infrastructure
CISA	Cybersecurity and Infrastructure Security Agency
CMCFDC	Central Military-Civil Fusion Development Committee
CMI	Civil-Military Integration
CNBC TV18	Indian media outlet
CNOOC	China National Offshore Oil Corporation
CNPC	China National Petroleum Corporation
CSSC	China State Shipbuilding Corporation
DGFI	Directorate General of Forces Intelligence
DoS	Denial of Service
ELM	Expert Level Mechanism
EMS	Executive Management System
EU	European Union
FARC	Revolutionary Armed Forces of Colombia
FATA	Federally Administered Tribal Areas
GGE	Group of Governmental Experts
GWE	Great Western Extraction
HuJI	Harkat-ul-Jihad-al-Islami

HuM	Harkat-ul-Mujahideen
HUMINT	Human Intelligence
IB	Intelligence Bureau
IBP	India-Bangladesh Protocol
IDA	International Development Association
IED	Improvised Explosive Device
IFS	Indian Foreign Service
IISS	International Institute for Strategic Studies
IMINT	Imagery Intelligence
IoA	Instrument of Accession
IoT	Internet of Things
IPS	Indian Police Service
ISDB	Islamic Development Bank
ISI	Inter-Services Intelligence
ISIS	Islamic State of Iraq and Syria
ISIS-K	Islamic State Khorasan Province
ISRO	Indian Space Research Organisation
ISS	International Space Station
J&K	Jammu and Kashmir

JEI-K	Jamaat-e-Islami Kashmir
JeM	Jaish-e-Mohammad
JKLF	Jammu and Kashmir Liberation Front
JRC	Joint River Commission
JSTOR	Journal Storage
KIA	Kachin Independence Army
KP	Khyber Pakhtunkhwa
LAWS	Lethal Autonomous Weapons Systems
LeT	Lashkar-e-Taiba
LNG	Liquefied Natural Gas
MCF	Military-Civil Fusion
ML	Machine Learning
MNAs	Members of the National Assembly
MoU	Memorandum of Understanding
MSS	Ministry of State Security
NACTA	National Counter Terrorism Authority
NASA	National Aeronautics and Space Administration
NDA	National Defence Academy
NDFC	National Development Finance Corporation

NGO	Non-Governmental Organization
NISC	National Centre of Incident Preparedness and Strategy for Cybersecurity
NLC	National Logistics Cell
NLI	Northern Light Infantry
NSAB	National Security Advisory Board
NSCN	National Socialist Council of Nagaland
NSCN (IM)	NSCN – Isak-Muivah faction
NSCS	National Security Council Secretariat
NTLM	NT LAN Manager
NWFP	North-West Frontier Province
OSINT	Open-Source Intelligence
PATA	Provincially Administered Tribal Areas
PIMS	Pakistan Institute of Medical Sciences
PLA	People's Liberation Army
PLO	Palestine Liberation Organization
PoK	Pakistan Occupied Kashmir
PPP	Public-Private Partnership
PRC	People's Republic of China

PTM	Pashtun Tahafuz Movement
R&AW	Research and Analysis Wing
R&D	Research and Development
RAND	RAND Corporation
RAS	Research and Analysis Service
SALWs	Small and Light Weapons
SCO	Special Communication Organisation
SIGINT	Signals Intelligence
SIGPAC	Signals Intelligence Pacific
SULFA	Surrendered United Liberation Front of Asom
TGE	Technical Expert Group
TTP	Tehrik-e-Taliban Pakistan
UAS	Unmanned Aerial System
UAV	Unmanned Aerial Vehicle
UCAV	Unmanned Combat Aerial Vehicle
ULFA	United Liberation Front of Asom
UN	United Nations
UNGA	United Nations General Assembly
UNO	United Nations Organization

UNODC	United Nations Office on Drugs and Crime
UNOOSA	United Nations Office for Outer Space Affairs
UPSC	Union Public Service Commission
US	United States
VDC	Village Defence Committee
VDG	Village Defence Guard
VNSA	Violent Non-State Actor

Indic Centre for China Studies (ICCS)

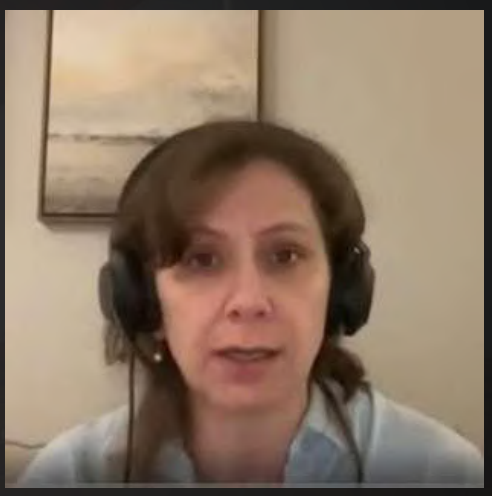
The Indic Centre for China Studies (ICCS) is a specialized research initiative of the Indic Researchers Forum, focused on critically analyzing the ideological, institutional, and geopolitical forces shaping the rise of the People's Republic of China. ICCS provides a dynamic platform for scholars, experts, and strategic thinkers to deliberate on developments in China's domestic politics, foreign policy behavior, technological advancement, and military modernization.

Rooted in an Indo-centric worldview, the Centre seeks to decipher China's long-term strategic calculus and its implications for India and the global order. Whether through border confrontations, digital coercion, economic leverage, or influence operations, ICCS assesses how China's actions are reshaping power dynamics across Asia and beyond. The Centre's work informs India's strategic preparedness in navigating the China challenge with clarity and foresight.

Imaofte Source: Edoftar Su | Reuters

Safeguarding India's Democracy & Civil Society: The China Threat

i» co»vc»s»ľio» »il'h



Lt Gen PR Shankar (Retd.)

Cleo Paskal

Imaofte Source: Edoftar Su | Reuters

Safeguarding India's Democracy & Civil Society: The China Threat

Lt Gen PR Shankar in conversation with Cleo Paskal

Lt Gen P R Shankar is a retired Director General of Artillery. He has held many important command, staff and instructional appointments in the Army. He has vast operational experience having served in all kinds of terrain and operational situations which has confronted the Indian Army in the past four decades. Major 155mm Gun projects like the Dhanush, M777 ULH and K9 Vajra, Rocket and Missile projects related to Pinaka, Brahmos and Grad BM21, surveillance projects like Swati WLR and few ammunition projects came to fructification due to his relentless efforts. He gave great impetus to the modernization of Artillery through indigenization. He is now a Professor in the Aerospace Department of Indian Institute of Technology, Madras.

Cleo Paskal is a non-resident senior fellow at Foundation for Defense of Democracies focusing on the Indo-Pacific region, in particular, the Pacific Islands and India.She has testified before the U.S. Congress, regularly lectures and moderates for seminars for the U.S. military, and has taught at defense colleges in the United States, United Kingdom, India, Canada, and Oman. From 2006 to 2022, she was an associate fellow at Chatham House, London, where, among other responsibilities, she was research lead on the multi-year futures project "Perspectives on Strategic Shifts in the Indo-Pacific 2019-2024."

She is widely published in the academic and popular press. Currently she is the North America Special Correspondent for The Sunday Guardian (India) newspaper.

Discussion

Lt Gen P.R. Shankar (Retd.): Thank you very much. It's an honor to be part of this dialogue on countering China and safeguarding Indian democracy. We must understand that China's tools of influence are not conventional. They are rooted in what is termed the "Three Warfares Strategy": public opinion warfare, psychological warfare, and legal warfare. These are part of the Chinese Communist Party's core tactics in influencing narratives and destabilizing open societies. This is not theoretical. We've seen attempts to influence elections in Taiwan, South Korea, and elsewhere. However, China's success rate has been abysmal. Despite Beijing's efforts, Mr. William Lai won the Taiwanese elections. Who lost that election? China. That's how I see it. In India, their chances are even lower. That said, we must not underestimate their capacity for long-term influence — not necessarily through elections, but through deep inroads into civil society, academia, media, and through ideological subversion. We must remember that parts of India have historically been susceptible to communist ideology — Kerala currently has a communist government, and Tripura and West Bengal did so until recently. Left-wing extremism, too, remains a challenge. So civil society can indeed be vulnerable. Further, we cannot ignore the collusive threat from China and Pakistan — particularly as it pertains to Jammu and Kashmir and the Northeast. China's ability to exploit strife in unsettled regions to challenge our territorial integrity is real. That is the framework in which this discussion must unfold. Before I continue, I would like to invite Ms. Cleo Paskal to present her opening remarks. She brings a global perspective that is both insightful and grounded in years of strategic observation.

Cleo Paskal: Thank you, General. It's a tremendous honor to join this discussion. I've learned a great deal by studying how India has responded to China's *unrestricted warfare* — a term the Chinese themselves use to describe their broad-spectrum, non-kinetic forms of strategic

aggression. Let me offer a bit of background on how I've observed this unfolding. After the Galwan clashes, India's decision to ban 59 Chinese apps — including TikTok and WeChat — was a watershed moment. These weren't just apps; they were *political warfare weapons*. India acted when many other countries were still debating. In Washington, where I'm speaking from, the conversation about banning TikTok continues even now. From that point onward, it became clear that China's unrestricted warfare model was being met by a coherent Indian counter-strategy. The Chinese Communist Party sees India not simply as a regional rival, but as an *existential threat*. Why? Because India invalidates the ideological foundations on which the CCP justifies its rule.

Let me explain.

The CCP claims that authoritarianism is essential to govern a population of over a billion people. But right next door, India — with over a billion people — is a vibrant democracy and doing just fine. China says you need a repressive regime to ensure economic growth. Again, India is disproving that, with growth rates now outpacing China's. Beijing argues that handling diversity requires coercion — they've interned over a million Uyghurs — while India, despite its internal challenges, remains fundamentally pluralistic. All of this undercuts the CCP's legitimacy. So, weakening India — not just geopolitically, but psychologically and ideologically — becomes a *strategic imperative* for Beijing. This is not a game. These are real threats, met by real responses. India has not only resisted, but also *countered* — whether by cracking down on Chinese investment, investigating companies like Xiaomi for money laundering, or restructuring foreign direct investment rules. Each move is part of a *masterclass* in defending national sovereignty through what I'd call comprehensive national defense. Meanwhile, countries like mine — I'm Canadian — are still grappling with recognizing the scale of China's political interference. There is an ongoing national inquiry into foreign

interference in Canadian elections, with well-documented evidence of Chinese influence campaigns. Frankly, much of what India has done pre-emptively, others are only beginning to wake up to. I'm not here to critique India's response. On the contrary, I'm here to learn. So I look forward to hearing more from General Shankar on how India conceptualizes this threat — and how others might learn from it.

Over to you, General.

Lt Gen P.R. Shankar (Retd.): Thank you, Cleo. You've raised several critical points that need to be fully understood by strategic communities worldwide. First — your articulation that *India is an existential threat to the Chinese Communist Party* is not only accurate but fundamental. It is India's *ideological contrast* — the model of a plural, chaotic, yet functional democracy — that threatens the core narrative of the CCP. Let's be very clear: *everything China does is political*. Their endgame is the preservation of the CCP — not prosperity, not peace, not even national pride. If the CCP loses control, nothing else matters to them. That's why Xi Jinping openly advocates a Sino-centric global governance model. In the 20th Party Congress and again at the recent "Two Sessions," he emphasized that China must shape global governance in its own image. This is not just about power projection — it's about *narrative domination*. India defies that narrative. India banned Chinese apps. Others had the capacity, but India had the *will*. India's restrictions on Chinese investments have been more stringent and consistent than almost any other democratic nation. We are pushing Chinese companies like Vivo and Xiaomi out, not through empty slogans, but through investigations, fines, and legal action. We've targeted their laundering networks. These are real actions, not symbolic posturing. Meanwhile, the United States — if I may say — faces a very different challenge. China uses *NAFTA loopholes* and the *Mexican trade corridor* to re-enter the U.S. market via the backdoor. Will American political consensus be strong enough to shut that route? I don't know. But India has

drawn a red line. Now, let's go one step further. Since 1979, China has benefited from a prolonged peace dividend. It rose on the shoulders of Western capital and markets. It's often compared to Germany and Japan — two post-WWII economies that were rebuilt with U.S. support. That support system was a *tailwind*. India, on the other hand, has grown *despite* sanctions, despite multiple wars, despite persistent headwinds. Whether it was Pokhran, the Kargil conflict, or sanctions following defense deals — India has had to claw its way forward. Despite that, we are now the *fifth-largest economy*. And if you believe alternate calculations, possibly fourth. The Chinese economy, by size, remains larger. But *our comprehensive national power* — the sum of economic, demographic, ideological, military, and civilizational strength — is narrowing the gap. So China now faces a dilemma. How is it that a pluralistic, multilingual, internally discordant democracy like India is *rising*, while a monolithic, unitary, command-driven China is starting to wobble? I'd be very curious to hear your thoughts, Cleo, on whether this ideological divergence is something China has *factored into* its long-term strategic planning — or if it's something they're only now being forced to reckon with.

Cleo Paskal: Thank you, General. That's an important shift in the lens. Let's examine it from the *CCP's internal worldview*. What you just described — the idea that pluralism equals strength — is *philosophically alien* to the Chinese Communist Party. The CCP requires obedience. It is designed to suppress rather than nurture human agency. But the things that give people inner strength — *faith*, *family*, and *freedom* — are antithetical to the Party's doctrine. These elements give people moral compasses outside of the Party's control.

The CCP understands this — and therefore seeks to *destroy* those anchors. They've gone after all forms of faith: Falun Gong, Tibetan Buddhists, Muslims, Christians. Anyone whose primary loyalty is not to the CCP is a threat. It's the same with family. The one-child policy was not just a demographic decision — it was a *civilizational fracture*. Entire generations have grown up

without siblings. Millions of Chinese people have no uncles, no aunts, no cousins. They've been raised in households where sharing was unnecessary — even unknown. Now contrast that with India. Families may be complicated, but they are interwoven into the cultural fabric. And family teaches you *compromise*, *reciprocity*, and *shared identity* — values critical for a functioning democracy. This is also why India's G20 presidency was so successful. You didn't just host a summit. You showcased a model of inclusive leadership. You invited the African Union. You brought developmental priorities front and center. You demonstrated not a Western model or a Chinese model — but a *human-centric* model.

And it resonated.

Because, as you rightly said, China's system is becoming increasingly *brittle*. Their control mechanisms must grow stronger just to keep pace with rising fragility. But India, despite its complexity, is *adaptive*. It breathes. That is why — and this might sound philosophical — I believe India's model is not only *morally right*, but also *functionally superior*. It's not just an alternative. It works.

Lt Gen P.R. Shankar (Retd.): You've hit the nail on the head. What we're witnessing is the intensification of China's ideological fragility, matched against India's rising civilizational confidence. Let me give you a simple but profound example. China is a nation that — due to its one-child policy — has produced a generation of people who have never known what it is to have a *sibling*. The entire concept of growing up with a brother or sister — that interplay, that competition, that cooperation — is missing. This is not just a demographic issue. It's a *psychological fracture*. Family is foundational to any stable society. In India, our children grow up not only with siblings, but with uncles, aunts, cousins — a full ecosystem of emotional intelligence. That's why, even with lower per capita income, our social cohesion remains stronger. When you remove that — as China has done — you don't just shrink population

growth. You erode *resilience*. Now pair that with China's rigid, top-down, command-style governance. It produces fragility, not adaptability. And the only way for the CCP to keep control of a brittle society is to increase surveillance, control, and repression. India, on the other hand, functions on *distributed chaos*. Our democracy is loud, messy, and argumentative — but also *resilient*. When something breaks in India, it *bounces*. When something breaks in China, it *collapses*.

Cleo Paskal: Yes, and this was visibly demonstrated at the G20. India brought the African Union to the table — not as a guest, but as an *equal*. That was historic. There was genuine warmth and engagement, a human-to-human connection. That's something China cannot manufacture. Let me give you another example — infrastructure. China exports its model through the *Belt and Road Initiative*, but it often ends up as the *Bribery and Repression Initiative*. The debt-trap diplomacy, environmental destruction, and exploitation of local labor are all part of a pattern. India, when it builds, *includes*. The perception of India is of a nation that's culturally close, non-imperial, and respectful of sovereignty. This isn't soft power. This is *civilizational power*. That is why India is becoming not just a regional actor, but a *global civilizational actor*. And that makes the CCP extremely nervous.

Lt Gen P.R. Shankar (Retd.): And they have good reason to be. As China's internal fragility deepens, its aggression grows. China wants to replace the United States in the global hierarchy, but its more immediate and achievable objective is to *contain India*. You see this clearly in the tools it's using:

- **Cartographic aggression**: Renaming towns in Arunachal Pradesh.
- **Economic interference**: Discouraging companies like Tesla from investing in India — I recently saw a tweet from *Global Times* advising Elon Musk not to invest in India.

- **Proxy narratives**: Funding misinformation campaigns about Indian pharmaceutical products, especially in Africa.

But all these acts reveal *fear*, not strength. China is not as confident as its wolf-warrior diplomats pretend to be.

Cleo Paskal: Exactly. China will try to cut India down — not always directly, but from the sides. It'll use African narratives, Southeast Asian supply chains, and disinformation in Western academia to delegitimize India. The irony is — even their framing often uses Indian terminology. They'll call something "colonial," "inequitable," or "Islamophobic" to mobilize Western liberal guilt against India. It's very sophisticated — and very dangerous. And it means that *every success India has* — whether it's a vaccine rollout, an election, a summit, or a trade deal — will be *targeted*. Which is why India must understand that in this era, even *success* is a vulnerability if it's not defended.

Lt Gen P.R. Shankar (Retd.): Absolutely. And that's why I now firmly believe that India and China are in a *Cold War*. Not just a rivalry — a Cold War.

Everyone's focused on China–US competition. But there's a *parallel Cold War* developing between India and China — less visible, but deeply consequential. On one side, you have a rising, inclusive, democratic civilizational state. On the other, an insecure, repressive, monolithic party-state.

The Indian strategic community needs to recognize this. The Chinese already have. They've begun adapting. They've increased their investment in understanding India. They're studying our economy, our elections, our civil society. And the more they understand, the more they will try to exploit. Which is why we must be ahead — not reactive, but *proactive*.

Cleo Paskal: Let's talk about the kind of external fronts where China is trying to hurt India. One of the under-discussed strategies is the use of disinformation and counterfeit goods in Africa. There have been several documented attempts to push *counterfeit Indian pharmaceutical products* into African markets — deliberately discrediting India's image as the "pharmacy of the world." The goal is simple: weaken India's economic credibility in the Global South, where China is simultaneously pushing its BRI investments. There's a strategic intent behind it — not just economic sabotage, but *geopolitical decoupling* of India from countries that are naturally inclined to partner with it. Let's take another case — the India–Middle East–Europe Economic Corridor (IMEC). It is elegant. It solves many issues in trade realignment post-COVID and bypasses volatile chokepoints. It presents a democratic infrastructure alternative to the Belt and Road Initiative. But the moment it was announced and began to gain momentum — *Gaza exploded*. Now, I'm not saying there's a direct Chinese hand. But strategically, the result is that IMEC has to go on pause, and the entire region is destabilized. Whether by design or opportunity, the result benefits China. Anything India builds — if it lacks a strong defensive mechanism — becomes vulnerable.

Lt Gen P.R. Shankar (Retd.): That's an important point. Galwan was China's last direct strike. Since then, their strategy has pivoted to asymmetric warfare: cyber, economic, social, narrative-based. But their problem is that India didn't respond with appeasement. We responded with resistance — economic pushback, infrastructure acceleration in border areas, and more assertive diplomacy. The old Chinese playbook no longer works on India. That's why — as you mentioned — China is increasingly trying to target India externally, not just internally. The Africa push is one example. Another is the strategic undercutting of India in Southeast Asia — trying to sideline India in ASEAN summits or portraying India as unreliable in defense deals. And yet, the more they try, the more India gains strategic maturity. The G20

showed that India can convene *not just democracies*, but *diverse civilizational states*. That's a diplomatic feat China could not replicate even with its economic clout.

Cleo Paskal: Yes. And the more successful India becomes at this global diplomacy — *the more threatening it becomes to the CCP*. That's why we must keep coming back to one core idea: this is not just a competition of interests — it is a contest of worldviews. China exports a model of control, suppression, and managed dependency. India — through its example — exports *pluralism, autonomy, and partnership*. One is brittle and top-down. The other is messy but resilient. Now, let's talk about the underestimation of India, especially pre-Galwan. In Chinese strategic literature — even in their most analytical military texts like *Unrestricted Warfare* — you'll find deep references to Clausewitz, to Machiavelli, even to Western postmodern theory. But almost no reference to Kautilya or the Arthashastra. India's strategic heritage was invisible to them. They studied India through a Western lens — as a soft, confused democracy — and therefore *underestimated* its ability to strike back, economically, politically, and psychologically. But that's changed now. I strongly suspect that the Chinese strategic establishment has been instructed to reassess India seriously post-Galwan. We should expect sharper, more tailored, more manipulative Chinese campaigns against India in the years ahead — not less.

Lt Gen P.R. Shankar (Retd.): You're absolutely right. If you go back even five years, most Chinese analysts were dismissive of India's rise. They saw us as a perennially conflicted, slow-growth country with too much democracy to make decisive progress. But they misread one thing: India is antifragile. When pushed, we organize. We adapt. We respond. Post-Galwan, India rapidly mirrored Chinese deployments. We rearmed. We rebuilt mountain infrastructure. We imposed real economic costs. And we made it *clear* that Chinese misadventures would have consequences. And now, the strategic calculus has shifted. China cannot risk a kinetic

escalation anymore — because it no longer has the certainty of escalation dominance. So it is *doubling down* on indirect instruments — NGO manipulation, digital propaganda, cyber attacks, cultural and academic infiltration, and diplomatic isolation games. This is what makes it a Cold War.

Cleo Paskal: Yes — and a very asymmetric Cold War at that. India doesn't want it. It didn't start. But it is in it. And we must all realize that the future will not be shaped solely by who has the bigger economy or more missiles — but by who can build trust in a world battered by disinformation, polarisation, and authoritarian overreach. India has the opportunity to lead — *not just as a state*, but as a civilizational compass for others. And that, I believe, is the most profound threat to the CCP.

Lt Gen P.R. Shankar (Retd.): Let me be blunt. While the world is focused on the U.S.–China Cold War, a parallel Cold War is unfolding between India and China. It is quieter, subtler — but just as strategic. Unlike the U.S.–China standoff, this isn't just about trade or tech. It's about two civilizational states with fundamentally incompatible worldviews. China cannot afford India's rise because it undermines its global narrative. Every Indian success — whether in diplomacy, democracy, or technology — is a direct challenge to the CCP's legitimacy. India is climbing. China is peaking — and deeply aware of its demographic and economic slowdown. So how will China act?

It will try to contain India through:

- Economic deterrence (e.g., discouraging FDI like Elon Musk's Tesla project),
- Narrative manipulation (portraying India as hostile or unstable),
- And, increasingly, proxy interference in the Indo-Pacific and Global South.

Cleo Paskal: That's exactly right. And Taiwan is the pivot point where all of this converges. Now, many talk about China invading Taiwan. But the cost-benefit calculus doesn't support it. Militarily, it's far more complex than people think — akin to a Normandy-style amphibious landing under 21st-century surveillance and missile defense. China may rattle sabres, but a full invasion would threaten:

- Its economy (via sanctions and port disruptions),
- Xi Jinping's political survival,
- And the fragile legitimacy of the CCP itself.

More importantly, if the U.S., Japan, and Philippines form an integrated strategic triangle, China will be outflanked. That's why India's quiet support matters — even without formal defense ties.

Lt Gen P.R. Shankar (Retd.): Exactly. India–Taiwan military collaboration is minimal — but economic ties are growing, especially in semiconductors and manufacturing diversification. We're careful. China is watching. But we're also clear-eyed. India cannot afford to provoke China recklessly — not while we depend on Chinese APIs and raw materials. But we also cannot remain passive while China threatens regional peace. Strategic restraint does not mean strategic paralysis. We are building slowly — in trade, tech, and trusted partnerships. And when the time comes, we will act. But let there be no illusion: India will never be neutral in a confrontation between democracy and authoritarianism.

Cleo Paskal: What stands out most to me in India is the *clarity of thought* across generations. Today's discussion was filled with strong, grounded questions — no evasion, no ambiguity. That is India's strength. India has the potential to lead not just by its economy or military, but by example — as a state that can argue without falling apart, grow without conquest, and maintain cultural confidence without needing uniformity. This is something deeply human, and deeply

civilizational. And the rest of the world is taking notice. India's democracy is not a Western import. It is rooted in family, faith, and community — structures that existed long before modern states did. And these are exactly the values that the Chinese Communist Party seeks to dismantle. India doesn't need to mimic the West or compete with China on authoritarian terms. You are *already offering an alternative* — and the world is ready for it.

Thank you for the invitation to learn from you today.

Lt Gen P.R. Shankar (Retd.): Thank you, Cleo. Let me close with one thought: India is returning to its civilizational trajectory. That's what this century is about. Not dominance — but *rediscovery*. China rose quickly, yes. But its one-child policy, brittle society, and rigid control model are already limiting its future. India's rise will be slower — but it will be more *sustainable*. India's youth are now global. They speak English, code in Python, and quote the Gita — in the same sentence. That's powerful. But we must also understand ourselves better. Most of us know our state, maybe our region — but not our country. India isn't one monolith. It's ten Indias — from Manipur to Gujarat to Kashmir to Tamil Nadu. *We must experience them*. That builds empathy. That builds unity. And we must grow with our neighbors. A powerful India surrounded by weak, unstable neighbors isn't success — it's risk. Only when India rises with its region, with compassion and strength, will we be seen not just as a great power — but as a *great civilization restored*.

Navigating the Dragon's Path: Assessing China's Infrastructural Projects on Brahmaputra and its Security Implications for India

Yubaraj Das

Introduction

South Asia is a region of shared waters, history and rivers. Rivers keep us all alive, our culture alive. It sustains us and our agriculture. However, numerous conflicts have occurred over water control in the region. States are seen adopting a strategic lens rather than the notion of connectivity when it comes to water politics. Constructions of Dams, disputes over Water usage, deterioration of water quality, flooding due to release of excessive water are some of the leading causes of tension between riparian neighbours. The Brahmaputra river, which is a transboundary river in Asia. The river has its origin from the Angsi Glacier of the northern side of the Himalayas, Tibet where it is known as the Yarlung Tsangpo. Travelling southwards cutting through the Himalayan gorges it enters India via Arunachal Pradesh where it is known as Dirang or Siang River. Upon entering Assam, it is referred to as the Brahmaputra. Further it entered Bangladesh from Dhubri and merged with Ganga and Meghna River before finally emptying into the Bay of Bengal (Mahapatra & Ratha, 2015). The politics involving China, India, and Bangladesh were significantly influenced by this river. Diplomacy is frequently applied as a tool to enhance cooperation and negotiation, however States have failed to come to a mutually benefitting agreement on river water sharing with China’s reluctance to come to the negotiable table.

Literature Review

The geopolitics of transboundary rivers, particularly the Brahmaputra, has garnered increasing scholarly attention over the past two decades. The river’s significance spans hydrological,

ecological, economic, and strategic dimensions, shaping the power dynamics among China, India, and Bangladesh.

Several scholars emphasize the strategic dimension of water resources in China's regional policy. Chelleaney (2024) articulates how China's unique riparian position—being upstream to most Asian rivers—has enabled it to influence hydropolitics across the region. Amrith (2020) adds a historical-cultural lens, arguing that for China, rivers such as the Brahmaputra are not just physical resources but also symbolic tools of national rejuvenation.

The South–North Water Diversion Project (SNWTP), especially its proposed Western Route affecting the Yarlung Tsangpo (Brahmaputra), has been extensively analyzed. According to Aqua Tech (2024), this megaproject, rooted in Mao Zedong's developmental vision, aims to redirect southern waters to the arid north through massive canal networks. Bisht (2020) and Jeong (2015, as cited) interpret this as both a tool for internal consolidation in Tibet and a lever for external engagement with South Asia, reflecting Beijing's dual-use approach to infrastructural development.

From an Indian perspective, concerns primarily revolve around hydrological uncertainty and national security. Vivekanandan (2024) discusses the securitization of the Brahmaputra issue, especially with regard to flash floods and reduced downstream flow. The 2000 natural dam burst incident is often cited as a cautionary example of ecological vulnerability. Furthermore, Baruah (2012) and Hazarika (2022) underline how dams disturb sediment flows, fish migration, and local agricultural economies—particularly affecting Assam and Bangladesh.

River diplomacy is another major area of scholarly interest. Samaranayake and Wuthnow (2018) provide a comprehensive account of the bilateral and trilateral mechanisms developed over the years, such as the MoUs for data sharing between China–India and China–Bangladesh. However, they note that China's selective engagement—being more forthcoming with

Bangladesh than with India—creates a diplomatic asymmetry. Despite the establishment of Expert Level Mechanisms (ELMs) and hydrological agreements, the lack of a formal multilateral water-sharing treaty keeps tensions simmering (Ministry of Jal Shakti, 2023; Hussain, 2013).

In sum, the existing literature points to a confluence of environmental, strategic, and diplomatic factors that make the Brahmaputra not just a river but a contested geopolitical space. While there is ample documentation of the problem's technical and political dimensions, what remains underexplored is an integrated assessment of how Chinese infrastructural actions on the Brahmaputra simultaneously reshape India's ecological security and regional diplomacy.

Methodology

This research adopts a qualitative, multi-source, and analytical approach to assess the implications of China's infrastructural projects on the Brahmaputra for India's security and regional diplomacy.

1. Research Design

A descriptive-analytical design has been employed to explore both factual developments and their implications. The study does not aim to propose causal theories but seeks to understand linkages between Chinese infrastructural decisions and India's strategic responses.

2. Data Sources

Primary sources include:

- Official reports and MoUs from the Ministry of Jal Shakti (India)
- Statements from China's Ministry of Water Resources
- Parliamentary and media reports on Indo-China water agreements

Secondary sources consist of:

- Peer-reviewed journal articles (e.g., India Review, Asian Survey)
- Policy papers (e.g., Marine Corps University Press)
- Books and monographs by leading scholars (e.g., Amrith, Chelleaney, Baruah)
- Verified digital platforms such as Aquatech and Indiaspend

3. Analytical Framework

The study uses a three-tiered analytical framework:

Ecological Analysis: To examine the downstream impacts of Chinese dam construction, diversion, and sediment interruption on Assam's ecosystem and economy.

Strategic Analysis: Using concepts from geopolitical and realist theories, the study assesses India's perception of threats arising from Chinese control over upper riparian waters and its implications for national security and Northeast India's stability.

Diplomatic Mapping: Through timeline-based tracking of diplomatic engagements (2002–2023), the paper evaluates the effectiveness and limitations of bilateral and trilateral cooperation frameworks between China, India, and Bangladesh.

4. Limitations

The study is limited by language barriers in accessing original Chinese documentation.

Absence of real-time hydrological data from Tibetan Plateau restricts empirical verification.

Interviews or field visits were not conducted due to geographical and logistical constraints.

Chinese intention on Brahmaputra: The South- North Water Transfer project

China's distinctive position as a major riparian nation sets Asia's water maps apart. Unlike any other country globally, China acts as the primary riverbed for numerous nations. This unique position of China enhanced its capability to emerge as a key influencer in inter-riparian relations across Asia (Chelleaney, 2024). Historically, water has played a profound role in shaping China's destiny, beyond its practical utility. It symbolises freedom and serves as a vital ingredient in a nation's emergence from a century of humiliation under imperial powers (Amrith, 2020). China with its extensive network of over 1,500 rivers, covering a drainage area of more than 1,000 square kilometres, underscores the nation's geographical richness. Among these waterways, the Chang Jiang (Yangtze River), Huang He (Yellow River), Zhu Jiang (Pearl River), Huai He, Hai He, Liao He, and Songhua Jiang stand out as the seven principal rivers supporting more than 80% of China's population and cultivated land (Popov & Greer, 2023).

For the Chinese, The Brahmaputra holds an immense potential in meeting China’s hydropower ambition in Tibet. Over the past two decades, China has made significant strides in enhancing water resources in this region. This issue of water diversion in China first came up with the ambitious South- North Water Transfer Project which aimed to address the water scarcity concern of the Northern region of China by diverting water from the Southern rivers through Massive canal infrastructure projects, covering over 1,200 kilometres (Aqua Tech, 2024). This project has its roots in the vision of Chinese leader Mao Zedong. In 2002, Mao's vision started to come to fruition with the commencement of a major project featuring three main routes: the Central, Eastern, and the proposed Western routes. The Central Route, famously called the Grand Aqueduct, which draws water from the Yangtze River's tributaries to provide for Beijing (ibid).

The issue of water diversion in the case of Brahamaputra first came to public attention in 1999 when Jiang zemin announced China's Great Western Development policy that aimed at developing the western region (Bisht, 2020). This issue became popularised with the Great Western Extraction (GWE) which involved transfer of water from Tibet within the South-North water transfer project as a part of opening of the west and west east transfer project. China has also considered using water, energy and minerals as essential resources to develop the autonomous regions of Xinhiang, Tibet and Ningxia (Jeong 2015 cited by Bisht, 2020). This investment in water diversion by China as argued by many scholars serves two primary objectives: internal consolidation and external connectivity. Internally, the goal is to strengthen its presence in Tibet by transforming it into a hub of modernization capable of supporting economic activities in the region. Externally, the aim is to foster economic trade with South Asian neighbours, thereby positioning Tibet as a crucial strategic communication node.

This suggests that China's policies toward Tibet and projects on the Yarlung-Tsangpo are part of a grand strategic plan, creating a network of strategic nodes (Bisht, 2020). Over the past two decades, China has made significant advances in enhancing water resources in this region led by the Ministry of Water Resources. This initiative has resulted in improved access to clean drinking water for 2.39 million people and has provided electricity to approximately 360,000 Tibetan herdsmen, as per data from the People's Republic of China. This investment in water resource infrastructure in Tibet alone amounted to $4.87 billion by 2014 (Samaranayake & Wuthnow, 2018)

The Impact of Multipurpose Dams on Assam's Ecology and Economy

India’s worries about Chinese activity on Brahmaputra are twofold : too less (caused by water diversion projects such as the South-to-North Water Transfer Project) and the flow downstream

would be reduced; too much (when released by dams upstreams during the monsoon might trigger flash floods) (Vivekanandan, 2024). Though China claims that these to be ‘run of the river projects, India suspects that these could store water, thereby affecting the flow downstream (ibid, p.135-136). Further, it is believed that the dam China is planning in the Matuo on the Great bend will outstrip the Three Gorges dam in capacity. The flood caused by the bursting of a natural dam in 2000 that killed thirty and left 50,000 homeless in India only served to underline India’s fears as a lower riparian (Biba,2020 as cited by Vivekanandan, 2024, p. 136).

Thus, because of this riparian mistrust and growing insecurity between countries, the state is seen adopting a realistic lens and engaged in what (Chelleaney, 2014) called ‘Dam racing’ in order to have more control over the river. Further, Baruah (2012) and Hazarika (2022) highlight that a river, which is considered a body of flowing sediment as much as flowing water, if obstructed by these large dam projects, will have a negative impact on the floodplains for agriculture, upon which much of Assam's economy as well as Bangladesh depends (Baruah, 2012). Moreover, changes in water temperature and manipulation of water levels to meet power generation demands will reduce oxygen levels, adversely affecting fish migration and spawning habits (ibid). This will impact the diet of water communities living in and around the river who depend on the river for their daily food security. These multipurpose dams will destroy the aquatic fauna and flora that rely on the river for their sustainability, with the river dolphin population in Assam being a prime example (ibid).

Moreover, the lives of people in downstream areas will be significantly impacted, leading to economic insecurity in various ways. For instance, the country's transportation infrastructure will be dramatically affected, disrupting motor boats that transport people, domesticated

animals, crops, thatches, pottery articles, and forest products from one part of the region to another.

River Diplomacy Efforts Among Countries: Challenges and Failures

To further the relaxation of conflict, tension and mistrust. All the three countries have taken numerous steps in this regard. In 2002, the Government of India signed a MoU with China for the sharing of hydrological information on the Brahmaputra river during the flood season by China to India (Ministry of Jal sakti, 2023). In 2008 a technical expert group (TGE) was established to “draw up an action plan for establishing India’s user right on Brahmaputra and its tributaries coming from China" (Samaranayake & Wuthnow,2018, pp. 47). During the visit of Indian vice President Hamid Ansari to China, both countries signed the Implementation plan: Provision of Hydrological information on the Yarlung Zangbu/Brahmaputra River in Flood season by China to India (ibid.,Pg 56). Furthermore, another MOU was signed on strengthening co-operations on ‘Trans-Border River’ on 23th October 2013 through this agreement the scope of hydrological information of three hydrological stations was enhanced (Hussain, 2013).

During President Hu Jintao visit to India an Expert Level Mechanism (ELM) was formed to discuss the interaction and co-operation on the provision of flood season hydrological data. The last ELM was held at New Delhi in June, 2023 (Ministry of Jal sakti, 2023). For Bangladesh, over the years China has taken a liberal stand. It emerged as a reliable partner in extending Military, economic, diplomatic support. In 2008, China agreed to share hydrological data on the Brahmaputra. During a summit in 2010, the two countries decided to enhance collaboration in managing water resources, sharing hydrological data, controlling floods, and reducing disasters. China also pledged support to Bangladesh by aiding in riverbed dredging and providing training for personnel. Furthermore, in March 2015, both countries signed another

Memorandum of Understanding (MOU) focused on sharing rainfall data from the river's catchment area in China (which China does not share with India). This data would be valuable for improving flood forecasting in Bangladesh (Samaranayake & Wuthnow,, 2018).

This Chinese willingness to share hydrological information and provide assistance in river dredging led to good diplomatic culture between China and Bangladesh. Moreover, Beijing continues to assure Dhaka that it has no such plan of diverting the river (ibid. pp 93). For India, The close physical, historical, and political ties between India and Bangladesh significantly influence their bilateral relations, particularly concerning the Brahmaputra River (ibid., 63).In 1972, Indo-Bangladesh Joint River Commission (JRC) was established with a view to maintain a contract in order to ensure the most effective joint effort in maximising the benefits from the common river system. In 1996, Indo- Bangladesh opened up a new chapter of cooperation regarding the sharing of water of Ganges. Discussions have been continuing with Bangladesh for sharing of water from the river Testa and Feni (Ministry of Jal sakti, 2023).

Recently, India and Bangladesh has also signed the India - Bangladesh Protocol (IBP) which will revive the pre partition connectivity of Halide port of Kolkata with the Panda port in Guwahati via Dhubri (Assam) and Sirajganj in Bangladesh using the Ganga - Brahmaputra network (Assam Inland Water Transport Development Society). Bangladesh is also very much interested in multilevel co-operation to improve further cooperation between China - India - Bangladesh. As three of the countries lack a mutual multilateral agreement. Bangladesh sees water cooperation as opening up greater possibilities for regional integration such as through river navigation, with both India and hydroelectric power generation with India and China (Samaranayake & Wuthnow,, 2018)

Conclusion

Thus, The Brahmaputra River is an essential geopolitical entity that shapes the diplomatic relationship and politics of China, India, and Bangladesh. Its significance is undeniable in every aspect whether economically, culturally, or environmentally, among the three countries. The river has also been a source of tension, with China's ambitious water projects that concern India's Northeast and Bangladesh's lack of river water. However, despite challenges, efforts are being made through river diplomacy, such as sharing hydrological data and collaborative bilateral agreements, to ease the tensions and increase cooperation. These ongoing diplomatic engagements provide hope for resolving conflicts and promoting sustainable management through a more multilateral agreement for this vital transboundary river.

References

- *Amrith, S. (2020). Unruly Waters: How Mountain Rivers and Monsoons Have Shaped South Asia's History. Penguin Books.*

- *AQUA Tech. (2024, February 26). China's Water Diversion: Progress & Challenges. Aquatech. Retrieved June 21, 2024, from https://www.aquatechtrade.com/news/water-treatment/china-south-north-water-diversion-project*

- *Baruah, S. (2012, July 21). Whose River Is It Anyway? Political Economy of Hydropower in the Eastern Himalayas. Economic & Political weekly.*

- *Bisht, M. (2020, February). Brahmaputra and its Imageries: Strategising Sustainable Development. Institute of Chinese Studies.*

- *Chelleaney, B. (2024, July). Water, Power, and Competition In Asia. Asian Survey, 54(4), 621-650. https://www.jstor.org/stable/10.1525/as.2014.54.4.621*

- *Hazarika, S. (2022, July 8). River Reflections: Shifting Sands And Stressed Lives. Indiaspend. https://www.indiaspend.com/river-reflections/shifting-sands-and-stressed-lives-825312*

- *Hussain, W. (2013). MoU on the Brahmaputra River. IPCS. Institute Of Peace & Conflict Studies. http://www.ipcs.org/comm_select.php?articleNo=4149*

- *Mahapatra, S. K., & Ratha, K. C. (2015, Jan 1). Sovereign States and Surging Water: Brahmaputra River between China and India. Fondazione Eni Enrico Mattei.*

- *Ministry of Jal sakti. (2023, January 3). INDO-BANGLADESH COOPERATION | Department of Water Resources, River Development and Ganga Rejuvenation | India. Ministry of Jal Shakti. Retrieved June 21, 2024, from https://jalshakti-dowr.gov.in/indo-bangladesh-cooperation/*

- *Popov, I. V., & Greer, E. C. (2023, August). Yellow River | Location, Map, & Facts. Britannica. https://www.britannica.com/place/Yellow-River*

- *Samaranayake, N., & Wuthnow,, J. (2018). Raging Waters: China, India, Bangladesh, and Brahmaputra River Politics. Marine Corps University Press.*

- *Vivekanandan, J. (2024). Where we need water, we find guns instead": understanding the securitization of sovereignty claims on the Brahmaputra. India Review, 23(2), 134-153. https://doi.org/10.1080/14736489.2024.2324639*

Navigating the Murky Waters of State-Sponsored Cyber Warfare and Asymmetric Tactics in China

Puloma Pal

Introduction

The emergence of state-sponsored cyber warfare poses a serious moral conundrum with far-reaching effects in modern technologically connected society. With special emphasis on China, this article would explore the complex mechanics of negotiating the muddy seas of state-sponsored cyber warfare and asymmetrical cyber-tactical strategies. This research article would then revolve around digital warfare in the bigger picture of contemporary geopolitics. This research article would further emphasis on its importance as well as the changing nature of cyber warfare. From early cyber endeavours to the strategic incorporation of digital capabilities into military doctrine, it would trace historical growth of China. It would also lay the groundwork for a thorough examination of China's involvement in state-sponsored cyber operations.

The research article then explores the hazy boundaries of Cyber espionage for commercial gain and national security. A Case study would be used to highlight the moral dilemmas that China faces in its cyber operation. Furthermore, instances regarding China's Cyberattacks and its impact on targeted individuals would be used. The debate would delve into the nature of asymmetrical cyber warfare and evaluate its impact at international level. The assessment of these strategies emphasizes how urgent it is for nations to work together to reduce the risk associated with asymmetrical cyber warfare. The article also explores China's involvement in international security, highlighting the ways in which its technical breakthroughs are causing anxiety, especially in close neighboring nations such as India. In order to confront rising cyber risks and protect national interests, the paper highlights the need for proactive steps by analyzing the possible consequences of Chinese technical growth.

In short, this study in the form of a research article would provide insightful information about the moral quandaries and tactical difficulties presented by state-sponsored cyber warfare, using China as a case study. In order to successfully negotiate the complicated terrain of cyber warfare in the twenty-first century, it needs more awareness, teamwork, and ethical frameworks.

Literature Review

The academic and strategic literature on cyber warfare has rapidly evolved over the last two decades, paralleling the digitization of military capabilities and geopolitical competition. China's cyber strategy, in particular, has been a focal point of concern, due to its fusion of technological innovation with authoritarian statecraft and global ambition.

Scholars such as Jinghua (2019) and Handler (2023) highlight the doctrinal evolution of China’s cyber capabilities, especially through publications like The Science of Military Strategy and national white papers that formally integrate cyber power into military doctrine. The PLA's Strategic Support Force (SSF), established in 2015, represents China’s institutional commitment to developing integrated cyber, electronic, and space warfare capabilities.

Aitel et al. (2022) present a compelling analysis of China's Advanced Persistent Threat (APT) ecosystem, emphasizing groups like APT41 (Double Dragon), which blend state intelligence operations with economically motivated cybercrime. This aligns with Eftimiades (2018), who discusses China’s “dual-use” espionage strategy targeting both national security secrets and commercial intellectual property.

The convergence of civil and military technologies is another key theme. Fritz (2019) and Mallick (2022) discuss the concept of Military-Civil Fusion (MCF)—China's strategic framework that blends academic research, private tech innovation, and PLA modernization

goals. This mirrors Xi Jinping's ambition to make China a "cyber superpower" by 2030 (Montgomery & Ma, 2023).

In the broader geopolitical context, Ven (2023) and Proctor (2022) argue that cyber warfare now underpins modern hybrid warfare, with the Russia–Ukraine conflict providing a real-world template. These dynamics have led to blurred boundaries between peacetime espionage and wartime sabotage, as seen in the case of infrastructure attacks, AI-driven disinformation campaigns, and attribution challenges.

Lastly, Kuo (2024) and Fraser (2024) examine how China's digital expansionism—including AI, quantum computing, and global tech diffusion—creates strategic vulnerabilities for rival states like India. These developments raise urgent questions about digital sovereignty, critical infrastructure security, and the future of deterrence in cyberspace.

Collectively, this body of work underlines that Chinese cyber operations are not isolated acts of disruption but are embedded in a coherent, long-term grand strategy with asymmetric leverage at its core.

Methodology

1. Research Approach

This paper employs a qualitative and case-based exploratory research design, drawing on multidisciplinary insights from cybersecurity, strategic studies, international relations, and Chinese military doctrine. The focus is on descriptive analysis and strategic interpretation, rather than empirical testing of hypotheses.

2. Data Sources

The study relies on open-source intelligence (OSINT) and secondary data, including:

- Peer-reviewed academic publications
- Think tank reports (e.g., IISS, Carnegie, ORF)
- Cybersecurity advisories from threat intelligence firms and government agencies (e.g., US-CERT, HHS, Health Sector Cybersecurity Centre)
- Government white papers and doctrinal releases (e.g., China's National Cybersecurity Strategy, PLA doctrine)
- Reputed media and professional cybersecurity blogs (e.g., The Diplomat, BBC, Statista, DarkReading)

3. Case Study Method

A detailed case study on APT41's cyberattack on Air India (2021) serves as the empirical anchor. This event was selected for:

- Its high-impact operational duration (over 3 months),
- Its attribution to a Chinese state-linked actor (APT41),
- Its relevance to India's national cyber threat landscape.
- The case is analyzed along four dimensions:

  -Attack lifecycle and tactics (e.g., Cobalt Strike, Mimikatz)

  -Nature of exfiltrated data

  -Operational and reputational damage

  -Attribution and policy implications

4. Analytical Framework

The analysis uses a hybrid framework combining:

- Strategic Studies lens: to evaluate cyber warfare as an extension of statecraft and power projection.

- Cybersecurity threat models: to understand attack vectors, APT behaviours, and mitigation challenges.
- Geopolitical mapping: to position China's cyber strategy within the broader context of Indo-Pacific power dynamics.

5. Limitations

The study does not employ real-time threat forensics or technical vulnerability testing. Attribution in cyber warfare remains inherently complex and partially speculative. Limited access to Chinese-language primary sources may affect interpretation of intent.

Evolution of Cyber Warfare as a Strategic Concept

A larger backdrop of great power struggle and the increasing use of information technology in military operations have propelled the development of cyber warfare as a strategic concept. While cyber warfare was not a major worry in the 1990s, it became more significant as information technology became more vital to military operations. Cyberspace has emerged as a new and crucial arena for military conflict, according to the PLA Academy of Military Science's 2013 edition of *"The Science of Military Strategy."* (Tewari, United Service Institution, 2019) In 2015, China released its Military Strategy, which further cemented the position of cyber warfare in military doctrine by characterising cyberspace as a *"new pillar of social and economic growth and an emerging field of national security."* (Jinghua, Carnegie Endowment for International Peace, 2019)

China's cyber warfare capabilities have increased along with its military might and economic might. Chinese cyber warfare now employs university students and nationalistic hackers in addition to the PLA, forming a *"whole of nation"* strategy. By adding assaults on satellites and

space warfare to its offensive activities, it has also raised cyber warfare to a level of strategic importance (Tewari, China’s Cyber Warfare Capabilities, 2019).

China's hybrid conflict and information warfare strategies are closely linked to its cyber warfare plan. To weaken an enemy's capabilities, it employs cyber espionage to find vulnerabilities and get information that may be used in wartime. It targets vital infrastructure, including banks, financial institutions, electricity, water, and sewage systems, railroads, and telecommunication networks (Tewari, United Service Institution, 2019). China also uses information operations and cyberattacks to sway public opinion, cloud the judgment of foreign leaders, and create circumstances where the boundaries between peace and conflict are blurred.

A) Cyber warfare in Modern Geopolitics:

Modern geopolitics has become significantly influenced by cyber warfare, as nation-states use digital capabilities more and more to further their strategic objectives. A new age of hybrid warfare has begun with the Russia-Ukraine conflict (Ven, 2023), which has starkly demonstrated how cyber operations have become effectively linked with conventional military measures (Cyber Threat IntelligenceTeam, 2023).

The integration of cyber and kinetic actions has become one of the most prominent themes. (Ven, 2023). Cyberattacks and military offensives are carefully synchronized to optimize their combined effect. This resulted in a mutually reinforcing effect that increases the potency of both strategies. With the deep consequences of the intersection of the digital and physical spheres, this cooperation represents a fundamental advance in the conduct of conflict. The escalation of damaging cyberattacks represents an additional noteworthy development. Malware with the intent to permanently erase data or render computers unusable has proliferated. Such assaults raise the stakes of cyber warfare by interfering with operations and

causing permanent harm that makes recovery attempts more difficult. Additionally, hybrid cyber-influence efforts have gained prominence (Cyber Threat IntelligenceTeam, 2023).

These days, malicious actors utilize the internet to manipulate public perceptions and erode institutional trust through dishonesty, disinformation, and sophisticated disinformation campaigns. To sow division, warp perceptions, and undermine the social fabric of the countries being targeted, psychological warfare is employed in tandem with actual acts of violence.

There is an additional element of complication when non-traditional players are involved. The distinction between politically motivated digital operations and illegal activity is blurred by cybercriminals working along with nationalist activists and challenging governments. Their participation makes it difficult to establish detection and reaction strategies. It also increases the number of organisations involved in cyber warfare. Due to their involvement, attribution and response plans become more challenging to implement and the number of entities engaged in cyber warfare. (Cyber Threat IntelligenceTeam, 2023).

In Contemporary times, the hallmark of cyber warfare involves piercing the critical infrastructure. There are some significant risks to the safety and security of the public when critical services like the electrical grid, healthcare facilities and water supply are usually attacked. These interruptions are deliberate and often done to terrorize the general public. These intentional cyber-attacks seeks to endanger the underscore strategic significance of cyber defences in modern combat (Ven, 2023). Strong cyber defences, international collaboration, and a global approach to combating cyber threats are critical as cyberspace increasingly serves as a theatre of war for geopolitical conflicts (Townsend, 2023). Given the confluence of geopolitics and cyberspace, a comprehensive and collaborative approach is required to safeguard national interests in this digital age. The international community cannot hope to manage the threats and handle the obstacles presented by the constantly changing terrain of

cyber warfare without coordinated efforts and shared comprehension (Cyber Threat IntelligenceTeam, 2023).

B) Cyber warfare in Modern Geopolitics: A Transformative Force

The use of cyber warfare has transformed international relations, power dynamics, and government interaction and protection. It has become a critical and inventive component of contemporary geopolitics. A multitude of viewpoints emphasise its immense significance and show how crucial it is to modern global politics. The major significance of cyber warfare in the Modern Geopolitics can be-:

1. **The Modern hybrid warfare methods**. This method includes cyber warfare as a key component. It is because it smoothly integrates with conventional military operations. With synchronized cyberattacks, a country's Critical infrastructure can be seriously compromised. This may lead to generalised disorder without the necessity for a military intervention. The countries are able to attain the tactical goals with less direct conflict because of this non-kinetic technique (Proctor, 2022).
2. In contrast to conventional warfare, **the Global Reach of cyber warfare** is just not limited by physical location. The cyberattacks have become a global danger to national security. This is because they may be launched from almost anywhere on the globe. This worldwide reach highlights how ubiquitous and persistent cyber dangers are, calling for a thorough and well-coordinated multinational response (Proctor, 2022).
3. The **Strategic significance of cyber warfare** encompasses the possibility of a catastrophic *"Cyber-Pearl Harbor,"* has been extensively discussed. It is still, however, a very powerful instrument that countries may use to exercise control and exert influence. Through cyber operations, nations can preserve plausible deniability while undermining the political stability, public opinion, and essential facilities of their opponents (Ven, 2023).

4. Information manipulation, intelligence collection, and communication disruption are all made possible by cyber operations at **the tactical and operational levels**. These talents offer significant advantages when dealing with conventional and unconventional warfare circumstances, having the potential to significantly influence the course of battles (Schulze, 2020).
5. By using previously unheard-of access to private information, **cyber espionage** gives countries the ability to shape diplomatic ties and get an advantage in geopolitical discussions. The limits of statecraft and spying have been redefined by the capacity to get strategic intelligence surreptitiously without physical interference (LORELEI, 29923).
6. As **cyber warfare** has increased, cybersecurity diplomacy has become an increasingly important area of international relations. Negotiating cyber rules and working together to improve collective security is becoming more and more common across nations. By creating a structure for ethical state behavior in cyberspace, this geopolitical initiative seeks to reduce the likelihood that a dispute would escalate (Ven, 2023).
7. **Critical infrastructure** and industrial sectors are also seriously threatened by cyber warfare. Prominent cyberattacks targeting *supply chains*, *financial institutions*, and *energy grids* underscore the pressing necessity for strong cybersecurity protocols in public as well as private domains. Preserving these crucial resources is necessary to keep the country stable and economically resilient (Industrial Cyber, 2024).

To sum up, we can say that cyber warfare has radically changed the current geopolitical environment and made cybersecurity a top concern for all countries. The future of international politics, technology, and strategy all intersect in this intricate and multidimensional field, influencing both diplomacy and global security. Cyber-dangers are always evolving, which emphasises the need for constant adaptation and cooperation to protect the globalized society.

State Sponsored cyber warfare – In Dragon's Style

China has developed strong cyber warfare capabilities over the years. The development is mostly made in its national security and achieves its strategic objectives. The main aim to do such rapid and fast development is just to become the worldwide internet giant. Now seen as a crucial element of its national strength, the government of China has made large expenditures on advancing its cyber warfare capabilities. For example, the Chinese government's technology's spread. In adversary countries' networks, China has actively participated in the dissemination of its technology. This may include computers, laptops, modems, and telecommunication devices. This is accomplished by implanting malware, Trojans, and viruses into these devices. These viruses have the capability to corrupt sensitive or confidential data and damage or destroy Critical infrastructure (Tewari, 2019).

China has adopted a comprehensive national strategy for cyber warfare. This strategy consists of university students acting as cyber warriors and patriotic hackers. These hackers/students often collaborate with the People's Liberation Army. China may undertake cyber operations by utilising its extensive resources and skills through the implementation of the "Whole of Nation" concept.

The Dragon's cyber warfare approach is centered on causing disruption and destruction through the targeting of vital infrastructure, the exfiltration of private data, and the employment of intelligence-related tactics to influence the actions and choices of adversaries (Tewari, 2019).

The Chinese leadership has shown that it is prepared to showcase power and intimidate enemies via cyber capabilities. Also, to improve its cyber operations, China has been actively pursuing the development of AI. Artificial intelligence has a potential to enhance malevolent cyber operations by facilitating quick device vulnerability analysis, customised phishing lure generation, and improved malware. The Dragon's desire is to rule the AI world by 2030

(Montgomery & Ma, 2023). Hence, probably what will motivate it to attempt to acquire AI technology from nations around the Globe?

Statecraft and cybersecurity are closely related in China. As a major tool of national power, cyber power is seen by the Chinese government, and President Xi Jinping has made it clear that he wants to turn China into a "cyber superpower" through home-grown innovation. China's drive for leadership has produced a multifaceted, very skilled cyber threat, from sophisticated APT operations to laws and policies that create data vulnerabilities. Around 40 separate APT organisations have been identified as active in government and cybersecurity industry reports. This indicates a wide range of entities that China has that are linked to state-sponsored or authorised hacking. These groups have ties to the PLA and the Ministry of State Security (MSS). Although, the majority of them merely have ties to China in terms of victimisation, infrastructures, and instruments (Kuo, 2024).

Now, the rapid advancements in China’s technology may be helpful to China but are they helpful to the world? What consequences does China's technological advancement bring to International Cybersecurity? China's digital abilities are a serious danger to cybersecurity worldwide, especially for nations with which it has strained relations. Serious concerns over the possibility of cyber warfare and the requirement for nations to have strong cyber defenses have been raised by the Chinese government's readiness to utilise technological resources to project power and intimidate enemies (Kuo, 2024).

In a nutshell, China has adopted a comprehensive strategy for state-sponsored cyber warfare that involves the entire nation and makes use of its considerable resources and experience. China's approach to cyber warfare is centred on causing chaos and destruction, and the use of AI will probably improve its capabilities (Montgomery & Ma, 2023). Significant ramifications for international cybersecurity result from this, emphasising the necessity for nations to build

strong cyber defences and collaborate internationally in order to counter China's rising cyber threat (Kuo, 2024) (Tewari, 2019).

HISTORICAL OVERVIEW

In China, scholarly discourse on cyber warfare started in the 1990s, with an emphasis on information warfare. China modified its military strategy guidelines in 1993 to emphasise winning local conflicts with contemporary technologies, following the US military's lead in the Gulf War. A revision to the PMS for the military was made in 2004 to "winning local conflicts amid circumstances involving informationization. “When the Chinese military first took a comprehensive approach to cyber warfare, it was in the 2013 edition of "The Science of Military Strategy”.

Cybersecurity was also included in the 2015 Ministry of National Defence report, which defined it as a new area of national security and discussed security risks to its computer infrastructure. China's stance on cyber warfare is consistent with its military doctrine, which is adjusted in response to changes in the environment of national security, internal circumstances, and actions of foreign armed forces (Jinghua, What Are China’s Cyber Capabilities and Intentions?, 2019) (Handler, 2023). Over the past few decades, China's role in cyber operations has changed significantly -:

1. China began its attempts to digitise later than other countries but advanced quickly as the Internet spread around the world in the early 1990s. China was the country with the most Internet users worldwide in 2008. China's pursuit of cyberspace expanded quickly as a result of what it saw in American military activities, beginning in 1991 with Operation Desert Storm.


GULF NEWS
LATE EDITION
WAR IS ON
Liberation of Kuwait has begun – U.S.
Iraqi targets hit in 'Desert Storm'
Dollar soars
SANGEAN

(Source: Gulf News, Article titled- Iraqi invasion of Kuwait and Gulf War, through the pages of Gulf News, dated: August 03, 2020)

2. China began to emphasise cyberspace as a critical front in its conflict with major rivals and enemies like the US and the West in general, by 2013. By updated its cyber goals, China has made espionage, loss of intellectual property, confidential data, state secrets, and offensive capabilities, a key component of its strategy. These strategies are for attaining information dominance (Aitel, et al., 2022).

Picture 1

Picture 2

*(Source: **Picture 1;** US Accuses China of Using Criminal Hackers in Cyber Espionage Operations, Article on DarkReading; **Picture 2;** President Obama, Chinese President Xi Jingping Announce Agreement to Stop Hacking, Article at US News)*

3. An American corporation, Mandiant, asserted in *February 2013* that the *Chinese force was solely accountable for hacking Critical infrastructures, government agencies, and various companies in America*. Many people view the China-US cyber espionage conflict under the Obama administration as an effective example of crisis handling. China is nevertheless held accountable for cyberattacks on public and commercial organisations in the United States, India, Russia, Canada, and France, even if Beijing disputes any involvement (Handler, 2023).

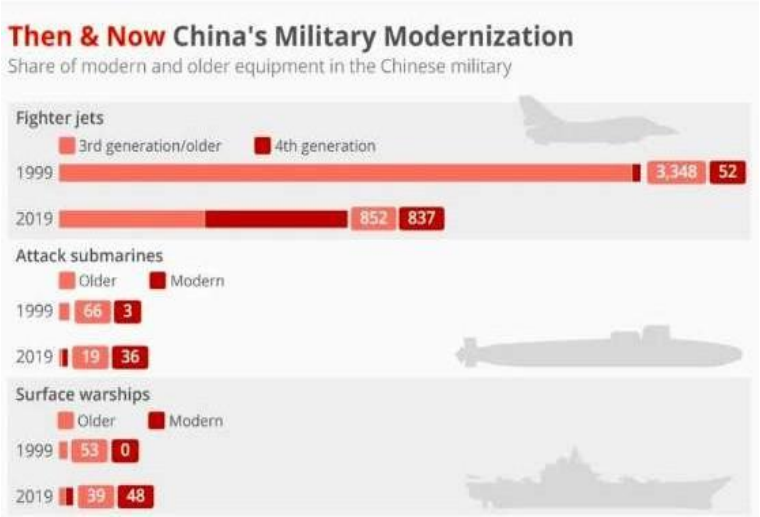
4. China has acquired foreign military technologies. Therefore, China is expanding its cyber skills and military technological powers. By enhancing the cyber warfare awareness, enhancing information networks for military training, and constructing digital and virtual labs and advanced educational facilities, it backs the "Informatization" of the armed forces. China is 'harvesting the expertise of its private sector' and gaining access to Microsoft source code to strengthen its cyber capabilities, both offensive and defensive. The majority of reports on China's ability to wage cyber warfare have not been verified by the Chinese government (Handler, 2023).

China’s Military Civil Fusion

By combining resources and working together on research and applications, this strategy seeks to foster a more intimate working relationship between the military and civilian sectors. MCF is carried out in a variety of ways, one of which is through the Central Military-Civil Fusion Development Committee (CMCFDC), which was founded in 2017 and is responsible for planning and executing MCF (Fritz, 2019).

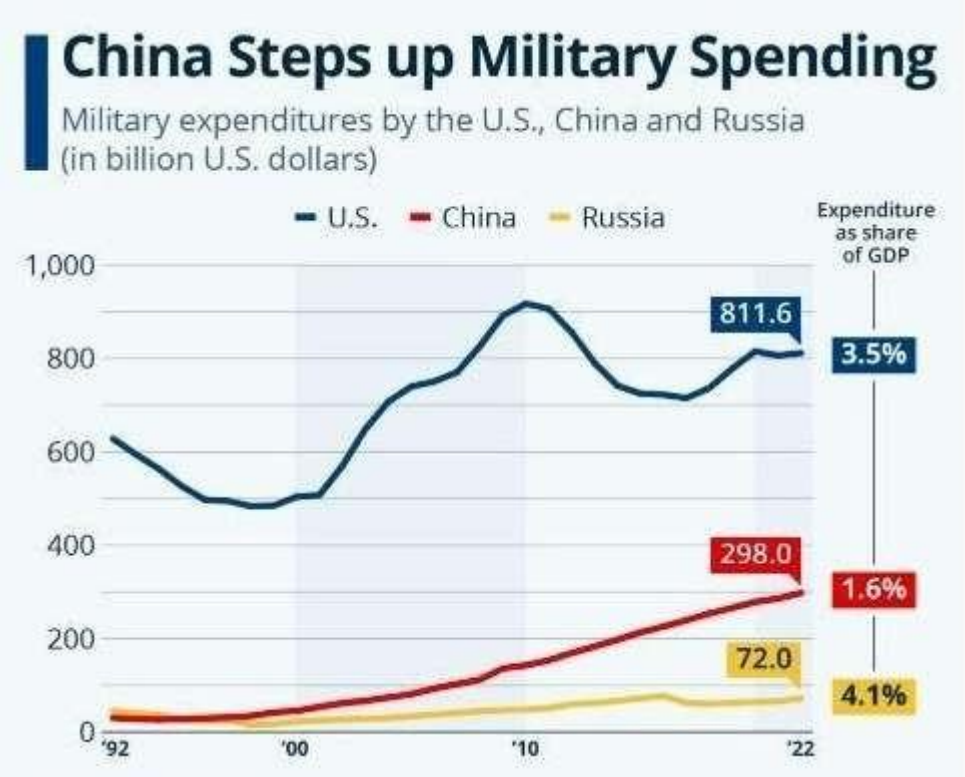
Hu Jintao, who first introduced the word **"Military-Civil Fusion"** in the late 1990s. The word Military Civil Fusion or MCF can be defined as a means of coordinating between the Civil and Military domains. But over a period of time the concept of MCF changed and evolved. Today, this concept is replaced with the term "civil-military integration" (CMI). These drastic changes

occurred during Xi Jinping's administration. With a strong focus on promoting the integration of the military and civilian sectors, the shift from CMI to MCF indicates a more comprehensive and fair approach for civil-military interactions (Fritz, 2019).



(Source: Statista is licensed under CC BY-ND 3.0.)

China has become a worldwide leader in a number of areas, particularly defence and technology, thanks in large part to MCF. But other countries, especially the United States, are worried about China's ability to obtain and appropriate Western technologies as a result of this policy. In response, the U.S. government has implemented steps to limit Chinese access to specific technologies and has published definitions of MCF that highlight the potential for technology transfer. A key element of China's national development objectives is the Military-Civil Fusion strategy, which aims to promote more collaboration between the military and civilian sectors in order to spur technical innovation and military modernization. A crucial component of China's ambitions to lead the world in science, technology, and military might, despite the strategy's unease among certain other countries, is its implementation (Mallick, 2022) (JOSHI, 2023).



(Source: SIPRI and Statista is licensed under CC BY-ND 3.0.)

Key Cyber Strategy

There are many important strategies that China came up with. For example, China's focus on Cyber Situational Awareness. In this campaign, China keeps an eye on and analyzes cyber activity both inside and outside its borders (Jinghua, Carnegie, 2019). These kinds of efforts help in improving the situational awareness in the field of cyber. China also has a strong emphasis on cyber defense. With a particular emphasis on defending the country's Critical information infrastructure or CII and preserving national security (Jinghua, Carnegie, 2019). China intends to use its cyber skills to assist other countries in their cyber activities, such as international collaboration and the establishment of a positive online culture. Improved cyber governance is required, and this includes putting the Cybersecurity Law and the Juvenile Online Protection Regulations into effect, according to China's National Cybersecurity Strategy.

China is also a cyber-resilient nation. This resiliency was developed over time. China wants to improve and work more on its cyber resilience (Kuo, 2024). To do this, it will create a unit devoted to cyber resilience. This unit would be led by a person with experience in both business and IT, and it will put strict identity and access management controls and Zero Trust security frameworks into place. With the goal of turning China into a ***"Cyber Superpower"*** through domestic innovation, China's authorities view cyber power as a crucial tool of national strength. China has carried out extensive cyber operations overseas (Kuo, 2024). These operations have a goal of obtaining intellectual property, gaining political clout, engaging in state-on-state espionage, and putting itself in a position to cause disruption in the event of future conflict. To guarantee the security of CII, China's National Cybersecurity Strategy calls for the extension of the cybersecurity review regime (Kuo, 2024).

(Source: Global Cyber Bites, Article by Lucky Ogoo, LinkedIn)

China is a strong proponent of international collaboration in cyberspace, vigorously pushing for the globalization of Internet resources and endorsing UN programs. China invest, spread and develops cybersecurity education and training. Recognizing that a significant internal

restriction is the low importance that China's educational system and training institutions place on cyber-security capabilities, China seeks to enhance these areas. With an emphasis on both offensive and defensive capabilities, as well as on both local and international development, these policies show China's all-encompassing approach to cyber operations (IISS, 2019).

The Blur line between cyber espionage for national security and Economic Gains

It can be quite difficult to distinguish between China's commercial interests and its use of cyber espionage for national security. China engages in various cyber espionage operations for a range of objectives, including economic gain, national security, and geopolitical objectives.

China focuses on the defence of the nation. The main goal of China's cyber espionage efforts is to get sensitive data on military technologies, space capabilities, and other critical sectors. China utilizes this knowledge to improve its military capabilities, especially in the domains of autonomous robots, hypersonics, avionics, and naval systems (Eftimiades, 2018). The National Security Strategy of China poses a significant emphasis on cyber espionage, as seen by the establishment of the PLA's Strategic Support Force in 2015. This force is committed to cyber, space, and digital warfare (Eftimiades, 2018).

China wishes to develop themselves in terms of industry and economy. To achieve this, China had come up with a plan. Its plan prioritizes the acquisition of various evidence and other materials. These materials and evidence can be trading secrets, intellectual property, or other economic data. These confidential and sensitive material China gathers is through its cyber espionage operations. This covers technological theft pertaining to materials research, sophisticated manufacturing, and consumer market information. Cyber espionage has substantial economic rewards. Its estimates indicate that China's economic espionage efforts cost the US economy at least $320 billion annually (Eftimiades, 2018) (Seth & Priyandita, 2023).

A famous strategist, army general in China – Sun Tzu once said – *"All men can see these tactics I conquer, but what none can see is the strategy out of which victory is evolved."* Another example we can mention here is Napoleon Bonaparte.

He once said that, *if someone wishes to maintain its superiority then, one must change its strategy every ten years*. Both Napoleon Bonaparte and Sun Tzu, who were great strategists in their prime time, focused on making strategies. If we talk about China in this regard, it also stresses more on building strong and effective strategies. Defense is the planning of an attack on China's geopolitical objectives. For example, the desire to balance off the military might and economic might of the United States, also motivate its cyber espionage efforts. China wishes to become less reliant on foreign technology. It wants to become more competitive with the US by obtaining technology and sensitive information (Fraser, 2024).

In short, we can say that it's quite difficult to differentiate between China's commercial interests and its use of cyber espionage for national security. China pursues a number of objectives through its cyber espionage efforts. These objectives may include economic gain, national security, and geopolitical goals. As these boundaries become more blurred, it becomes more apparent how intricate China's cyber espionage operations are and how urgently these problems need to be addressed.

Case Study

Active since 2012, APT41 is a Chinese State sponsored cyber gang. As per reports, it is believed that this group has been in contact with the Ministry of State Security (MSS) of China. The APT group after 2012, also known as Double Dragon, had orchestrated many cyber-attacks across the globe. These cyber-attacks were majorly targeted USA and its tech firms, Healthcare infrastructures and Manufacturing sectors (Health Sector Cybersecurity coordination Centre, 2023) (Team Cyber Pacific, 2023). The Double Dragon or APT staged a sophisticated

cyberattack against an Indian airline named Air India. This incident took place in June 2021. The security and daily operations of the airline were significantly impacted by this hack, which lasted for over three months.

Originally, this attack first began in the month of February same year, a device named SITASERVER4 was infected. This server was connected to a server used for command and control running Cobalt 2020 over Air India's network. By using deft techniques to get passwords and perseverance, APT41 agents were able to penetrate the larger network and take control of more than 20 machines. In less than twenty-four hours, they collected about twenty-four megabytes of data from five devices by using hash dump and Mimi Katz methods to extract sensitive data, such as passwords and NTLM hashes, from local systems. The group's capacity to operate quietly and inflict tremendous harm over a lengthy period of time was demonstrated by this operation (CNBCTV18.com, 2021).

Air India suffered severe consequences that included interruptions to operations, network intrusion, and data exfiltration. Critical information was extracted as a result of APT41's operations, which may have opened the door to more network access and operational interruptions. Because of APT41's well-planned strategies, the attack's protracted duration, and its significant effects on Air India, this case study is essential. To effectively address such attacks, it emphasises the need for advanced threat identification, ongoing monitoring, and a well-thought-out incident response strategy. The attack on Air India by APT 41 is a clear illustration of the complex and dangerous nature of state-sponsored cyber warfare, highlighting the vital role that preventive cybersecurity measures play in defending against such hostile actions.

Asymmetric warfare

Asymmetric warfare is a military tactic. When a country doesn’t know about its opponent

country's strengths and weaknesses and still decides to fight, it is known as Asymmetrical warfare. Usually, this kind of warfare techniques are used against terrorism and insurgency. This is because the army of the country doesn't know how well the terrorists are trained, how much weapons they have etc. In such cases, the military uses Asymmetrical warfare to fight the enemy.

It is said that the Asymmetrical warfare tactics evolved after World War 2 and during the Cuban revolution which took place from 1953 to 1958. But if we trace this term back to ancient civilization, there are evidences that can be found where our ancestors have been using Asymmetrical warfare tactics during war. For instance, during the 2nd century BCE, the Saka's, who were a tribal community, used such techniques to harass the soldiers of the Mauryan Empire. The Saka's who were expert in archery and cavalry, allied with local rulers and exploited the political instability of the Mauryan Empire after the death of Ashoka (Lal, 2018).

Another example we can quote here about Alexander the Great and his attacks/invasion of India. There are many records that can be found on pages of history where Alexander the Great faced fierce opposition from the Indian kingdoms, especially from King Porus of Paurava, who had a large army of infantry, cavalry, chariots and elephants (Chehtman, 2022).

Questions here arise: is cyberspace becoming a new field for war?

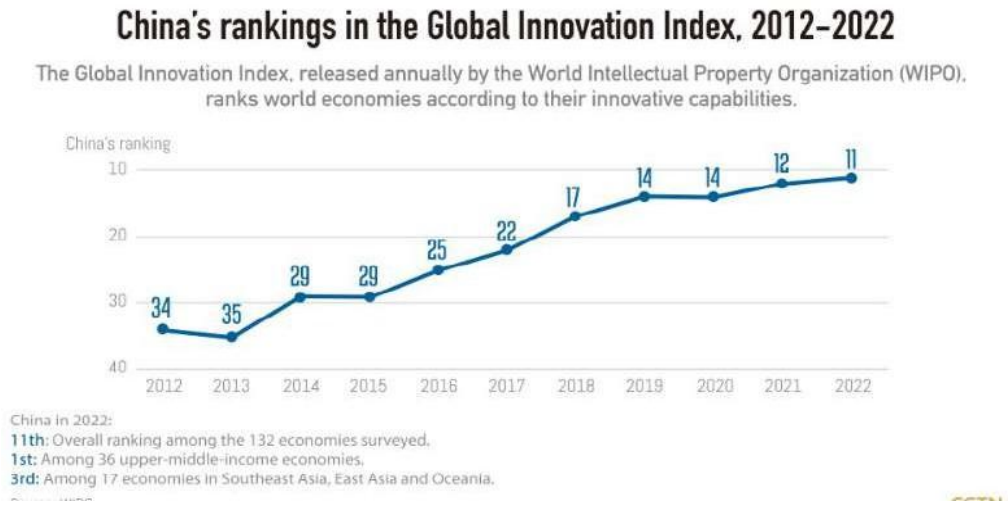
Cyberspace has indeed become a significant arena for conflict, with nations recognizing the importance of digital warfare alongside traditional military operations. The use of cyberattacks to target crucial infrastructure, such as power and communications systems, is a growing aspect of modern warfare. These attacks can disrupt the activities of a state or organization, leading to significant economic and social impacts.

For example, recent conflicts have seen allegations of state-sponsored cyberattacks that aimed to weaken enemy capabilities by causing widespread disruptions. The digital battlefield is now

as critical as the physical one, with cyber operations being integrated into military strategies. This shift reflects the evolving nature of conflict in the 21st century, where technological advancements have opened new fronts for nations to assert power and protect their interests.

China's technological advancement, a threat to India?

China has achieved great strides in the field of Science and Technology in the last numerous decades. This has helped China's frugality and also developed its manufacturing. China's impact on scientific exploration has also improved over a period of time. For illustration, China's Global Innovation Index and The National Innovation Index Report has placed China to 12th place in 2023. Before, China was placed at 34th rank. As per Global Times, China awarded 921,000 inventions, a patent instrument in time 2022. Piecemeal from patents, the publication of Scholarly works in these fields was recorded to be around 360,000 in foreign journals (Dzodin, 2022) (MCNICOLL, 2023). Major technological advancements are still being made in China, as substantiated by the completion of a moon charge, new uses for aerospace operations, the homegrown C919 large passenger aircraft, and the addition of the BeiDou Navigation Satellite System in the International Civil Aviation Convention norms.



(Source: Article at CGTN)

China is organising and promoting the structure of scientific and technology invention centers in a comprehensive manner. China's value contributed in high- tech manufacturing grew by 2.7% in 2023, making up 15.7% of artificial businesses larger than the needed size. Also, the investments in the high- tech sector grew by 10.3% in the former time (Dongmei, 2024). China has been putting a lot of trouble into low- carbon and green transnational cooperation (He, et al., 2020).

While engaging similar sweats, it also engaged itself with global climate governance. China has been working on erecting a new energy system more snappily. This New energy system would include, photovoltaic, wind power, ultramodern energy storehouse, and innovative energy buses (World Bank, 2024). The R&D spending of China also went up latterly from 1.03 trillion Yuan in 2012 to 3.3 trillion Yuan in 2013 (Dongmei, 2024).

Given how fleet technology is advancing, India has been expressing its serious concerns about the rising influence of China in global affairs. India faces several challenges as a result of China's specialized improvements, particularly in the fields of cybersecurity, amount computing, and artificial intelligence. China's fast technological improvements have made it a crucial part in the global IT geography (Dongmei, 2024).

The country has made some significant advancements in the field of cybersecurity, AI, and amount computing. This kind of advancement has frenetic demitasse to be in a position where it can make major metamorphosis or impact Global security. As a significant player in the region, India must nearly cover these developments and assess how they may impact public security.

Cybersecurity is a largely important topic. China poses a direct trouble to India’s public security. This trouble is majorly through its expansive cyber spying sweats and sophisticated cyber capabilities. India's cyber structure might be jeopardised by the capability to conduct sophisticated cyberattacks; therefore, the nation has to fortify its defences and remain watchful.

Quantum computing is another arena where China’s inventions have significant influence. China has a significant strategic advantage due to its capability to transfigure data encryption and cryptography through its improvements in this field. India must both keep up with these developments and enhance its own computing capabilities to maintain its security posture and safeguard critical data. The fast development of artificial intelligence is a major concern across the globe.

However, the development is growing briskly, if we talk about rapid-fire development of AI in demitasse. China may have a strategic advantage in military operations as well as operation due to its capacity to produce and use advanced AI systems. But to secure its strategic objects and maintain public security, India must make countermeasures and bolster its AI capabilities.

Hence, we can say that India is getting increasingly concerned about China's specialized progress in light of world security. India must exercise caution in view of the possible dislocations in artificial intelligence, amount computing, and cybersecurity. It's imperative that India fortifies its cyber structure, fends off pitfalls from amount computing, and gets ready for AI problems in order to lessen the pitfalls associated with China's specialized superiority.

Recommendations

Contemporary Cybersecurity issues that are of utmost importance may include, China’s cyber warfare Advanced Persistent Threat or commonly known as APT’s and Private- Public Partnership or PPP’s.

The employment of AI and ML for the threat actor profiling and APT detection, tracking threat actors and identifying the APT’s, now require the use of AI and ML. The APT’s are highly skilled cyberattacks which are mostly intended to go unnoticed. These kinds of attacks usually stay hidden and unnoticed for a very long period of time. A large amount of data can be analyzed by algorithms that use artificial intelligence and machine learning to identify new

trends and abnormalities that can point to an APT attack. In order to detect threats specifically and provide context for diverse behaviors, Flare's Threat Actor Profiling, for example, uses generative AI to find commonalities across multiple communication services. Similar to this, by spotting odd patterns and behavior, machine learning models may be used to evaluate data that is at rest and identify dangers.

Public-Private Collaboration in Cybersecurity can also be beneficial. The advancement and development of cyber defences, public-private partnerships, or PPPs, are very crucial for countries. To better safeguard the Critical infrastructure and national security, PPP should entail cooperation between public and private sectors as well as other interested parties. This can take place in the form of information, resources, and expertise sharing.

Another initiative we can talk about here is from Japan. The initiatives from PPP are essential to safeguarding Critical infrastructure in Japan. The creation of the Cyber Security Strategy Headquarters and the National Centre of Incident Preparedness and Strategy for Cybersecurity (NISC) are two of the initiatives the nation has put in place to support PPP in cyber defence. Improving cyber defence systems is essential for maneuvering through the intricate terrain of asymmetrical cyber tactics and state-sponsored cyber warfare. This is where AI and ML come into play, since they enable quicker reaction times to new threats and provide real-time threat intelligence. Furthermore, PPP can facilitate the dissemination of best practices and threat intelligence among involved parties, enhancing the overall posture of cyber defence. The creation of stronger defences and incident response plans may also be aided by this cooperation.

The Bottom Line

This research paper attempts to explore the complex and twisted dynamics of State Sponsored Cyber Warfare and tactics involved in Asymmetrical Cyber Warfare in Modern geopolitics. This paper delves into the moral dilemmas and tactical challenges posed by state-sponsored

cyber activities. The paper consists of a case study on China. Examining China’s Historical development in Cyber Operations helps clarify the blurry lines that separate the cyber espionage for profit from national security. This research paper also examines the characteristics of asymmetrical warfare and its worldwide ramification, highlighting the critical need for International collaboration to reduce related dangers. As more and more we move to the future, the warfare techniques, tactics, goals, objectives and strategies have changed rapidly. Cyber warfare is becoming a more and more important instrument in today’s geopolitics for nation states to accomplish their strategic goals. The conflict between Russia and Ukraine serves as an example of how hybrid warfare has emerged and how cyber operations are now easily combined with conventional military strategies. A recurring topic is the synchronization of Cyber and physical acts, wherein a well-planned cyberattacks and military offensives maximizes their combined effects.

Another significant development is the rise of destructive cyberattacks, with malware designed to permanently erase data or incapacitate systems becoming more prevalent. Hybrid cyber-influence campaigns have also gained traction, where malicious actors manipulate public opinion and erode institutional trust through deception and disinformation. The lines between politically motivated digital operations and criminal activities are increasingly blurred. This has further complicated the detection and response strategies for governments. Today, cyber warfare often targets critical infrastructure—such as power grids, healthcare systems, and water supplies—posing severe threats to public safety and security.

Global cybersecurity is significantly impacted by China's technical achievements. This emphasises how important it is to have strong national defense and international cooperation in order to combat China's increasing cyber threat. In the 1990s, China's intellectual community developed an interest in cyber warfare, originally concentrating on information warfare. China started its digitization efforts later than many other nations, but when the Internet spread over

the world in the early 1990s, it advanced quickly. By 2013, China had come to see cyberspace as a key front in its geopolitical competition with the US and other major Western powers.

China has increased its cyber capabilities and military technology prowess in addition to acquiring Western military technologies. Through strengthening cyber warfare awareness, building digital and virtual labs along with cutting-edge educational facilities, and expanding information networks for military training, it promotes the "Informatization" of its armed forces. In addition, China places a high priority on resilience to cyber threats. To this end, it has established specialised units to improve situational awareness and is putting strict access and identity management rules in place in addition to Zero Trust security structures.

China advocates for international collaboration in cyberspace, actively promoting the globalization of Internet resources and endorsing UN initiatives. It invests in and disseminates cybersecurity education and training, addressing the internal challenge of the relatively low emphasis placed on cybersecurity skills within its educational and training institutions. China's cyber espionage efforts are intricate and multi-dimensional, targeting a range of objectives from economic gains to national security and geopolitical ambitions. These efforts primarily aim to acquire sensitive information on military technologies, space capabilities, and other critical sectors. Such data enhances China's military capabilities, particularly in areas like autonomous robotics, hypersonic, avionics, and naval systems.

Hence, at the end, this paper presents a deep and comprehensive analysis of the role of China in state-sponsored cyber warfare. This research paper also talks about the broader implications of asymmetric cyber-tactics in International politics. The paper then talks about rising International cooperation. It also suggests the need to address the challenges and vulnerability in the coming future.

References

- *Aitel, D., d'Antoine, S., Bulazel, A., DeSombre, W., Garcia-Camargo, I., Garwin, T., ... Wagner, A. (2022). China's cyber operations: The rising threat to American security. New York, NY: Margin Researcher. Retrieved April 29, 2024, from https://margin.re/content/files/2023/01/China-s-Cyber-Operations-Full-Report.pdf*

- *Chehtman, A. (2022, January 1). Asymmetrical warfare. In A. Chehtman, Chehtman, Alejandro (pp. 55-65). Cham, Switzerland: Palgrave Macmillan. Retrieved February 29, 2024, from https://link.springer.com/referenceworkentry/10.1007/978-3-030-77954-2_27*

- *CNBCTV18.com. (2021, June 12). China-backed APT41 behind SITA and Air India cyberattacks. Retrieved May 25, 2024, from https://www.cnbctv18.com/aviation/china-backed-apt41-behind-sita-and-air-india-cyber-attacks-9634641.html*

- *Cyber Threat Intelligence Team. (2023, December 18). Geopolitical factors shaping the future of the cyber domain. Retrieved April 12, 2024, from https://www.criticalstart.com/geopolitical-factors-shaping-the-future-of-the-cyber-domain/*

- *Dongmei, L. (2024, March 26). China has vigorously promoted the integration of big data and artificial intelligence technologies in its national strategy. Retrieved May 2024, from https://www.globaltimes.cn/page/202403/1309550.shtml#:~*

=China%20has%20vigorously%20promoted%20the,year%20growth%20of%2010.3%20percent

- *Dzodin, H. (2022, October 15). The rise of China's cyber capabilities. Retrieved May 2024, from https://theory.southcn.com/node_89b9e2eda3/7c11fb4964.shtml*
- *Eftimiades, N. (2018, December 4). The impact of Chinese espionage on the United States. Retrieved May 14, 2024, from https://thediplomat.com/2018/12/the-impact-of-chinese-espionage-on-the-united-states/*
- *Fraser, S. (2024, March 26). China's cybersecurity advancements. Retrieved May 14, 2024, from https://www.bbc.com/news/world-asia-china-68655786*
- *Fritz, A. (2019, August 2). China's evolving conception of civil-military collaboration. Retrieved May 13, 2024, from https://www.csis.org/blogs/trustee-china-hand/chinas-evolving-conception-civil-military-collaboration*
- *Handler, S. (2023, January 30). China's cyber operations. Retrieved May 1, 2024, from https://www.atlanticcouncil.org/content-series/the-5x5/the-5x5-chinas-cyber-operations/*
- *He, J., Li, Z., Zhang, X., Wang, H., Dong, W., Chang, S., ... Zhao, X. (2020, July 1). Comprehensive report on China's long-term low-carbon development strategies and pathways. Chinese Journal of Population, Resources and Environment, 1-4. https://doi.org/10.1016/j.cjpre.2021.04.004*

- *Health Sector Cybersecurity Coordination Centre. (2023). HC3: Threat profile. Health and Human Service. USA: U.S. Dept of Health and Human Services. Retrieved May 25, 2024, from https://www.hhs.gov/sites/default/files/china-based-threat-actor-profiles-tlpclear.pdf*

- *International Institute for Strategic Studies (IISS). (2019). Cyber capabilities and national power: A net assessment. Washington, DC: International Institute for Strategic Studies. Retrieved from https://www.iiss.org/globalassets/media-library---content--migration/files/research-papers/cyber-power-report/cyber-capabilities-and-national-power---china.pdf*

- *Industrial Cyber. (2024, February 18). Growing convergence of geopolitics and cyber warfare continue to threaten OT and ICS environments in 2024. Retrieved April 1, 2020, from https://industrialcyber.co/features/growing-convergence-of-geopolitics-and-cyber-warfare-continue-to-threaten-ot-and-ics-environments-in-2024/*

- *Jinghua, L. (2019, April 1). What are China's cyber capabilities and intentions? Retrieved May 13, 2024, from https://carnegieendowment.org/posts/2019/04/what-are-chinas-cyber-capabilities-and-intentions?lang=en*

- *Joshi, M. (2023, July 21). China's military-civil fusion strategy: The US response and implications for India. Observer Research Foundation. Retrieved May 13, 2024, from https://www.orfonline.org/research/china-s-military-civil-fusion-strategy-the-us-response-and-implications-for-india/*

- *Kuo, M. A. (2024, February 20). China's cybersecurity and statecraft. The Diplomat. Retrieved May 1, 2024, from https://thediplomat.com/2024/02/chinas-cybersecurity-and-statecraft/*

- *Lal, D. A. (2018, November 30). Indian warfare. World History Encyclopedia. Retrieved February 29, 2024, from https://www.worldhistory.org/Indian_Warfare/*

- *LORELEI. (2023, December 30). 10 main purposes of cyber warfare explained. Toptut. Retrieved April 12, 2024, from https://www.toptut.com/10-main-purposes-of-cyber warfare-explained/*

- *Mallick, M. G. (2022, August 1). Military-civil fusion in China. VFI. Retrieved May 13, 2024, from https://www.vifindia.org/article/2022/august/01/military-civil-fusion-in-china*

Exploiting the Uncharted: China's Interest in Space Program and the Polar Silk Route

Priyanshu Pandey

Introduction

Historically, military concerns were limited to territorial disputes across the continents, making it easier to divide the market and allocate geographical resources and limitations to countries. However, over time, certain areas of the global geographical landscape have been allocated as global commons - or regions which are not under the direct national jurisdiction of any country. These included the high seas, cyberspace, the Arctic and Antarctic regions and Space. Due to the lack of a singular influence, necessity of common usage and capacity of scientific exploration, these regions were left in a power vacuum without any structure of governance.

While this method of common ownership worked for a while, the Global Commons have always been subjected to power struggles and unilateral influences to secure strategic advantages. During World War II, both the US and Germany exercised their influence in the high seas and Antarctica to gain a strategic military advantage, whereas post-Cold War Russia and the US projected their dominance over Space. All these Ventures are primarily aimed at gaining a strategic foothold, particularly in the military and development spheres, to ensure that one nation has an upper hand. After the establishment of the United Nations, there was a call to stop such arbitrary intrusions, leading to various treaties and clauses to secure the rights of every nation to the resources in the Global Commons.

The United Nations Convention on the Law of the Sea is a prime example of how nations sought to plan and establish a status quo for the resources in the Global Commons. The

problem with such treaties was the lack of compliance, further deteriorated by the lack of consequences when a nation broke the treaty. This ultimately led to a power vacuum in the Global Commons, where Nations sought to exert their influence directly or indirectly while also claiming legitimate rights through legislative means due to the lack of a regulatory body. China is no stranger to this geopolitical power struggle and has always sought to establish its influence in the Maritime and technological spheres. Its policy towards the South China Sea and the ambitious deep-sea exploration projects are proof of its ambition to utilize the resources in the Global Commons. While the reframing and struggle over defining the high seas is not a new problem, China's assertiveness in the sphere of Arctic and space exploration provides a unique case study of a resilient and disruptive state power in the status quo of the Global Commons.

The People's Republic of China has explored many regions for geopolitical and economic interests and has always had ambitions to acquire more. The hunger to be in touch with every part of the world gave birth to the Belt and Road Initiative (BRI), a pioneer in China's efforts to establish common linkages across the globe. BRI has already established trade and military relations with a lot of neighbouring countries like Pakistan (China-Pakistan Corridor), and other parts of Europe. China aims to extend this initiative to establish global trade and revive the legacy of the Silk Route. One of the most important aspects of this BRI is the Polar Silk Route. The road, established essentially along the coast of Russia, connected to the China-Mongolia-Russia Corridor, aims to reduce trade costs between Asia and Europe by almost 35%, and China aims to be at the forefront of this trade exploitation.

Literature Review

The concept of Global Commons—domains beyond national jurisdiction such as the high seas, outer space, cyberspace, and the polar regions—has long been a subject of international law,

diplomacy, and power competition. Scholars have increasingly examined the erosion of these commons due to unilateralism, technological exploitation, and strategic encroachments, with China emerging as a central actor in both the Arctic domain and outer space geopolitics.

China and the Global Commons

Pic et al. (2023) characterize outer space as a fragile global commons lacking strong enforcement mechanisms, while Peiqing et al. (2023) analyze China's assertion of itself as a "Near-Arctic State," a self-declared status lacking legal legitimacy under the Ottawa Declaration. These moves are seen as part of China's broader strategy to redefine governance narratives and increase its global standing through legal reinterpretation and strategic investments.

In the Arctic context, Descamps (2019) and Graceddo (2024) highlight China's motivations as multifold: access to untapped energy reserves, a new maritime trade corridor (Polar Silk Route), and expansion of soft power through scientific research. The development of the Yamal LNG project, Kirkenes Port, and China's investments in Greenland demonstrate a calculated approach to economic and geopolitical integration in the Arctic, often piggybacking on its alliance with Russia.

China's strategy is often met with skepticism. RAND Research (2022) and Garamone (2024) caution that China's presence threatens the Arctic Council's governance mechanisms and introduces asymmetrical power dynamics that marginalize smaller Arctic states like Iceland and Norway.

Space and Strategic Autonomy

China's space diplomacy and military strategy are increasingly the subject of scholarly concern. Davidson (2017) and Schaffer & Bingen (2024) argue that China's exclusion from the

International Space Station catalyzed its push for independent capabilities, leading to the Tiangong space station, the International Lunar Research Station with Russia, and regional alliances via APSCO.

Uppal (2025) and Honrada (2024) explore the military dimension of China's space program, particularly its ambitions in counter-space capabilities and satellite disruption systems, which are seen as direct threats to the US-led strategic framework under the Artemis Accords.

The rise of private space firms such as iSpace, Galactic Energy, and LandSpace, supported by the Chinese state, represents a unique hybridization of state-driven and commercially flexible innovation. Scholars like Peiqing et al. (2023) note that this model allows China to achieve technological advancements rapidly and at significantly reduced costs compared to traditional space powers.

India's Role in Balancing Power

India's evolving Arctic and space policy is also discussed in emerging literature. While ISRO remains a cost-effective and technically advanced space agency, India has also maintained observer status in the Arctic Council, promoting equitable scientific cooperation. Strategic scholars argue that India could serve as a balancing actor, navigating alliances with the West while also engaging constructively with Russia and China in multilateral commons governance (Schaffer & Bingen, 2024; Honrada, 2024).

In sum, existing literature highlights how China's assertiveness in both the Arctic and space represents a transformative shift in the control of the global commons. These efforts blur the lines between peaceful development and strategic militarization, warranting vigilant policy responses and adaptive multilateral diplomacy.

Methodology

1. Research Design

This study uses a qualitative, interdisciplinary research design combining geopolitical analysis, strategic mapping, and comparative case studies. The aim is to explore how China's Arctic and space strategies are reshaping governance dynamics in the global commons and how these shifts impact other players like India.

2. Data Collection

The study primarily relies on secondary sources:

- Academic literature: journal articles, working papers, and books on international law, strategic studies, and global governance.
- Government and institutional reports: publications from the Arctic Council, UNOOSA, CSIS, RAND Corporation, and national space agencies.
- Media and industry reports: The EurAsian Times, Global Times, CGTN, CNBC, and SpaceNews.
- Official investment data and project updates from Chinese sources like CNPC, COSCO, and the Chinese State Shipbuilding Corporation.

3. Analytical Framework

The paper follows a two-track analytical model:

- Track I: Arctic Strategic Mapping
- Investment tracking in Arctic infrastructure
- Stakeholder influence analysis (e.g., Nordic countries, Russia, China)
- Impact on Arctic Council decision-making

- Track II: Space Governance Analysis
- Comparative evaluation of ISS vs. Tiangong
- Role of private actors and militarization
- Emerging governance models (e.g., Artemis Accords vs. APSCO)

Each track is examined through the lens of realist international relations theory, focusing on power projection, strategic autonomy, and great-power rivalry.

4. Case Studies

The study includes:

- Yamal LNG Project and Polar Silk Route as cases of Arctic economic diplomacy.
- Tiangong Space Station and China's role in APSCO as cases of space nationalism and south-south cooperation.
- These are contextualized within China's long-term national strategies (e.g., BRI, Military-Civil Fusion, Five-Year Plans).

5. Limitations

- Limited access to confidential Chinese internal documents may restrict insights into decision-making logic.
- Environmental data from Arctic exploration is scarce and often underreported.
- The evolving nature of space policy, especially post-ISS decommissioning, may render some analysis time-sensitive.

China’s Arctic Policy

The Arctic is governed by a shared treaty between Canada, the Kingdom of Denmark, Finland, Iceland, Norway, the Russian Federation, Sweden, and the United States, under a common treaty named the Ottawa Declaration. China and its usage of the area for the Polar Silk Route will bring a group of key players to the forefront of the international sphere, the Nordic nations (Peiqing et al., 2023). This situation is similar to the Cold War and is are warning bell of another such confrontation. So, understanding the long-term implications and proper analysis is necessary to float countermeasures to prevent the China-US confrontation from causing a vacuum.

In the current decade, China has expressed increasing interest in strategic and research development in the Arctic region, presenting a unique and complex geopolitical conundrum. The Arctic and the autonomy over its resources, including scientific exploration, is primarily granted to countries bordering the continent, often termed as Near-Arctic States. China has often referred to itself as a self-declared Near-Arctic State, staking the claim for diplomatic, scientific and economic Ventures into the Arctic continent.

Geopolitical and Strategic Interests

China's interest in the Arctic is driven by the interest to secure energy, secure channels and global positioning of the country as a dominating power. After years of scientific exploration, it is common knowledge that the Arctic has huge reserves of oil, natural gas and other rare Earth minerals, which are important for developed countries to sustain their energy consumption. The maintenance of the energy grid is necessary to sustain High operating economies, which has increased the level of engagement and tension in the Arctic sphere from powerful countries like the US, Russia and Canada. China's involvement in this region raises warning bells of stark diplomatic and security confrontations to look out for. Another crucial aspect in this

conundrum is the climate change influence. Due to Rising temperature and melting of the polar ice caps, the sea connecting Russia and China to the Arctic Circle is rising, providing a clear passage term for the Northern sea route (Descamps, 2019), which can potentially be an alternative to the Suez Canal for China to establish trade connections with Europe. This is of significant economic interest to China, further compounding its interest in exerting regional influence and control. Considering the geopolitical tensions, China's involvement in Arctic governance interferes with the operation of the Arctic governance Council, disrupting the influence of powerful Nations as well as smaller Nordic countries like Finland and Iceland, overpowering their rights and claims to the region. While China is not an Arctic Nation, it has used its diplomatic influence through bilateral ties and an observer status in the Arctic Council to position itself as an indispensable power and investor in the infrastructure, research and geopolitical developments of the Arctic.

Table 1: China's investments in the Arctic Region

Project Name	**Country**	**Sector**	**Investment Amount**	**Key Chinese Stakeholder(s)**	**Description**
Yamal LNG	Russia	Energy (LNG)	$12+ billion	China National Petroleum Corp (CNPC), Silk Road Fund	China owns a 29.9% stake; supplies LNG to China and other markets.

Arctic LNG 2	Russia	Energy (LNG)	$21+ billion	CNPC, CNOOC	Major LNG project on the Gydan Peninsula with 20% Chinese stake
Kirkenes Port Expansion	Norway	Infrastructure	Undisclosed	COSCO Shipping, China Communications Construction Company (CCCC)	Planned Arctic shipping hub for China's Polar Silk Road.
Isua Iron Ore Project	Greenland	Mining	$2+ billion	General Nice Group	One of the largest iron ore deposits, acquired by a Chinese firm.
Zinc and Rare Earth Mining	Greenland	Mining	$1+ billion	Shenghe Resources, China Nonferrous Metal Industry's Foreign Engineering and Construction	Strategic investment in Greenland's rare earth resources.
Polar Silk Road Shipping	Multiple	Infrastructure	Undisclosed	COSCO Shipping, State Oceanic Administration	China's strategic development of Arctic shipping

Routes					routes.
Snow Dragon 2 Icebreaker	China	Research/ Shipping	$300+ million	China State Shipbuilding Corporation (CSSC)	First domestically built icebreaker for Arctic research and navigation.

The diplomatic and projective nature of China's influence on the Arctic presents itself as a unique opportunity to understand how Nations tend to leverage their geopolitical prowess to harness legitimate influence over the Global Commons, often at the expense of smaller countries who have a righteous stake. While the situation is very young and volatile currently, it is important to understand the latest developments to foresee any power struggles or strong-arming maneuvers by China or its allies like Russia, against the smaller Nations involved in the Arctic Council. It is also important to understand that while the Arctic Council has the singular governance rights, the developments in the Arctic Circle have an economic and environmental impact across the globe, making it a very sensitive area for security confrontation.

Economic and Scientific Engagement

The first leg of development in China's Arctic policy is the investment in Arctic infrastructure through Russia and bilateral agreements with Greenland. The Sino-Russian alliance has invested significantly in energy development and extraction projects like Yamal LNG and Arctic LNG 2 (Graceddo, 2024), which have proven to be scientifically advanced and economically prosperous ventures. These Investments are directly in line with China's Belt and

Road initiative, connecting its Arctic policy through the development of a Polar Silk Road (Descamps, 2019) to further consolidate the trade networks.

The polar Silk Road is a manifestation and extension of the Belt and Road initiative, expanding in northern China and the Northern Russian region, running parallel to the newly cleared Arctic sea route. While the economic benefits contribute significantly to Chinese interest in the area, Xi Jinping has also expressed interest in scientific research, validating the development of research stations in smaller Nordic countries like Norway and Iceland. The Yellow River Station (Garamone, 2024) partnership with Norway is an example of how China has directed significant funding towards studying climate change, glacial melting and deep-sea marine biology. The Chinese claim that these research developments are focused on environmental purposes and are for scientific and peaceful measures, but many Western powers, including Canada and the USA, are skeptical of the dual-use functions of research stations and are concerned about China's long-term strategic ambitions in the Arctic.

Challenges and Global Implications

The Chinese ambition in the Arctic region presents three pressing concerns which have plagued the Arctic Council. Firstly, the USA, Canada, and even the European Union are concerned with the Strategic and military implications (RAND Research, 2022) of rising fiscal investments by China in the region, disrupting the economic influence that these countries hold over the Arctic region. Arising dominance over resources and strategic positioning in the Arctic would allow China to threaten the European Global Order much easily, increasing the threat index it poses to the European and American counterparts as compared to today.

Secondly, China's economic influence and the potential to disrupt trade Networks are a major concern for a lot of countries involved. Nordic countries are wary of their influence and have

expressed concerns over being strong-armed into treaties and collaborations, where they give up more autonomy and resource allocation to China than they benefit. Russia, a key player in the Arctic region and a close ally of China, has also maintained a diplomatic distance between the economic and geopolitical influence over the Arctic, in an attempt to preserve its geopolitical dominance in the region. China's involvement has not triggered confrontations yet, but has certainly complicated the situation a lot more, giving rise to tensions and calculative measures in the Arctic region, making it one of the most volatile Global Commons.

Lastly, many arctic and non-arctic countries have expressed their concerns over the environmental impact of large-scale exploration and extraction of resources by China and its allies. The Arctic Circle maintains a very fragile ecosystem which cannot be replicated anywhere in the world, providing a home to unique and rare flora and fauna. The rising economic activities pose a serious threat to the destruction of habitat for these organisms, as well as contributing to the worsening effects of climate change.

China’s growing role in the Arctic is a testament to its broader global ambitions and strategic adaptability. By positioning itself as a key player in Arctic governance and economic development, China is seeking to reshape the geopolitical landscape in ways that favor its long-term interests. However, its involvement is met with considerable scrutiny, particularly from Western nations, which view China’s Arctic expansion as part of a larger pattern of strategic encroachment. The situation in the Arctic currently hangs in a tense balance between China and the involved Arctic Nations. There is uncertainty regarding China's long-term gains and implications, but China will certainly face eventual resistance from the Arctic Council, needing a more competitive legislative struggle over the region.

However, China needs to prioritize environmental responsibility and cooperative action to ensure itself a legitimate role in the development of the Arctic region, engaging in geopolitical tensions and conflicts. This volatile situation and the promulgated response from the Chinese government make it very important for the world to keep its eye on Chinese development in the Arctic landscape. The situation presents itself as a microcosm of global strategy, where China, a crucial global power, can use economic expansion and diplomatic engagement to increase its influence and strategic positioning in a global commons. This could play a pivotal yet contentious role in shaping the future of the global order while also setting up residence over the governance and resource sharing in the Global Commons.

China's Space Policy

Fast-paced technological advancements have always altered global politics. From the development of the submarine to the Advent of nuclear warfare, the face of global geopolitics has changed significantly due to scientific research. One such Avenue of rapid development and privatization is outer space. Space is regarded as a global common, which falls beyond the jurisdiction of any nation and has very few agreements and treaties governing actions beyond the stratosphere. China was initially left out of the space race when Washington, DC did not allow China to be a part of the International Space Station project, citing concerns over militarization and protection of domestic research. But as the technology evolved, access to space has become far more common than it was during the Cold War. It has not only become a pivotal Corner in scientific research but is also a significantly impactful diplomatic tool.

China is a crucial example of how individual Nations can exert significant influence in space through technological superiority backed by a robust economy. As a remnant of the space race between the US and USSR, China now plans to carry out the baton against the USA, for space dominance and lunar exploration. PRC has not taken it quietly, after being excluded from the

International Space Station, and has been expanding the already operational Tiangong Space Station, which would also be crucial for any space exploration after the demolition of the ISS in 2030. (Davidson, 2017).

China, as a growing superpower, has made leaps and bounds in the development of its space programme, and comparing its growth to the ISS makes the technological gap even more evident. The International Space Station was conducted by the contributions of over 15 countries over 10 years and 30-plus missions to be fully operational. At its peak, ISS had 16 modules for research and information gathering. Tiangong, the China-built space station, at 1/5th the capacity, has 3 modules and hosts 6 astronauts for 6-month research projects. The size difference is also massive, with Tiangong forming only about 22% of the size of the ISS. Astonishingly, the regularity of research missions to Tiangong has been more frequent than ISS, and it has achieved complacency with international standards at 5.3% of the ISS budget. At $150 billion, ISS is the biggest human project, whereas Tiangong took $ 8.5 billion to finish itself within the same timeframe. With the planned decommissioning of the ISS in 2030 and subsequent plans to maintain a low-orbit presence, it becomes increasingly necessary for countries to collaborate with China and be on the positive side of its expertise.

These figures and the current situation establish China’s space programme as the biggest example of why exclusionary and disjunctive strategies are ineffective and harm the collective good of the international commons. China's space policy is diverse, involving bilateral and multilateral agreements for investment, development and technological cooperation with many countries of the Global South. With the Asia Pacific Space Cooperation Organization (APSCO), China has managed to consolidate Africa, Latin America and Southeast Asia into a

global space network which rivals the capacities and ambition of the space missions in the Global North.

Beyond regional cooperation, China is also involved in the functioning and management of the United Nations Office of Outer Space Affairs (UNOOSA) (Schaffer & Bingen, 2024). It has engaged in coordinating specific projects like the International Lunar Research Station in collaboration with Russia, validating its interest in subverting the Western-led space race, which is dominated by the European Space Agency and NASA. Their recent missions, to space and the race to the moon, are not just for exploration and the technological dominance over the US, but also show a much more problematic sphere of geopolitics over the moon. Beijing has never shied away from inflating the superiority of the Chinese Space program, but now it is clear that they have significant technological advancements to back those claims. (Peiqing et al., 2023)

While exploration of space is primarily controlled by nations, the privatization of space is a rising concern in recent years. Commercial space forms owned by private entities have supported government policies and are hubs of innovation in the field of space exploration, like SpaceX and Blue Origin. The problem with these private Industries is the lack of regulation and accountability in terms of geopolitical responsibility. While SpaceX is responsible for one-third of the debris in the lower stratosphere, the responsibility is seldom imposed upon the USA.

China, too, supports a slew of private firms like LandSpace, iSpace and Galactic Energy to manage satellite payloads (Uppal, 2025) and develop reusable rocket capsules. Since 2014 China's space policy has been aggressive towards catalyzing the growth of the sector and enabling startups to contribute to the national space ambition.

Table 2: China's Private Space Companies and Their Roles

Company Name	Founded	Key Projects	Investment Amount	Role in National Space Program
iSpace (Interstellar Glory)	2016	Hyperbola rocket series (Hyperbola-1, Hyperbola-2)	$300+ million	First private company in China to reach orbit; supports low-cost satellite launches.
Galactic Energy	2018	Ceres-1, Pallas-1 rockets	$400+ million	Complements state-owned launch capabilities with commercial satellite deployment.
LandSpace	2015	Zhuque-1, Zhuque-2 (methane rocket)	$500+ million	First Chinese company to launch a methane-powered rocket; supports next-gen propulsion research.
OneSpace	2015	OS-M series rockets	$200+ million	Develops low-cost, rapid-response launch vehicles for commercial and military applications.
Deep Blue Aerospace	2016	Nebula-1, Nebula-M	$140+ million	Focuses on reusable launch technology, aligning with China's goal of cost-

				efficient space missions.
ExPace (subsidiary of CASIC)	2016	Kuaizhou rocket series	$600+ million	Supports military and state-backed satellite launches for national security.
Orienspace	2020	Gravity-1 rocket	$100+ million	Aims to provide high-capacity commercial launch services in alignment with China's space strategy.

Key Challenges and Strategic Implications

With China becoming a major contributor to the space race and lunar exploration projects, collective organizations like the United Nations and ASEAN need to develop regulatory frameworks of lunarization my locations from space projects. The US-led Artemis Accords (Honrada, 2024) for lunar exploration are an effective counter to China's rising ambition in the sphere, but also present a precarious situation where blocs of nations are exercising control and legislation over space exploration without the presence of a globally agreed-upon treaty or framework. This can barrel towards a conflict very quickly, leading to confrontations either in space or the diplomatic sphere, endangering technological development and exploration by less influential countries. Space is a global common that has not yet been breached enough to be a ground of geopolitical contention, but the lack of regulatory frameworks makes it very susceptible to rapid militarization, private ownership, exclusion and marginalization towards smaller countries, restricting access to space.

Inferences and Broader Implications

China's space diplomacy and privatization strategies reflect broader geopolitical ambitions. By integrating space capabilities with economic and diplomatic outreach, China is not just positioning itself as a space power but also reshaping international norms and alliances. One key inference is that China's space strategy is deeply intertwined with its larger geopolitical agenda. The expansion of the BDS, lunar ambitions, and commercial space collaborations demonstrate a long-term vision that aligns with China's aspirations for technological self-sufficiency and strategic autonomy.

Another important development is that while privatization of space exploration has improved the technological capabilities of China, the projects are still State guided. Individual corporations align themselves with the national space exploration program to ensure that the hybrid model of privatization includes commercial space firms into the national objectives while giving them the autonomy to operate independently. Lastly, China has formed a comprehensive policy of space diplomacy with bilateral agreements in dividing Global space governance. It has managed to create competing groups motivated and composed of different regulatory Frameworks and strategic interests, positioning itself against future space endeavors shaped by geopolitical rivalries. With increased collaboration among Latin American and African countries, China has championed itself as the face of space exploration in the Global South.

India in the Mix

India is set to play a crucial role in either complementing or countering the growing influence of China in the Arctic and space. Through diplomatic flexibility and nurturing diplomatic conditions, India has managed to maintain an observer status in the Arctic Council, advocating

for scientific coordination and managing Equitable governance in the Arctic. The friendly treaties and robust scientific vigor that India brings to the table would be crucial in countering one-sided influence from China. With strengthening ties between India, the European Union, Japan and the US, the consolidation of the Arctic strategy in India is almost complete. While the country does not face a direct threat from China in its engagement with the Arctic Circle, India needs to be at the forefront of the countermeasures to establish itself as a global power capable of power projection.

Similarly, ISRO from India has had commendable feats in the recent past, presenting itself as an avenue of investment against the defense-focused satellites of China. With enriching partnerships in Europe, India has become a small yet crucial part in the global space governance, contributing to the efforts and capabilities of the global World Order in complementing and countering China.

The militarization of space by China poses a significant threat to India due to the far inferior projection of power in space by the Indian military. It is also crucial to notice that India's involvement in various treaties countering China's growing influence, like the SQUAD and close ties with the European Union and the US, are necessary for the Western powers to balance the vacuum and disruption in Asia. However, while these countries depend on India's strategic geopolitical positioning, India seldom draws benefits in technological advancements and militarization from these groups. ISRO was not favored by US or European powers in the development of its lunar project, and various European powers like the United Kingdom were openly hostile towards the development of space-based military capacities in India.

While India has a significant presence in both the Global Commons, the country needs to understand if China is only an adversary or a neighboring country with dynamic opportunities for collaboration. India and China find themselves on the same side of global affairs regarding exclusion from international space programs and limited resources towards the privatization of Arctic research. This can lead to sympathetic diplomatic ties regarding the global Commons, providing India with the Strategic backup it requires to consolidate itself as a global power. China and its close ties with Russia, and in turn Russia's close ties with India, provide the perfect environment to foster a collaboration between the three biggest countries on the Asian continent to counter any Western influence against the exploration of the Global Commons.

Conclusion

The paper aims to understand the implications of China's advances in the geopolitical regions that are not governed by laws or are not sovereign territories. The analysis is based on observations and political and economic trends in the Asia-Pacific, Arctic and Space. The future of Arctic and space security depends on cooperation, regulatory transparency, and global diplomacy, rather than an arms race across the Global Commons. The international world order must remain aware, take part in dialogue, and compromise towards peaceful cooperation in the Global Commons while preparing for potential challenges posed by the militarization of these regions. This paper brings to light the acute lack of any diplomatic or legal framework to prevent the exploitation of such spaces.

References

- *China's "Mind-Boggling" Space Militarization Raises Alarm In The U.S.; Beijing Says Pentagon Inflating "China Threat" Theory. (2024, November 2). The EurAsian Times.*

- *Descamps, M. (2019, February). The Ice Silk Road: Is China a "Near-Arctic-State"? Institute for Security & Development Policy.*

- *Garamone, J. (2024, December 5). China Increasing Interest in Strategic Arctic Region. US. Department of Defense News.*

- *Graceddo, A. (2024, October 14). China and Russia Arctic Policy Convergence? Shifting Geopolitics in the North. Geopolitical Monitor.*

- *Honrada, G. (2024, July 1). China's growing appetite for a space fight with US. Asia Times.*

- *Peiqing, G., Huiwen, C., Lalonde, J., Devyatkin, P., & Cunningham, A. (2023, June 20). Chinese Perspective on the Arctic and its Implication for Nordic Countries. The Arctic Institute. Retrieved May 31, 2024, from https://www.thearcticinstitute.org/chinese-perspective-arctic-implication-nordic-countries*

- *Pic, P., Evoy, P., & Morin, J.-F. (2023, September 5). Outer Space as a Global Commons: An Empirical Study of Space Arrangements. International Journal of the*

Commons. Retrieved May 31, 2024, from https://thecommonsjournal.org/articles/10.5334/ijc.1271

- *RAND Research. (2022, December 29). What Does China's Arctic Presence Mean to the United States? RAND Commentary.*

- *Schaffer, A., & Bingen, K. A. (2024, October 31). Engaging China on Space with Eyes Wide Open. Space in Focus - Center for Strategic and International Studies.*

- *Uppal, R. (2025, January). China's Escalating Space Militarization: Assessing Destructive 'Counter-Space' Capabilities and Weapons Advancements. International Defense, Security & Technology, 2(4).*

Indic Centre for Pakistan Studies (ICPS)

The Indic Centre for Pakistan Studies (ICPS) is a critical research hub under the Indic Researchers Forum, devoted to examining the structural and ideological drivers behind Pakistan's enduring volatility. ICPS investigates the formation and evolution of the Pakistani state through the lens of religious identity, military dominance, and political fragility, with a focus on how these factors have steered Pakistan toward chronic instability.

Adopting an India-first analytical framework, the Centre explores Pakistan's state-sponsored security threats, its strategic use of proxy warfare and jihadist networks, and the functioning of its military-intelligence establishment. ICPS also contributes to the formulation of coherent Indian policies and doctrinal responses to cross-border terrorism, grey-zone warfare, and regional destabilization efforts emanating from Pakistan.

Image Source: Google

Inaugural Pashtun Security Dialogue

Levsa Bayankhail

Tilak Devasher

Fazal Ur Rehman Afridi

Zia Ullah Hamdard

Inaugural Pashtun Security Dialogue

transcribed by Sathya Pulukuri

- Levsa Bayankhail, General Secretary of PTM Denmark and Convener of Pashtun Security Dialogue, Indic Researchers Forum, who will moderate today's discussion.
- Shri Tilak Devasher, Member of India's National Security Advisory Board and a renowned author on Pakistan and Pashtun issues.
- Fazal Ur Rehman Afridi, PTM's Head of International Advocacy, UN Representative, and President of the Khyber Institute, Paris.
- Zia Ullah Hamdard, journalist, activist, and UK-based academic pursuing a PhD in Media and Cultural Studies.

- Samidha Jain, Session Host of IRF

1. Levsa Bayankhail: (General Secretary, PTM Denmark & Convenor, Pashtun Security Dialogue, an initiative of the Indic Researchers Forum): Thank you to the Indic Researchers Forum for giving me the opportunity to moderate this important discussion. I'm truly honored to be part of this platform and to engage with such esteemed panelists.

The Pashtun Security Dialogue is an initiative to highlight the security challenges faced by Pashtuns across the Durand Line. Our aim is to provide a space for geopolitical thinkers, academics, human rights defenders, and security experts to speak about the historical and present-day issues affecting Pashtun society. But this dialogue is also about reviving historical and civilizational ties between Pashtuns and India. We must remember the shared legacy of leaders like Bacha Khan, Mahatma Gandhi, and Subhash Chandra Bose, who stood united in the freedom struggle against colonial rule. Bacha Khan, in particular, felt betrayed by the Indian

National Congress at the time of partition—his people were left at the mercy of a rising authoritarian regime in Pakistan.

And that betrayal still echoes today.

Pashtuns continue to face a silent genocide carried out by the Pakistani military establishment. Meanwhile, the international community remains silent—choosing strategic interests over human lives. Pakistan has spent decades crafting a false narrative that portrays Pashtuns as extremists or terrorists. But we know who the real extremists are—the Pakistani army and intelligence agencies who have turned our lands into launching pads for proxy wars.

As a proud member of the Pashtun Tahafuz Movement (PTM), I see hope in our nonviolent resistance. PTM carries forward Bacha Khan's legacy—we are standing up to the real forces of terror in our region: the Pakistani state itself. Through peaceful advocacy, we appeal to global civil society, human rights bodies, and democratic governments: recognize the oppression, the enforced disappearances, the extrajudicial killings that Pashtuns have suffered and continue to suffer.

I will conclude my remarks here, as I want to leave time for our distinguished speakers.

I now invite our first speaker, Shri Tilak Devasher, a renowned expert on Pakistan and author of four acclaimed books, including his latest work on the Pashtuns. Sir, it is truly an honor to have you with us today. Your analysis of Pakistan's internal dynamics gives us critical insight into the struggles Pashtuns have faced since 1947.

The floor is yours.

2. Tilak Devasher

Member, National Security Advisory Board; Author of several books on Pakistan

Topic: Pakistan-Afghanistan Relations Since 1947

Tilak Devasher: thank you very much for inviting me to this Pashtun Security Dialogue. It is truly a privilege to be here. This subject is close to my heart, not only as a strategic analyst but also because I have written an entire book on the Pashtuns. Throughout my research, I found that Pashtuns remain one of the most misunderstood communities in the region. It's easy to make assumptions without truly grasping their rich historical legacy, deep-rooted civilizational identity, and resilient character. My aim has always been to bring their real story to light and correct the misperceptions that dominate public discourse.

Turning to today's topic—Pakistan-Afghanistan relations since 1947—it's important to clarify one thing from the outset. While we use the term "Pakistan-Afghanistan relations," what we're really discussing is Pakistan's relationship with the Pashtuns. Pashtuns have been the pivotal factor shaping this relationship, and much of the geopolitical tension between the two countries revolves around them.

One issue lies at the heart of it all: Pakistan's enduring insecurity over the Durand Line. The Durand Agreement of 1893, as many know, arbitrarily split the Pashtun population between British India and Afghanistan. After Pakistan's creation in 1947, Afghanistan stood as the only country to oppose its entry into the United Nations, specifically because it refused to accept the legitimacy of the Durand Line. In 1949, Afghanistan formally rejected the boundary, and no Afghan regime since—whether monarchy, republic, mujahideen, or Taliban—has recognized it as an international border. On the other hand, Pakistan continues to treat the Durand Line as a settled matter, yet remains deeply anxious about its contested status.

That insecurity has dictated Pakistan's entire approach to Afghanistan. The core objective has always been to ensure that Kabul remains weak, fragmented, and dependent. A strong, autonomous Afghan government could threaten Pakistan's hold over its Pashtun borderlands, rekindle the historical idea of Pashtunistan, and ultimately challenge the country's territorial integrity. This is where the concept of "strategic depth" comes into play. Pakistani strategic planners believe that in the event of a war with India, they would require a fallback zone—and a compliant Afghanistan would serve that role.

Let us briefly trace how this policy has played out over the decades. Contrary to popular belief, Pakistan's interference in Afghanistan did not begin with the Soviet invasion in 1979. As early as 1973–74, under Prime Minister Zulfikar Ali Bhutto, Pakistan began training and supporting Afghan insurgents. During the Soviet-Afghan War (1979–1989), General Zia-ul-Haq seized the opportunity to position Pakistan as the U.S.'s frontline ally. The ISI took control of the mujahideen network, and Pakistan received billions in aid, while shaping the Afghan resistance to suit its strategic aims.

After the Soviet withdrawal, Pakistan shifted its support from fragmented mujahideen groups to the Taliban. By 1996, with direct ISI backing, the Taliban captured Kabul. However, despite Pakistan's pivotal role in their rise, it still failed to secure formal recognition of the Durand Line. After 9/11, the story took another turn. Pakistan officially became an ally in the U.S.-led War on Terror, but covertly provided safe havens for Taliban leadership in FATA and Balochistan. Over the next two decades, Pakistan enabled the Taliban to regroup, rebuild, and eventually recapture Kabul in 2021.

When the Taliban returned to power, Pakistan's political and military elite were euphoric. They believed they had achieved strategic victory. Expectations were high: the Taliban would recognize the Durand Line, curb Indian influence in Afghanistan, and suppress the TTP

(Tehrik-i-Taliban Pakistan). But none of this came to pass. India reestablished diplomatic engagement in Afghanistan. Taliban forces clashed with Pakistani troops over border fencing. And the TTP, far from being dismantled, has grown stronger and more aggressive.

Today, Pakistan faces a serious internal contradiction—a dual Pashtun dilemma. On one side is the Afghan Taliban, who refuse to accept Pakistani control over Pashtun lands. On the other is the TTP, which continues to wage an insurgency and demands reversal of the FATA-Khyber Pakhtunkhwa merger. If Pakistan fails to address this situation wisely, it risks igniting renewed calls for a unified Pashtun region—an outcome that would directly challenge the state's territorial and ideological foundations.

In summary, Pakistan's Afghan policy has failed. The very actors it cultivated for decades—the Taliban—are now acting independently and refusing to serve Pakistani interests. Meanwhile, the internal insurgency in its Pashtun regions is intensifying. This is a direct consequence of decades of flawed, coercive, and short-sighted policies.

3. Fazal Ur Rehman Afridi

Head, PTM Committee on International Advocacy & Foreign Affairs; Principal Representative at the UN; President, Khyber Institute of Research & Strategic Studies

Topic: The Killing of Gilman Wazir and the Condition of Pashtuns in Pakistan

Fazal Ur Rehman Afridi: Thank you for having me in this important dialogue. It is an honor to be part of a platform that brings international attention to the systematic oppression of Pashtuns by the Pakistani state. Today, I wish to speak about the extrajudicial killing of Gilaman Wazir and the broader condition of Pashtuns in Pakistan. Gilaman Wazir was not just a poet—he was a revolutionary voice for our people. He was a human rights activist who wielded poetry as a weapon of resistance. Through his verses, he gave voice to the pain, the injustice, and the truth

of the Pashtun experience. And for that, he was silenced. On July 7, 2024, in broad daylight at a coffee shop in Islamabad, Gilaman was attacked by four masked men. One of them struck him on the back of the head with a metal rod—deliberate and precise. Present at the scene was Adeel Wazir, identified as one of the masterminds, armed with a pistol, ready to execute him if needed. Disturbingly, no law enforcement intervened. The attackers fled without resistance.

Gilaman was rushed to PIMS Hospital, where doctors declared him brain-dead upon arrival. He remained in a coma for four days and passed away on July 10, 2024. This was no random act of violence. It occurred in Islamabad, under the full view of the country's most powerful intelligence agencies. One of the main suspects was even allowed to leave the country freely. No arrest. No accountability. Just deafening silence. Gilaman's murder follows a chilling pattern of targeted assassinations of PTM leaders and Pashtun intellectuals. Arman Loni was killed in 2019. Sardar Arif Wazir was assassinated in 2020. Senator Usman Kakar died under mysterious circumstances in 2021. Tahir Dawar, a senior police officer, was abducted and murdered in 2018. Now, Gilaman Wazir joins this tragic list. His only "crime" was speaking out for basic human rights.

This wasn't the first time he was targeted. On July 7, 2023, he was abducted by Pakistani military intelligence from Peshawar Airport. He was held illegally for over seven months in a secret facility at the Peshawar Corps Commander's headquarters. When he was finally brought before a court, his body and mind bore the unmistakable marks of brutal torture. During his detention, Gilaman was subjected to horrific abuse. Trained dogs were unleashed on him, biting into his legs. He was beaten repeatedly with fists and batons, stripped naked in freezing temperatures, and denied sleep for prolonged periods. He was threatened with being crushed by military vehicles, kept chained in painful positions for hours, starved, and confined in

inhumane conditions. Despite this torture, Gilaman refused to record any false confession against PTM. He never renounced his beliefs or betrayed his principles.

Since 2018, over 600 targeted killings of Pashtun activists have been reported. The Pakistani state employs a calculated strategy to silence dissent: enforced disappearances, extrajudicial killings, and military operations that destroy entire villages and displace thousands. The only "threat" these victims posed was their courage to speak the truth. PTM has consistently raised these grave concerns at the United Nations and other international platforms. We have demanded independent investigations into these crimes, sanctions against Pakistani military officials involved, and accountability at global forums. Yet, the Pakistani state continues to deny everything. It refuses to allow any international inquiry. It continues its violent crackdown on peaceful activists. This silence is not a sign of innocence. It is a clear indicator of guilt.

The state believes that by killing our poets, intellectuals, and truth-tellers, it can crush the Pashtun resistance. But they are wrong. The assassination of Gilaman Wazir has only strengthened our resolve. Across the globe, the Pashtun diaspora is mobilizing. PTM will not be silenced. We demand full accountability for the crimes committed against Pashtuns, a transparent inquiry into Gilaman's murder, and urgent international action to halt Pakistan's campaign of repression. I will close with this: the world must not stay silent. The genocide of Pashtuns is real, and it is happening right now. We will not rest. We will not forget. And we will not stop until justice is served.

Thank you.

4. Zia Ullah Hamdard

Journalist, Lecturer, and Human Rights Activist from Pakistan

Topic: Legacy of Bacha Khan and the Pashtun Tahafuz Movement (PTM)

Zia Ullah Hamdard: Thank you for the opportunity to speak on such a crucial topic. I am grateful to the Indic Researchers Forum for organizing this important discussion and for creating space where Pashtun voices can be heard on an international platform. Today, I want to reflect on the enduring legacy of Bacha Khan—a towering figure in Pashtun history—and how his philosophy of nonviolent resistance continues through the Pashtun Tahafuz Movement (PTM). Bacha Khan, or Khan Abdul Ghaffar Khan, was one of the most revered leaders of the Pashtun people. Deeply inspired by Mahatma Gandhi, he dedicated his life to the ideals of peace, education, and justice. As the founder of the Khudai Khidmatgar (Servants of God) movement, he mobilized tens of thousands of Pashtuns to challenge British colonial rule through peaceful civil disobedience.

His message was revolutionary for its time: that Pashtuns, despite their warrior reputation, must choose nonviolence, unity, and dignity in the face of injustice. Bacha Khan demanded not just political rights but also education, social reform, and self-respect for Pashtuns.

Yet, after Partition, his greatest betrayal came not from the British but from his former allies in the Indian National Congress. Despite his lifelong opposition to the division of India, Bacha Khan and the Pashtuns were given no democratic choice. The newly created Pakistani state crushed the Khudai Khidmatgar movement with brutal force. Bacha Khan himself was imprisoned for over 30 years for merely demanding the rights of his people and opposing military dictatorship. His vision of a peaceful, autonomous, and progressive Pashtun society was systematically dismantled by Pakistan’s military establishment.

Since 1947, Pashtuns have endured a sustained campaign of marginalization. Our language and cultural traditions have been sidelined. Our political leaders have been imprisoned, exiled, or assassinated. In place of genuine representation, the state promoted religious extremism as a tool of control. Pashtun lands were turned into battlegrounds—first during the Soviet-Afghan war and later during the so-called "War on Terror." The Pakistan Army created and armed militant groups to serve its foreign policy objectives, using Pashtun territories as strategic depth. When these groups became uncontrollable, military operations were launched in our regions—razing villages, displacing millions, and labeling Pashtuns as terrorists. In truth, we have been the victims of state terrorism.

In 2018, after decades of silence and state repression, the Pashtun Tahafuz Movement emerged as a powerful force of peaceful resistance. Sparked by the extrajudicial killing of Naqeebullah Mehsud—a young Pashtun falsely accused and murdered in a staged police encounter—PTM quickly evolved into a mass grassroots movement inspired by Bacha Khan's nonviolent legacy. The movement demands an end to extrajudicial killings and enforced disappearances, the removal of landmines from civilian areas, and accountability for the war crimes and human rights abuses committed by the Pakistani military. Despite its peaceful nature, PTM has faced relentless crackdowns. Its leaders have been harassed, jailed, tortured, and, in some cases, assassinated. Manzoor Pashteen, the face of PTM, has been repeatedly imprisoned for simply voicing the truth. The Pakistani media is banned from covering PTM's activities, as the state seeks to erase our presence from the national narrative. In response, PTM has turned to social media platforms—Facebook, Twitter, YouTube—to document injustices, share testimonies, and organize across borders. Citizen journalism has become our lifeline, exposing military atrocities that would otherwise remain hidden. Despite intense censorship, PTM's message has reached millions and drawn international attention.

PTM is the first movement since Khudai Khidmatgar to unite Pashtuns across tribal, political, and ideological lines. It has shattered the myth that Pashtuns are inherently violent or extremist, and instead presented them to the world as victims of a militarized state. PTM has lifted the veil on Pakistan's deep state and its use of terrorism as a tool of policy. It has also brought the Pashtun cause to the global stage—highlighting enforced disappearances, targeted assassinations, and systemic war crimes.

But our fight is far from over. Hundreds of Pashtuns are still missing. Surveillance, intimidation, and military violence against PTM activists continue unabated. The international community, despite acknowledging our suffering, has yet to take any meaningful action. We therefore call on the United Nations and other global bodies to investigate Pakistan's war crimes in Pashtun regions and to formally recognize the slow-moving genocide being committed against us. At the same time, we urge Pashtuns to continue organizing, resisting, and building on Bacha Khan's vision of nonviolent justice.

PTM today is that voice of truth that Bacha Khan spoke of. And to those who believe they can erase our identity through fear, violence, and propaganda—know this: Pashtuns have endured centuries of oppression and have never been broken. We will continue to resist. The spirit of Bacha Khan lives on. And our fight for justice has only just begun. Thank you.

Q&A Session – Pashtun Security Dialogue

How can the PTM movement be joined with Baloch and Sindhi voices to create a larger movement against oppression in Pakistan?

Fazal Ur Rehman Afridi responded by emphasizing that a unified front of oppressed ethnic groups—Pashtuns, Baloch, Sindhis, and even Kashmiris—is exactly what the Pakistani state fears the most. He noted that such unity would directly challenge the military-dominated structure of Pakistan. Afridi pointed out that cooperation has already begun at the international level. PTM has held joint protests with Baloch and Sindhi activists at the UN Human Rights Council and collaborated with them in discussions at the European Parliament. These groups frequently communicate and coordinate, often appearing together at side events and international forums to present a united stance against Pakistani military atrocities. On the ground, PTM members have shown solidarity with the Baloch cause—such as during Mahrang Baloch's long march for the disappeared. Moving forward, Afridi argued for a more structured alliance, one that ensures deeper national and international coordination, shared platforms, and a unified political voice. According to him, Pakistan thrives on dividing these groups using propaganda, infiltration, and violence. It's time, he concluded, to counter that with organized unity.

You mentioned "Punjabi colonialism." What role does ethnicity play in determining the treatment of minorities in Pakistan?

Zia Ullah Hamdard explained that ethnicity is central to how power is distributed in Pakistan. The country's military, bureaucracy, and media are overwhelmingly dominated by Punjabis. Consequently, the entire system is designed to benefit Punjab while systematically suppressing ethnic minorities like the Pashtuns, Baloch, and Sindhis. In Pashtun regions, he pointed out, the Pashto language is marginalized, cultural expressions are censored, and infrastructure is

neglected. Schools teach Urdu and English but not Pashto, and media portrayals of Pashtuns are often stereotyped or absent. Hamdard noted that Pashtuns are exploited as cannon fodder in Pakistan's wars—recruited en masse for military campaigns in Kashmir and Afghanistan, while their own regions remain underdeveloped. Similar patterns exist in Balochistan, where natural resources are extracted, but the population remains impoverished and politically sidelined. Sindhis, too, are politically marginalized and have lost control of their cities to non-native power structures. He called this not just systemic discrimination but a form of internal colonialism, where Punjab acts as the metropole and the rest as subjugated peripheries.

Pashtuns have suffered one of the worst genocides, yet the world does not recognize it. What are the reasons for this, and how can Pashtuns bring global awareness?

Fazal Ur Rehman Afridi identified three main reasons for the lack of global recognition. First, Pakistan has a well-established lobbying network that presents the country as a "victim of terrorism" to the West—particularly the U.S.—while concealing its role in sponsoring terror and suppressing minorities. Second, international attention is dominated by other crises like Palestine, Ukraine, and Afghanistan, pushing Pashtun suffering out of the spotlight. Third, Pakistan's control over media ensures that Pashtun voices are muted both domestically and internationally. To change this, Afridi urged the Pashtun community to increase engagement with global institutions like the UN and EU, document human rights abuses through social media, and build alliances with other marginalized communities. He reminded the audience that just as the truth about the 1971 Bangladesh genocide eventually came out, so too would the truth about the atrocities against Pashtuns—if they continued to speak out.

The Taliban are often called "Pashtun nationalists." Do you agree with this label?

Zia Ullah Hamdard firmly rejected this characterization. He argued that the Taliban do not represent Pashtun nationalism at all. In fact, they actively suppress Pashtun identity—banning Pashto literature, rejecting traditional Pashtun culture, and targeting nationalist leaders. The Taliban, he emphasized, are a creation of Pakistan's military and intelligence agencies, designed as a strategic tool to control Afghanistan. While the Taliban do reject the Durand Line, their motivation is not rooted in Pashtun nationalism but in their broader Islamist expansionism. Hamdard warned that labeling the Taliban as Pashtun nationalists is a deliberate distortion used by the Pakistani state to mislead the global community.

Former PM Imran Khan compared the situation of Pashtuns today to the 1971 Bangladesh genocide. Do you think Pakistan is heading for another civil war?

Fazal Ur Rehman Afridi said that what's happening now is not a prelude to genocide—it is genocide, unfolding in real time. Drawing a direct parallel to 1971, he recalled how the Pakistani state refused to accept the democratic victory of the Awami League, choosing instead to respond with military force, leading to mass killings, rape, and displacement. Today, he said, a similar pattern is repeating itself with Pashtuns. Over 880,000 have been killed in military operations and drone strikes, more than 30,000 forcibly disappeared, and entire villages flattened under the pretext of fighting terrorism. While Imran Khan's comparison was accurate, Afridi questioned why Khan took no action when he was in power. He concluded by warning that unless the world acts soon, Pakistan risks repeating the horrors of its past—this time against Pashtuns and Baloch.

Given the civilizational links between India and Pashtuns, should Pashtuns build a long-term relationship with India?

Tilak Devasher affirmed that Pashtuns and Indians share deep civilizational bonds going back millennia—from Gandhari in the Mahabharata to the transmission of Buddhism through Pashtun lands. Historically, many Pashtun dynasties ruled parts of India, and modern figures like Bacha Khan had strong ties with Indian leaders such as Gandhi. Despite being abandoned during Partition, Pashtuns have never considered India an enemy. The rupture, Devasher argued, was manufactured by Pakistan's suppression of any cross-border historical or cultural ties. Moving forward, he suggested India should actively re-engage Pashtuns by supporting civil society, offering platforms in Indian academia and media, and advocating for Pashtun human rights at international forums. India must not repeat the mistake of 1947—it should now stand on the side of justice.

What should be the ideal approach for Indian policymakers toward the Pashtun issue?

Tilak Devasher outlined a three-pronged strategy. First, Indian policymakers should engage directly with Pashtun intellectuals, scholars, and activists—providing them with platforms in think tanks, universities, and the media. Second, India should offer humanitarian support, such as educational scholarships and community development programs in Pashtun areas. And third, India must take Pashtun issues to international forums, pushing for recognition of enforced disappearances, extrajudicial killings, and war crimes. By doing so, India can both support the Pashtun struggle and challenge Pakistan's narrative at the global level.

Historically, Shia Hazara and Turkmens have been persecuted in Afghanistan. Do you see ethnic riots breaking out under Taliban rule?

Tilak Devasher acknowledged the serious risks facing ethnic minorities—especially the Hazaras—under Taliban rule. He recounted the 1998 massacre of Hazaras in Mazar-e-Sharif

and pointed out that Shia mosques and cultural sites continue to be attacked. Although the Taliban are currently avoiding mass atrocities to gain international recognition, they have not stopped groups like ISIS-K from targeting minorities. He warned that the real danger lies in Pakistan's tendency to exploit ethnic divisions in Afghanistan to maintain strategic influence. Pakistan has a long history of supporting sectarian violence, and any escalation of unrest could be manipulated to justify deeper interference. While full-scale ethnic riots may not erupt immediately, Devasher cautioned that tensions are high, and the situation remains volatile.

.Conclusion of Q&A Session

The Q&A session concluded with a powerful and unified call for continued advocacy, international awareness, and collective resistance against the Pakistani state's ongoing repression. Each speaker underscored the unshakable resolve of the Pashtun people. They reiterated that Pashtuns will not remain silent—their struggle for justice and dignity will endure. The panelists urged the global community to recognize Pakistan's war crimes and take concrete steps toward accountability. They also emphasized that unity among oppressed ethnic groups—Pashtuns, Baloch, Sindhis, and others—remains the most effective force against Pakistan's entrenched military dictatorship.

Revisiting FATA (Federally Administered Tribal Areas): An Amalgamation of Internal and External Instability for Pakistan

Priyanshu Pandey

Introduction

FATA or the Federally Administered Tribal Areas of Pakistan was a highly unstable region of the South Asian nation for a long time. Established in the year 1970, the area got a special status in 1973. Historically the FATA was governed with a special status since the times of British colonial occupation, and that system was later adopted to be part of Pakistan's constitution too. The special status which was granted to FATA, was intended to bring stability and peace through the ease of governance to the region. But years of instability, ineffective governance strategies, and most importantly the "Talibanization" of the region due to Taliban militants entering for refuge and recruitment, led to FATA being marginalised and on a decline both economically and socially.

In 2018, through the 25th Amendment of the Pakistani constitution, the region of FATA was integrated into Khyber Pakhtunkhwa. The integration of the FATA was one of the most controversial decisions by the Pakistani Parliament.

Image 1: Map of FATA

The integration of FATA into Khyber Pakhtunkhwa was a step to focus more administrative machinery in the area and alleviate the struggles of the common people. It has been 5 years since the integration and there is a need to evaluate the changes and the development in the area, and also re-evaluate the areas of contention that were previously an issue in the FATA region.

Literature Review

FATA: Voice of the Unheard

The paper focuses on the plight of tribal people in the FATA region, brings to the forefront their struggles and provides a significantly important narrative of the Periphery which provides a realistic image of the so-called development and military administration of the region. Such data proves to be important in understanding the Socio-Political context but will benefit more with the addition of a socio-economic context. (Khan, n.d.)

Mainstreaming FATA: A Public Policy Imperative

The paper evaluates and develops a public policy mechanism in the context of the Frontier crimes regulation for the FATA region. It's a qualitative paper with a focus on three main elements which are historical analysis, demarking key players and development of a public policy. (Khan, n.d.)

Determinants of entrepreneurial behaviour in FATA Pakistan

The paper hypothesised entrepreneurial behaviour through Logistic regression models to understand the socio-economic factors that could lead to entrepreneurs investing in certain regions. The importance of this lies in the possibility of exploiting such patterns to Garner support for Industrial development in the FATA region. (Muhammad & Junaid, n.d.)

In all the papers that analyse and study FATA have been before or right after the merger in 2018. The current research literature lacks the analysis of FATA after the merger to prepare a study to understand the effect of the merger on the economic and political sphere of the area.

Methodology

The paper uses a modified PESTLE format to analyse the recent developments in erstwhile FATA to study the changes in the economic, political, social, and security spheres post the merger in 2018. It takes into account Political, Economic, Social, Technological, Legal and Environmental factors and does a cost-benefit analysis of the implemented welfare programmes in the area. The paper also studies the security and military reports in the region to also take into account terrorism, radicalism and militant activities. The analysis takes a deeper look into the Pashtun conflict and public uprising in Pakistan.

Economic Development

The economic situation of erstwhile FATA has always been rather tumultuous. Due to the historic imbalance and discrimination, the economic development of the tribal region has been difficult even with the presence of an abundance of natural resources. Although the natural resources in the erstwhile FATA are not easily available as the resources in plains and valleys further down south, they are still invaluable not just to the lifestyle of the tribals but also to the economic biosphere of the country.

In the last conducted census in the region in 2011, the FATA was housing more than 44 lakh people, and was said to have grown by 57% of its total population during the merger. This explosive population growth is not supported with an equal growth of the economy, making it a region of abject poverty and the lack of opportunities forces people to migrate outside to

balochistan and other regions making them a burden on the already strained resources of those areas.

Under this section, the paper evaluates five specific sections, that are:

Condition of employment and quality of life

Many records state the severity of the employment decline and economic collapse of the region, but little to no research has been done since the merger. This evaluation also is necessary because after merging with the nearby region of Khyber Pakhtunkhwa, migration for labour and safety has increased manifolds. So understanding the labour migration rate and preventing a workforce drain from the FATA region would be crucial to supporting any further economic or industrial development in the region.

The Global Data Lab has conducted regular research on the topics of national interest for Pakistan, including erstwhile FATA. From their latest comprehensive report in 2021, major inconsistencies are shown in the lives of people living in erstwhile FATA and those in other parts of Pakistan. The mean years of education for youngsters over 20 years of age in Pakistan is 5.78 years, while for erstwhile FATA it is 2.65. Falling at almost half of the national average it is also the lowest in the country. This prompts a huge lack of resources for education, leading to forced labour jobs and migration for the population. Without opportunities of skill development and education, it is impossible for people to seek employment and raise their quality of life.

In the year 2018, the then PM Nawaz Sharif had launched the 100-100-100 scheme for education promising 100% enrollment, study and graduation of students, with a special focus on girl child education for all of Pakistan, including erstwhile FATA. There were also

significant grants given out to the Islamia University in Peshawar to open another campus in the FATA region to facilitate further higher education and economic development.

But the ground image is far from the rosy narrative built by the central government. The region is filled with ghost schools that are a financial drain on the budget but add no value to the educated workforce. A lot of time these schools are fronts for money laundering and funding for militant activities in the region, which makes it pertinent to get rid of these schools. The leaders in erstwhile FATA, also known as MNAs have pleaded the government time and again to remove these ghost schools but to no avail. The plight of overall education is pathetic but it is worse for the female children in the region. Due to major influence of the Pashtun radicalists and militants from TTP (Tehrik-e Taliban Pakistan), most of the schools for girls have been forcefully shut down or demolished, making it a hostile and unsafe environment for people to send their children to schools. There were several protests throughout the region as a cry for help to the central government, and Waziristan even saw its first ever female-led protest for better education, but the requests have fallen on deaf ears (Wazir, 2022).

FATA also ranks the lowest in urbanisation and workforce growth at 6.27% and 1.78% respectively. Less than 2% of the total population is involved in regular, skill-based and organised employment. It is important to note the nature of employment as a lot of seasonal jobs crop up in erstwhile FATA, especially in agriculture during seasons of harvest, but that does not count under regular employment due to its seasonal nature and less availability.

On the other hand, central government reports on economic development and education in the erstwhile FATA region are phenomenal and positive, diametrically opposite from the ground studies done by private think tanks, independent journalists like Razia Mehsud and the common people. This is presumably done to show that the loans and investments from international

organisations are utilised effectively to maintain a state of liquidity by Pakistan, while covering up the pitiable condition of erstwhile FATA and Khyber-Pakhtunkhwa.

International Debt Burden

Pakistan suffers from a huge burden of international debt, and the past decade of economic hardships have only made the matters worse. At one of the all time highs, Pakistan's external debt was at $130+ Bn in March 2024. A very high percentage of this debt is in the form of non-remunerative loans for development projects like the BRI from China and National Development Finance Corporation (NDFC) Project by World Bank. While these centrally acquired loans are meant for development plans all over the country, there are several financial assistance provided to Pakistan with a special focus on erstwhile FATA[1]. This section explores those funds and seeks to analyse if they were utilised effectively.

Federally Administered Tribal Areas (FATA) Reconstruction and Rehabilitation Programme

This public sector loan was taken in 2017, before the integration into Khyber Pakhtunkhwa (KP). Valued at $803 Mn, the fund was a contribution from IDA, ISDB, China, USA, Italy, Germany and OPEC Funds[2]. The project was aimed at recovery efforts for the displaced families prior to the integration. This would include housing and public sector infrastructure development like hospitals, schools and other public sector enterprises. With the recent reports of ghost schools, lack of healthcare facilities and transport mechanisms are testament to the fact that these loans were not utilised to its maximum efficiency. This could be caused due to administrative inefficiency or corruption at the higher levels of administrative groups assigned to erstwhile FATA. Post-integration, as the federal boards were dissolved, there is little to no

1 https://www.ceicdata.com/en/indicator/pakistan/external-debt
2 https://opecfund.org/operations/list/federally-administered-tribal-areas-fata-reconstruction-and-rehabilitation-programme

possibility of tracing back the funds for development. Although it did not do much for the infrastructural development, the loan is still a financial burden on the nation.

Loan Agreement (Special Operations) for Federally Administered Tribal Areas Water Resources Development Project

These loan agreements with ADB (Asian Development Bank) were sanctioned in 2015 towards Pakistan for FATA, with a special focus on agriculture, water and natural resources. The proposed project under this fund was the FATA Water Resources Development Project over the Pakistan-Afghanistan border. The project has been completed and some of the key goals were achieved by the country, although in the final scoring given is satisfactory by the ABD which is the bare minimum rating rather than an actually efficient grade.

The project funds were utilised totally and various watershed and irrigation management infrastructure was made in various regions. One of the shortcomings of the plan was the low fund and time frame. With a higher budget and time, these efforts could be diversified into education and environment to further increase the quality of life in erstwhile FATA.

Smuggling and Illegal Agriculture

Due to the mountainous terrain of the FATA region and the significant economic decline, the area has become a hotbed for smuggling and trafficking activities. Supported by the local influx of the Taliban militants these illegal activities have propped up a significant part of their economy. Historically, FATA has been a hotbed of armed activities, either by insurgents or militants from the neighbouring Pashtun regions or Afghanistan. Post 1970s, FATA and its prominent town Darra Adam Khel emerged as the primary region of weapons manufacturing as it did not fall under Pakistani legal framework as this was pre-merger. Even though smuggling was prohibited by law, these manufactured weapons were supplied in large quantities and were

seen as the major driving force behind the Baloch insurgency of Pakistan and the coup d'état by PDPA in Afghanistan.

FATA was the main focal point for manufacturing the Small and Light Weapons (SALWs) that were cheap enough for the insurgents to smuggle and use regularly for militant and revolutionary activities. Over time, the expertise of weapons producers increased and there was a huge weapons network established that supplied weapons to Balochistan, Afghanistan and Pakistan, illegally through various weapon trade routes. This practice has reduced notably but has not stopped. Among the major buyers are the TTP insurgents, and smugglers from Afghanistan who use such weaponry due to their low price and untraceable acquisition (Malik, 2016).

Unsurprisingly this trade does not benefit the erstwhile FATA or Khyber-Pakhtunkhwa region economically, as most of this trade is done to support the drug trade from Afghanistan. The arms and ammunition were acquired in exchange of illicit drugs that are then distributed throughout Pakistan. During the 1980s Khyber-Pakhtunkhwa erstwhile North Western Frontier Province (NWFP) largely grew most of the poppy that was supplied into Central Asia. This trade surplus was used for various insurgent and terrorist activities, including the funding for Hizb-ul-Mujahideen and other branches of Lashkar. The cultivation of poppy was deeply supported by the state and army through illegal means and it was in erstwhile FATA that the line between the Pakistan government and militant leaders blurred. Since the merger, Pakistan has cracked down severely on opium and poppy production, which has shifted more and more towards Afghanistan. But due to an internal shortage, now there is an influx of poppy, that is usually in return for the weapons supplied by the producers.

Although primarily illegal, several reports by UNODC and Pakistan Central Government suggest that it is the drugs and arms trade that has supported the economy of the region and is

also the reason for the fragile peace. It is speculated that disruption of this trade will cause mass rioting due to lack of economic avenues and the overwhelming presence of militants. The Pakistan central government under Nawaz Sharif and Imran Khan have launched several "cleanliness" drives destroying the poppy seed cultivation and stockholders in erstwhile FATA, but the problem is much deeper than that. There has to be a systematic and rooted development of the area so that people are not forced into illegal smuggling activities just because they are lucrative.

Possibilities of resource expansion

To improve the economy of the region, there is a significant need to understand the resource and topographical condition, and in turn, suggest modes of investment and areas of infrastructural and manufacturing establishment. This can be done by cross-referencing any recent geographical analysis and cross-referencing it with investment trends of the Government and the private sector in Pakistan. The erstwhile FATA region is rich in natural resources, especially coal and petroleum reserves in Khyber Pakhtunkhwa and FATA. This diverse profile of copper, iron ore, marble , limestone and quartz, provide significant production and mining opportunities in the region.

The region can see a balanced development between agriculture and industrial development (Muhammad & Khan, 2020). Owing to the large scale military operations, the whole erstwhile FATA strip barely has urban developments with 97% of its population living in rural settings, which provides for a lot of opportunities for fresh developmental plans and investments.

Over $400 million have been invested in Pakistan with a specific focus on the erstwhile FATA region like the FATA development program by the German Federal Ministry of Economic Cooperation and Development, which was co-funded by the EU, given from 2016 to 2021, among others.

Preparing a report on these investments is crucial not only to provide a realistic image of the corruption and liquidity in the region but to also improve Pakistan's credibility in the international fear regarding foreign debt. Pakistan has already exceeded their foreign debt index and any more foreign direct investment can only arrive with a rise in credibility.

Talibanization and Militant Activities

The growth of the Taliban and local insurgencies in Pakistan has been one of the biggest problems in the country's internal and external security. The case of erstwhile FATA is not very different. The targeted legislation towards only certain militant groups, specifically with the national interest in mind, has led to a significant crisis for the Pakistani military. Initially, when militants from Uzbekistan, and erstwhile Chechnya came to Pakistan to fight for the freedom of their religion, they were arrested, and severely acted upon with special forces brought in from the US also. On the other hand, Pakistan's incorrect evaluation of Tehreek-e-Taliban Pakistan, Hizb-ul-Mujahideen, and the various branches of Lashkar, has landed the country in a situation of intense internal security threats.

The overlap of the administrative perception of non-state militants and the FATA revolutionaries led to a lot of propaganda deaths and civilian atrocities at the hands of the government. It spread a deep-rooted mistrust among the people who were already very afraid of the military and sceptical of the government.

Since before the Obama rule in the United States of America, FATA has been forcibly converted into a safe haven for militants from Afghanistan. After 2009, there was a shift in focus, when the Taliban developed by the US in the region was becoming difficult to handle, the US partnered with Pakistan to launch a series of operations in the tribal districts to root out all the terrorists and insurgents in the area. The military action had no oversight or evaluation and was ruthless in nature towards the locals. This sowed the seeds of the long standing fear and

aversion from the state army. The military oppression is one of the biggest reasons why the local Pashtun population finds themselves sympathising with the Tehrik e Taliban Pakistan's cause and tend to take part in harbouring them.

The militant insurgency is not just a security threat but is also rooted in the extreme social-economic disparity and the low quality of life among the people. The lack of faith in the nation, and misadministration invite more and more people to join the cause of these non-state militant and terrorist organisations. Pakistan has been unsuccessful in dealing with such problematic actors and hence there is a need to re-evaluate the presence of these organisations and their growth and influence. With the Taliban forming the state rule in Afghanistan, new challenges can sprout among these Talibanized areas of Pakistan. The motive of evaluation should be to understand the current situation keeping in mind the recent developments in the geopolitical scenarios, and the firm establishment and rise of Tehreek-e-Taliban Pakistan, and suggest plans of action that can be implemented at the local, national and international level to not only improved the stability of the region but also bolster Pakistan's image as the nation that stands against terrorism. The funding from these programmes are available from the FATA-specific investments from various countries, to make sure that the policy makers of Pakistan are well aware of the ground level problems in the region before making decisions.

Operations by Pakistani Armed Forces

The region of erstwhile FATA was a hotbed for various military operations, but one region saw the major concentration of them. Waziristan was a part of erstwhile defunct FATA region and is now integrated into Khyber Pakhtunkhwa. Waziristan was an important base for the Tehreek-e-Taliban Pakistan, and was an area that was buzzing with militant activities. There were several operations by the Pakistan armed forces like the Operation Zarb-e-Azb in 2014 to clear out the militants from North Waziristan and Operation al-Mizan in 2006 to remove foreign militants.

Both these operations, especially the 2014 Operation Zarb-e-Azb were criticised heavily for the inhuman atrocities committed by the Pakistan army on the common Pashtuns. The operations destroyed the shelter and livelihoods of millions in the region, severely harming the socio-political equilibrium. Since then, there have been various reports of human rights violations and complaints of inadequate compensation by the government. From various reports, an estimated 80,000 people including soldiers, civilians and militants have died in the region, and the situation has not stabilised still.

Taking into account recent development, most of the civilians in the FATA are against any new military operation being conducted in the region. With the support from tribal elders, the opposition party (Pakistan Tehreek-e-insaf) has presented a strong case for de-escalating any active conflict and resorting to peaceful ways, due to action portfolio that requires human rights watch, extensive research and targeted operations based on those research, against militant activities. The first step always will be to gain the trust of the people, for them to support this venture on the public front[3].

This paper establishes some literature for the formation of a separate committee that seeks to establish a constitutionally mandated administrative system after a thorough study of the socio-political and economic context of FATA and PATA. While also collaborating with the military wings to work on the matter would assist in the success rate of the committee.

Administrative Issues

Before the integration in 2018, the region of FATA was incredibly impoverished, suffering from low education, income and employment rates. This situation resulted due to a mix of political instability, internal disharmony, geographical alienation, misadministration and

3 https://www.rferl.org/a/khyber-pakhtunkhwa-pakistan-military-operation-compensation/33020533.html

discrimination. The literacy and employment rate of the region was far below the national average. The infrastructure development of the region too was almost non-existent due to the lack of investments. The Government of Pakistan, both under democratic and military rule, did not invest in research or evaluation of the FATA region, which is evident from some of the major laws from the age of British occupation still being implemented.

The tribesmen of FATA also believed that the integration with Khyber Pakhtunkhwa will lead to a tight clasp from the federal administration that will destroy their way of life. They also expressed significant distrust in the fairness of the central government and felt threatened from the dissolution of the Tribal Jirgas. With the integration of FATA into Khyber Pakhtunkhwa, most of the economic and administrative burden has fallen on the government bodies in Khyber Pakhtunkhwa. The neighbouring region of Balochistan has also been instrumental in providing stability through labour markets, resource allocation and shouldering economic responsibility. Understanding the burdens on Khyber Pakhtunkhwa and Balochistan will provide the required data to develop a plan for political and economic machinery that can be established to reduce the strain on the already dispersed government resources.

The current framework of the FATA administration allows a PATA (Provincially Administered Tribal Areas) form of governance. Since the integration into Khyber, a lot of regions fall under the Provincially Administered Tribal Areas instead of Federally Administered. In both these situations, the tribal areas are exempted from any benefits or support from Pakistan’s constitution and fall outside of its purview. The decisions previously taken by the President are now taken by Provincial Governors who report directly to the President. This prevents any judicial jurisprudence in the region for the people, meaning that there are little to no rights granted to them as citizens of Pakistan.

The Provincial Governors have been entrusted with a lot of administrative power for economic, socio-political and military decisions, with almost non-existent oversight. This lack of a system of checks and balances allows these leaders to completely undermine the local governance structure of Jirgas, that are supposed to be consulted before decision-making regarding the PATA and FATA region.

The Pashtun Problem

The Pashtun Rebellion by the PTM (Pashtun Tahafuz Movement) is one aspect that cannot be overlooked in the conversation about FATA. The PTM is a microcosm of all the reasons Pakistan administration has failed in the region. The rebellion has an ethnic title but not an ethnic demand. The primary concern of the people is the extensive military action, seclusion and alienation from the rest of Pakistan and the military support to the militants. Although many of these claims of militant support have not yet been corroborated but the people are angry at militant leaders like Ehsanullah Ehsan, the spokesperson of Taliban was allowed a TV interview while any reporters or coverage has been restricted for the people of FATA. The disgruntled population calls for a proper evaluation of the Zarb-e-Azb operation by the military, to get justice for unlawful killings and detention in FATA.

This non violent rebellion brings to light several important problems in the administrative system that have been blocked by Pakistan for over a decade, including the last 5 years after the integration of the tribal regions. One of the demands of the PTM, despite being called terrorists and dissenters like the colonial laws, is to establish a democratic committee under the Pakistani constitution to govern the tribal regions with the jirgas and local leaders included in the process.

Role of a Reformation Committee

The committee that was previously suggested, would have a two-step responsibility, with the primary role to investigate and evaluate the current condition of FATA. Due to a journalist and research blockade, the region has suffered without any tailored development or reformation plans. So this Reformation committee should focus first on building comprehensive reports on topography, population, economic constituency, socio-political problems, illegal activities, military and militant evaluation, before acting on stabilising operations.

To make the process democratic, the constituents of the committee should have 40% representation from the Jirgas and local leaders to make sure that their narrative is not ignored. With the rest of the seats to be distributed among central government representatives (15%), economic and political researchers (30%) and the military heads (15%). This would ensure that the output of the committee is easy to implement and just towards all the parties involved. The committee should also report directly to the Parliament with the full constitution being applicable on the operations so as to not alienate the region any further.

The data and the reports to be considered would be multitudinal in nature and each section of the evaluation should have a separate methodology addressing it. The research could be a blend of qualitative and quantitative reports and will focus on government-available data cross-reference with independent research and reports of internationally credible Organisations. For the evaluation of foreign direct investments, reports from the country of origin will also be taken into consideration as a viable source of information.

For the geographical and topographical evaluation, census and mapping reports, along with a climate analysis available from government sources can be taken into account, to suggest a plausible industrial plan. Any such intervention or suggestion can be compared to the already existing plans of action for development and economic growth in the erstwhile FATA region.

Any such suggestion will not necessarily be a new implementation but can also be an extension of the current programs. For this, the current implemented plans of development should also be analysed for possible loopholes or scope of improvement.

It would also be the responsibility of this committee to find a middle ground and integrate the Jirga form of governance and the Pashtun Code of Conduct into the administrative system to prevent the erosion of the way of life for the people in the erstwhile FATA region.

Conclusion

In conclusion, this paper aims to evaluate the status of the erstwhile FATA region after 5 years of integration into Khyber Pakhtunkhwa and build a formative conclusion toward the success and failures of the program. The paper explores various economic and socio-political issues that are not resolved after more than 5 years of the merger of erstwhile FATA with Pakistan. Research shows a huge disparity between the cosmetic development carried out by the government and the ground reality of the region. To mitigate this, the research suggests a reformation committee with a democratic composition to evaluate and form policy recommendations for the region, to ensure a democratic integration and balanced growth. It is a long way to go, but understanding the problem would be a positive first step.

References

Afzal, M. (2020, February 7). Why is Pakistan's military repressing a huge, nonviolent Pashtun protest movement? Brookings Institution. *https://www.brookings.edu/articles/why-is-pakistans-military-repressing-a-huge-nonviolent-pashtun-protest-movement/*

Asrar, S., & Malik, W. (2019). Pakistan's tribal areas: 'Neither faith nor union found'. AlJazeera. *https://interactive.aljazeera.com/aje/2019/pakistans-tribal-areas-fata/index.html*

Global Data LAb. (2023). Area Databse – Pakistan.

Khan, A. (n.d.). Indo-US Nuclear Deal: Altering Global Nuclear Order. Indo-US Nuclear Deal: Altering Global Nuclear Order. Retrieved May 28, 2024, from *https://www.issi.org.pk/wp-content/uploads/2014/06/1315805584_65172321.pdf*

Khan, M. Z. (n.d.). Mainstreaming FATA: A Public Policy Imperative. Researchgate. Retrieved May 28, 2024, from *https://www.researchgate.net/publication/330146921_Mainstreaming_FATA_A_Public_Policy_Imperative*

Malik, A. (2016). Darra Adam Khel "Home Grown" Weapons. ASPJ Africa & Francophonie, 1st Quarter, 73-96.

Muhammad, A., & Junaid, M. (n.d.). Wikipedia. Retrieved May 28, 2024, from https://www.ifpri.org/publication/determinants-entrepreneurial-behaviour-fata-pakistan

Muhammad, N., & Khan, M. M. A. (2020, June). Understanding Economic Potential of Erstwhile FATA and the Challenges Ahead. *Orient Research Journal of Social Sciences*, *5*(1), 81-93.

Wazir, A. (2022). Status of girls' education in merged districts of erstwhile Fata. *The Frontier Post*. https://thefrontierpost.com/status-of-girls-education-in-merged-districts-of-erstwhile-fata/

The Indic Centre for Internal Security Studies (ICISS)

The Indic Centre for Internal Security Studies (ICISS) is a strategic research division under the Indic Researchers Forum that provides an intellectual platform for scholars, practitioners, and policymakers to critically examine India's evolving internal security landscape. India today faces a convergence of kinetic and non-kinetic threats—ranging from insurgency, terrorism, and organized crime to radical ideologies, cyber threats, and information warfare.

ICISS is dedicated to fostering a cohesive, India-centric understanding of these security challenges by analyzing doctrinal responses, institutional capacity, legal frameworks, and strategic innovations. The Centre's research agenda includes counter-radicalization, intelligence reforms, border management, civil-military coordination, and threat forecasting. Through rigorous analysis, ICISS aims to strengthen India's internal resilience and national defense posture in an era of hybrid and asymmetric threats.

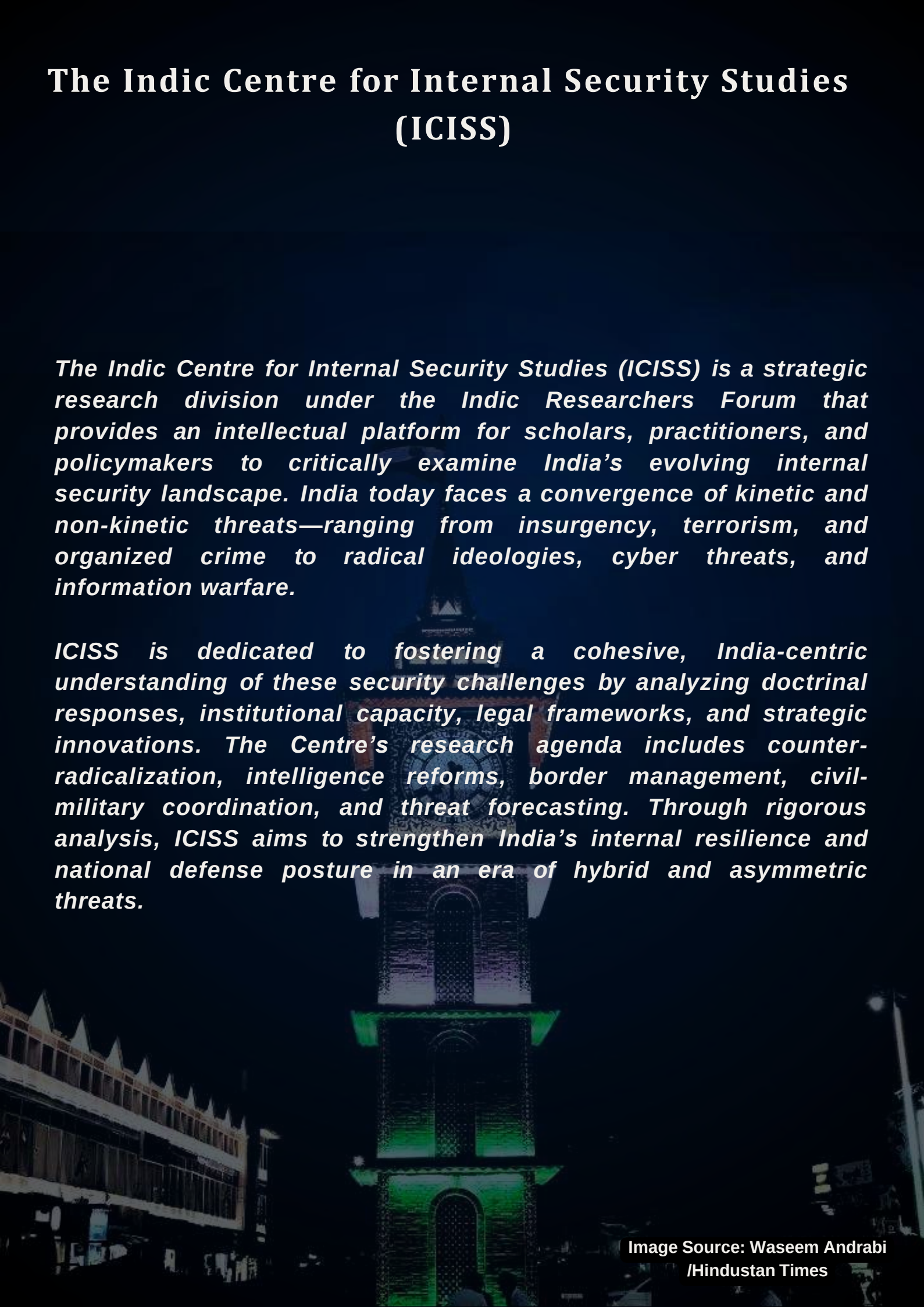
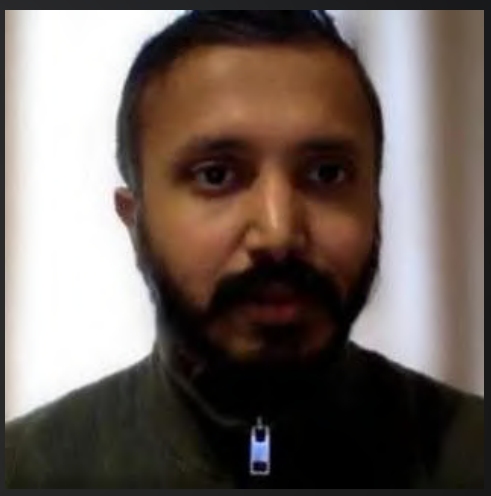


Image Source: Waseem Andrabi /Hindustan Times

India's Intelligence Culture & the Challenge of Reforms

i» co»vc»s»l'io» »il'h



Arghish Akolkar

Dr. Dheeraj PC

Imaofte Source: Edoftar Su | Reuters

India’s Intelligence Culture and the Challenge of Reforms

Transcribed by Sathya Pulukuri

Host: Arghish Akolkar, Contributing Editor, Indic Researchers Forum

Distinguished Speaker: Dr. Dheeraj Paramesha Chaya

Dr. Dheeraj Paramesha Chaya is a lecturer in Intelligence and International Security at the School of Criminology, Sociology and Policing at the University of Hull, UK. He secured a PhD in Intelligence Studies from the University of Leicester for his study on the impact of India's intelligence culture on its strategic surprises.Dheeraj is the author of the book 'India's Intelligence Culture and Strategic Surprises: Spying for South Block', which is the first academic work on India's foreign intelligence. Besides academic research, Dheeraj has been imparting training to Indian security forces in the fields of intelligence and national security. He is the author of the intelligence training manual of the Karnataka State Intelligence. He has also been delivering training lectures to the Internal Security Division and the Intelligence Wing of the Karnataka State Police on intelligence, counterintelligence, radicalisation, religious fundamentalism, and counterterrorism. Dheeraj's research interests lie in the area of strategic intelligence and counterintelligence for national security, sub-state conflicts, radicalisation and de-radicalisation.

1. Arghish Akolkar: Sir, in your book, you discuss Kautilyan intelligence culture and how *Rajadharma* shaped ancient Indian statecraft. Do you think our intelligence agencies today still embody that ethos? How has India's intelligence culture evolved since then?

Dr. Dheeraj PC: Thank you. The *Arthashastra* is often reduced to its references to spies, but that's a narrow reading. Kautilya structured intelligence as a civilizational tool serving three key objectives: *pālana* (administration), *yogakṣema* (welfare), and *rakṣaṇa* (protection). It wasn't just about espionage—it was about statecraft guided by *Rajadharma*.

In post-colonial India, we inherited British structures but lost that philosophical grounding. Being a democracy, *Rajadharma* had to be redefined through political leadership. Unfortunately, that leadership never articulated a vision. What emerged instead was a managerial model shaped by intelligence professionals rather than state ideology.

Figures like B.N. Malik and R.N. Kao brought a certain long-term vision and commitment to national interest, somewhat aligned with Kautilyan thinking. But that spirit never translated into institutional continuity. As a result, India's intelligence today retains fragments of its civilizational heritage, but not by design—more by inertia and individual leadership.

2. Arghish Akolkar: In your book, you analyze intelligence failures like the 1962 and Kargil wars. You make a distinction between "information gaps" and "knowledge gaps." Could you explain this framework? Also, what role does political leadership play in intelligence failure or success?

Dr. Dheeraj PC: Yes, just to clarify, I didn't cover 26/11 in the book; I stopped in 1999. I deliberately compared two failures (1962 and Kargil) with one success (1971), because we often study only failures, without asking why something worked. Information gaps are

inevitable—states like China or Pakistan will always protect sensitive data. But what really causes failure is a *knowledge gap*—misreading or ignoring the data we already have.

Take 1962: the Intelligence Bureau had warned for years that China would become adversarial. But Nehru believed in Asian solidarity, and ignored those assessments. That's not an intelligence failure—it's a political miscalculation.

In 1999, R&AW didn't assume that diplomacy or nuclear tests would change Pakistan's strategic posture. But policymakers did. When leaders act on instinct instead of institutional assessments, strategic surprise follows.

The military too must understand intelligence limits. Strategic intelligence gives a broad picture, but operational awareness—what the enemy might do in a specific theatre—has to come from within. Yet our military, like others, often undervalues intellectual study in favor of battlefield preparation.

For example, nine months before 1962, a retired general wrote in the USI Journal that China follows unconventional war tactics based on Korean experience. But we still weren't prepared. This gap in understanding the adversary—despite available signals—is what I call a knowledge gap.

3. Arghish Akolkar: We've seen the Five Eyes alliance act cohesively, especially during the Khalistan issue. Similarly, Islamic nations often align on geopolitical matters. Do civilizational identities shape intelligence cooperation? What does that mean for a civilizational state like India?

Dr. Dheeraj PC: Yes, civilizational identity matters—but interests matter more. During the Cold War, the West favored Pakistan not just for its geography but also because, as an Islamic state, it offered inroads into the Middle East. So, culture played a role, but material utility was

decisive. India wasn't part of Five Eyes, but that didn't mean we were isolated. We cultivated strong backchannel ties—with France, Israel, and even the U.S. Despite overt tensions, intelligence cooperation often continued quietly.

Post-26/11, India was brought into SIGPAC, a U.S.-led signals intelligence group. That inclusion wasn't because of cultural proximity—it was because India had value. That said, India sometimes "fires before it's ready." From Krishna Menon to today's assertive diplomacy, we've often projected strength prematurely. There's a perception—especially in the West—that India is becoming too aggressive. Whether that's accurate or not, it affects how we're viewed. India has no permanent friends. As a civilizational state, our leverage lies in what we bring to the table—demographics, geography, intelligence capabilities. The world engages with you when you add value. Cultural alignment alone won't open doors; strategic relevance will.

4. Arghish Akolkar: Should India adopt intelligence legislation or reforms like the U.S. Church Committee or UK oversight mechanisms? Would that bring clarity to intelligence mandates and limits?

Dr. Dheeraj PC: I'm still forming a settled view on this. Many argue that legislation would improve intelligence performance, but I'm not convinced. Countries like the U.S. and UK have had spectacular intelligence failures—often worse than ours—despite having robust legal frameworks. India's strategic environment is uniquely volatile. The kinds of threats we face are far more immediate and diverse than what Western democracies deal with. So, importing their models blindly won't work.

That said, I support greater accountability—especially around misuse of resources. Archival evidence shows that even powerful figures like B.N. Malik couldn't bypass bureaucratic checks easily. There were informal safeguards.

What's missing today is transparency. Declassification policies are weak. Ironically, I was able to write about Indian intelligence using declassified American and British sources—not Indian ones. We need to let researchers examine our past. Accountability doesn't only mean legal oversight; it also means enabling historical understanding.

5. Arghish Akolkar: Nearly 60% of intelligence and enforcement officers are on deputation. What structural reforms do you recommend, especially regarding recruitment and continuity within the Indian intelligence framework?

Dr. Dheeraj PC: This is a critical structural flaw in the Indian intelligence system. The widespread reliance on deputation—where officers are temporarily posted from other services—severely undermines continuity, expertise, and institutional memory. Intelligence is not a short-term assignment; it's a domain that demands long-term immersion, area specialization, and doctrinal consistency. Deputation disrupts that completely.

In the early years of the Republic, there were attempts to correct this. Leaders like B.N. Malik and R.N. Kao envisioned dedicated services for intelligence. Malik introduced the Executive Management System (EMS) within the IB, and Kao later developed the Research and Analysis Service (RAS) to staff R&AW with specially trained officers. These systems aimed to create a professional, in-house cadre committed to long-term national security goals.

Unfortunately, these reforms were eventually dismantled, largely due to bureaucratic resistance—especially from the Indian Police Service (IPS) cadre, which preferred maintaining its control over key intelligence postings. Over time, intelligence agencies became stepping stones in the career ladder of generalist officers rather than being treated as institutions requiring domain-specific commitment.

Today, most officers come on deputation for 3–5 years, often for personal or career advancement. They neither enter with the necessary expertise, nor stay long enough to build any. This creates a revolving-door effect where strategic knowledge, institutional learning, and area specialization are lost just as they are being developed.

The deeper problem lies with the UPSC recruitment model itself. It was designed for an administrative state—not a national security state operating in an age of cyber warfare, disinformation, and AI-based threats. You cannot realistically expect a future cyber warfare specialist to clear the Civil Services Exam, train in revenue, postal, or administrative law, and then pivot into strategic technology or counterintelligence.

We need to explore two models:

- First, build a dedicated intelligence cadre—similar to how diplomats have the IFS or soldiers have the NDA pipeline—where talent is identified, trained, and retained with a long-term institutional vision.
- Second, aggressively embrace lateral entry. India has world-class minds in academia, technology firms, data analytics, and even the startup ecosystem. But we don’t yet have a robust, trusted mechanism to recruit and absorb them into national security roles.

Until we fix this pipeline—both structurally and culturally—India’s intelligence system will remain reactive, overstretched, and under-equipped to handle the demands of 21st-century threats.

6. Arghish Akolkar: Given the secrecy around intelligence, how can institutional knowledge be preserved or passed down? Do you see declassification as essential to building expertise and continuity?

Dr. Dheeraj PC: Absolutely—and I consider this one of the most urgent but neglected areas of reform. A functioning intelligence system cannot operate effectively in a vacuum. Without institutional memory, each generation of officers ends up reinventing the wheel. The reality today is that most officers—especially those on short deputation—enter intelligence agencies with no access to prior operations, lessons learned, or regional case studies. There's simply no knowledge infrastructure in place.

There are no internal histories. No curated case studies. No documented reflections on past decisions, successes, or failures. In fact, and this is the irony, I had to rely almost entirely on U.S. and British declassified records to write my book on Indian intelligence. Our own files remain completely sealed—even decades after the fact.

This level of opacity not only hinders academic research but also paralyzes internal institutional learning. Officers posted in intelligence roles often operate without context—without understanding why a particular region, actor, or network matters, or what past responses have looked like.

Declassification does not mean revealing sensitive operational details in real time. What it means is developing a structured, secure, and phased system of internal dissemination and limited public access—so that India's own scholars, analysts, and future officers can begin to study patterns, behaviors, and strategic choices. It's about building a body of work—a "national security literature," if you will—that helps future generations think critically, historically, and strategically. We urgently need to develop what I call an intelligence learning ecosystem—a model that includes:

- Secure internal case libraries for officers,
- Collaborative research with vetted academic partners, and
- Publicly accessible historical material to shape policy discourse and intellectual continuity.

  Without that, we are essentially sending new officers into highly sensitive roles without a map. It's like navigating a minefield with no knowledge of where previous explosions happened.

7. Arghish Akolkar: As threats like cyber warfare grow in scale and sophistication, how should India rethink its recruitment model for intelligence services to remain future-ready?

Dr. Dheeraj PC: This is a pressing question. If we're serious about countering cyber threats—ranging from AI-enabled espionage to data manipulation and infrastructure attacks—we must first admit that our current recruitment framework is fundamentally inadequate. The UPSC system, designed for building a classical bureaucracy, is ill-suited to identify or nurture cyber talent. Let me put it bluntly: some of the most talented individuals in the cyber domain today are teenagers or early-career professionals operating in decentralized, non-traditional ecosystems. Many of them possess skills that outpace what conventional civil service training can offer. You cannot reasonably expect such individuals to sit for the Civil Services Exam, undergo generalist administrative postings in departments like revenue or transport, and then transition into cybersecurity or AI-based counterintelligence. It's not just inefficient—it's implausible.

The solution lies in creating alternative entry pathways into intelligence services—particularly for technical and analytical domains. This means:

- Opening up lateral entry into specialized wings,
- Building partnerships with academic institutions, research labs, and tech startups, and

- Creating semi-autonomous intelligence research units, akin to the RAND Corporation in the U.S., which can work closely with the government while retaining intellectual and operational flexibility.

Of course, this raises important questions:

- Which domains must remain under direct state control due to national security sensitivities?
- And which areas—such as open-source intelligence, threat modeling, or cyber defense simulations—can benefit from partnerships with private sector actors?

Unless we resolve these boundary issues, we'll continue relying on outdated, bureaucratic mechanisms to address threats that evolve faster than our organizational charts. We need a modular, layered intelligence ecosystem where domain knowledge, not just bureaucratic seniority, defines leadership and innovation.

8. Arghish Akolkar: What is the core challenge holding back intelligence reform in India? And what do you see as the first step forward?

Dr. Dheeraj PC: The biggest issue is that reform has always been tied to personalities—not systems. When someone like B.N. Malik or R.N. Kao comes along, things improve. But once they retire, the entire structure loses direction. That's not sustainable. We need systemic reform across the board—bureaucratic, political, cultural. Deputation won't work if incentives remain misaligned. Intelligence will stay reactive if we don't have a coherent national security strategy. India still doesn't have a public national security doctrine. Without that, different governments make different choices, and there's no institutional memory. Even during the Kargil war, the National Security Council Secretariat existed—but it had little operational influence. To fix

this, we must articulate long-term national goals, institutionalize training, declassify history, and professionalize recruitment. Intelligence should serve national security, not political convenience. Until we make that shift, reforms will remain cosmetic.

Examining External Support for ULFA: Implications for Security in Northeast India

Evin K.Vinoy

Introduction

India's Northeastern region, comprising eight states, is a complex geopolitical landscape marked by ethnic diversity, international borders, and a history of insurgencies driven by demands for autonomy or secession. These long-standing insurgencies, fueled by a range of grievances including socioeconomic marginalisation and ethnic tensions, have posed a formidable challenge to India's security apparatus. Adding to these internal strife are allegations that certain insurgent groups in the region have received covert support from external actors. The potential involvement of external involvement in abetting insurgencies within India's sovereign territory is a matter of grave concern for New Delhi. The Northeast's strategic location, situated along the borders with China, Myanmar, Bangladesh, and Bhutan, renders it a zone of immense geopolitical significance. Any external meddling that exacerbates the existing insurgencies could destabilise the region, undermine India's territorial integrity, and potentially strain India's already tense relations with China.

This research aims to critically examine the extent and nature of external support to insurgent outfits operating in India's Northeast, with a specific focus on the United Liberation Front of Asom (ULFA). Furthermore, this study delves into the strategic motivations that could potentially drive external involvement in ULFA’s insurgent activities. It explores whether such support is an instrument to disrupt India’s regional security, an attempt to create strategic leverage by exploiting unrest along India's periphery, or a retaliatory measure against India's perceived threats to external interests.

Literature Review

The United Liberation Front of Asom (ULFA) emerged in the late 1970s amidst socio-political unrest in Assam, rooted in long-standing ethnic and economic tensions. The group's objectives evolved from expelling "foreign nationals" to achieving complete sovereignty for Assam. This transition reflected a blend of historical grievances, such as marginalisation under colonial rule and demographic shifts due to large-scale migration, which the Assamese perceived as threats to their identity (Mahanta, 2013; Khanikar, 2018). ULFA's operational capabilities were significantly bolstered by external support, particularly in its formative years. Alliances with regional insurgent groups like the National Socialist Council of Nagaland (NSCN) facilitated access to training and arms. This collaboration marked a shift towards militarization, as ULFA adopted guerrilla warfare techniques and began formulating a constitution to legitimize its insurgency (Bhattacharya, 2023).

ULFA's attempts to secure Chinese backing achieved limited success, with early efforts, such as a 1986 memorandum to the Chinese Communist Party (Bhattacharya, 2023). However, indirect connections through the Kachin Independence Army (KIA) in Myanmar hinted at peripheral Chinese influence in regional insurgent dynamics. These ties provided ULFA with training and arms, reinforcing its attempts to build a broader network of alliances in the region (Mahanta, 2013). Meanwhile, ULFA's engagements with Pakistan’s Inter-Services Intelligence (ISI) proved more substantive, offering both financial and strategic support. Public acknowledgments by ULFA leaders revealed that these collaborations were particularly critical during periods like the Kargil War, when ULFA allegedly provided intelligence to Pakistan.

Additionally, Bangladesh's Directorate General of Forces Intelligence (DGFI) played a vital role, providing safe havens, training camps, and logistical support throughout the 1990s and early 2000s, driven by its strategic interest in counterbalancing Indian regional dominance (Bhattacharya, 2023; Mahanta, 2013).

The external support networks of ULFA have posed significant challenges to India's counterinsurgency efforts. Studies by Waterman (2022) highlight how these networks enabled ULFA to sustain operations despite military offensives like Operation All Clear in Bhutan. The availability of cross-border sanctuaries and funding allowed ULFA to regroup and adapt its strategies, complicating Indian security forces' efforts to neutralise the insurgency (Dutta, 2014).

The literature review reveals a complex interplay between ULFA's historical roots, its operational strategies, and the external support it has received. While alliances with external actors like Pakistan's ISI and Bangladesh's DGFI bolstered ULFA's capabilities, they also contributed to the group's transformation and eventual decline in public support. Future research could focus on comparative analyses of insurgencies in Northeast India to explore broader patterns of external influence and the efficacy of counterinsurgency measures.

Methodology

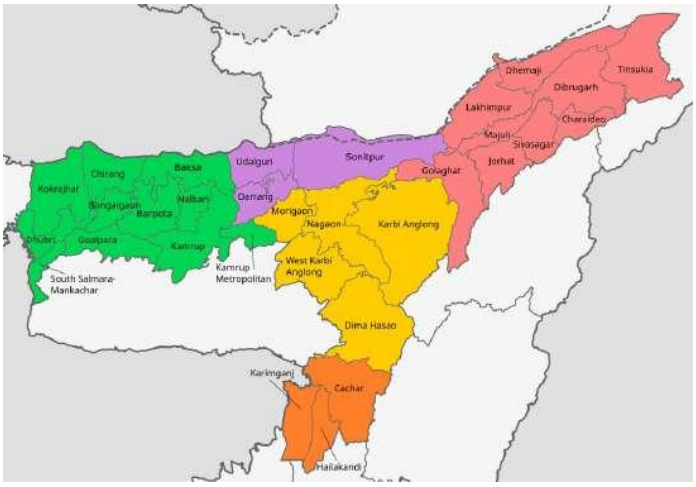
The methodology of this paper primarily involved conducting a systematic reading and literature review of existing papers and reports related to the external support for ULFA in Northeast India. The objective was to gather, analyse, and synthesise relevant information to understand the extent and nature of external involvement, its impact on the insurgencies, and the broader implications on India's national security. A comprehensive search was conducted

across several academic databases to locate relevant papers, articles, and reports. These databases included JSTOR, Google Scholar, Taylor & Francis, and other reputable academic repositories. Keywords and phrases used in the search included "External support for insurgent groups in Northeast India," "insurgency in Northeast India," "foreign support for insurgencies," and other related terms. Specific filters (e.g., publication date, peer-reviewed articles) were applied to refine the search results and ensure the inclusion of more pertinent studies.

The selection criteria for the literature review were based on relevance, credibility, and contribution to the understanding of external involvement in supporting ULFA in Northeast India. Only peer-reviewed articles, government reports, and reputable institutional publications were considered to ensure the quality and reliability of the information.

Background and Historical Context

Assam's history is deeply rooted in its distinct identity, shaped by a history separate from mainland India. This difference traces back to its geographical separation, being connected to the rest of India only by a narrow 22-kilometre land corridor (Mahanta, 2013). This isolationfostered a sense of distinctiveness, which some groups translated into aspirations for independence even before India gained its own freedom from British rule (Khanikar, 2018).



The arrival of the Ahoms in the 13th century marked a turning point. Through their advanced military and agricultural skills, they unified the numerous small kingdoms, laying the groundwork for an Assamese nationality (Khanikar, 2013). This unification, however, doesn't negate the historical presence of diverse sovereignties and fluid cultural and territorial boundaries that characterised Assam until the British ultimately took control in 1826 (Mahanta, 2013). The British, seeking to maximise profits from tea plantations, introduced large-scale labour immigration from other parts of India, altering the demographic landscape. While initially supported by the local population, this influx, particularly of Bengali farmers, sparked tensions. This period saw the seeds of an Assamese identity, rooted in anxieties about cultural and economic dominance by outsiders, a theme that would resonate through later movements (Khanikar, 2013).

After independence in 1947, the desire to protect Assamese culture, language, and resources from perceived threats, including immigration and exploitation from New Delhi, fueled a distinct Assamese identity. The Assam Movement of 1979-1985 exemplifies this sentiment, opposing perceived manipulation of electoral lists to favour certain groups and demanding the expulsion of "foreigners." This movement saw participation from civil society and student organisations (Waterman, 2023). The United Liberation Front of Assam (ULFA), emerging from the more radical elements of the Assam Movement, sought a complete separation from India. ULFA viewed the Indian state's control as "colonial" and aimed to establish an independent Assam. Reaching its peak in the late 1980s and 1990s, ULFA became a significant force in Assam, embodying the frustrations and aspirations of many (Khanikar, 2018).

Historical Background of ULFA

In the late 1970s and early 1980s, several groups in Assam engaged in efforts to address the issue of "foreign nationals," culminating in the formation of the United Liberation Front of Asom (ULFA). The group's initial focus was on expelling foreigners, controlling the influence of outsiders, and acquiring weapons from separatist groups in Manipur and Nagaland. A key figure in these early stages was Anup Chetia, ULFA's organising secretary, who spearheaded efforts to connect with rebel groups in neighbouring states (Bhattacharya, 2023). One of ULFA's first acts was the bombing of a pipeline carrying motor spirit from Digboi to Tinsukia in 1981, followed by another bombing in Sivasagar. Seeking weapons and training, ULFA attempted to establish contact with the National Socialist Council of Nagaland (NSCN) in Dimapur, Nagaland, between 1980 and 1982, but these attempts were unsuccessful. However, ULFA did manage to procure some weapons through other sources during this period. A breakthrough occurred in mid-1982 when a three-person ULFA squad met with Angelus Shimray, the foreign secretary of the NSCN. This meeting resulted in the suggestion that ULFA formalise its goals by creating a constitution and manifesto (Bhattacharya, 2023).

Towards the end of 1982, ULFA formed a central committee, but a formal constitution and clearly defined goals were still lacking. The common objective among most members remained the expulsion of foreign nationals from Assam, a goal established during a convention in Namrup four years prior. The concept of sovereignty as a goal was limited to discussions among a select few functionaries. (Bhattacharya, 2023). By mid-1985, ULFA's prominence grew as a result of the signing of the Assam Accord. While intended to end the six-year agitation against foreign nationals, the Accord was met with disapproval by hardliners who perceived it as a capitulation to the Indian government. ULFA's denouncement of the Accord

positioned the group as a radical alternative for those dissatisfied with the agreement. Capitalising on its expanded support base, ULFA issued a pamphlet in late 1985 outlining its objectives, which included "liberating" Assam from India through armed struggle. The pamphlet asserted that Assam had never been a part of India, thereby framing the movement as a liberation struggle rather than a secessionist one (Bhattacharya, 2023).

Seeking support for its campaign, ULFA made unsuccessful attempts to reach out to the Palestinian Liberation Organization (PLO) in Bangladesh. Subsequently, the group turned its attention to Punjab, where militancy was on the rise, in hopes of procuring weapons. Despite several meetings with rebel groups, including those associated with Jarnail Singh Bhindranwale, ULFA's efforts to secure weapons and establish lasting alliances in Punjab were unsuccessful. It was at an NSCN camp in Myanmar that ULFA finally drafted a constitution. This constitution, finalised in 1987, established ULFA as a "revolutionary political party" with a military wing operating under its control. The constitution outlined a two-stage revolution: first, achieving Assam's independence, followed by the implementation of "scientific socialism" (Bhattacharya, 2023).

By the close of 1987, ULFA had made strides in establishing a parallel government in Assam, marked by an increase in violence and expansion of its operations. The group's activities included assassinations of political opponents and government officials, with an estimated 113 killings attributed to ULFA between 1986 and 1990. ULFA's influence and control in Assam reached its peak in the late 1980s, a period that coincided with the declining popularity of the ruling Asom Gana Parishad (AGP). However, this period also revealed the organisation's underlying weaknesses. The group's leadership, primarily consisting of Paresh Baruah, Arabinda Rajkhowa, and Anup Chetia, lacked experience. Internal power struggles and a lack

of strategic planning hindered ULFA's effectiveness. The organisation also failed to establish clear guidelines for recruitment, leading to a decline in discipline and commitment among its ranks.

The first split in ULFA occurred as a result of peace negotiations with the Indian government in early 1992. While some members, particularly those associated with the All-Assam Students' Union (AASU) in Guwahati, were open to the peace process, the hardliners led by Paresh Baruah rejected the offer. This ultimately led to the division of ULFA into two factions: those who surrendered to the government (SULFA) and those who remained committed to the armed struggle for independence (Bhattacharya, 2023).

The Pro-Talks Faction, which took shape by the late 1990s, was led by Anup Chetia and Arabinda Rajkhowa. This group believed in engaging in peace talks with the Indian government, advocating for the release of imprisoned cadres and addressing significant issues like the influx of Bangladeshi migrants in Assam. The faction emphasised dialogue as a means to achieve their goals and considered leveraging abductions to negotiate the release of their jailed members (Bhattacharya, 2023). In contrast, the Anti-Talks Faction, headed by Paresh Baruah, opposed any negotiations that did not include discussions on Assam's sovereignty. This faction viewed the 1992 surrenders as a betrayal and remained committed to an armed struggle, focusing on continuing their campaign for an independent Assam. They were also responsible for safeguarding the organisation's weaponry, ensuring that resources remained secure (Bhattacharya, 2023).

Differences within ULFA extended beyond peace talks and included disagreements over operational methods. The pro-talks faction, for example, opposed certain violent tactics, particularly killings. There were also differing opinions on collaborating with other insurgent

groups, such as those in Punjab. Additionally, some members expressed concerns about the influence of Pakistan, fearing that it had transformed ULFA from a revolutionary group into a terrorist organisation (Bhattacharya, 2023).

Apart from these factions, ULFA also formed a women's group known as Enigma in 1997. This group was involved in gathering intelligence and conducting operations in the Brahmaputra Valley, although it was not considered a faction in the same way as the pro-talks and anti-talks groups. Despite its structured approach, ULFA faced internal disagreements about the origins of the movement and specific incidents from the 1980s, reflecting a lack of consensus among its leadership (Bhattacharya, 2023).

Operational Strategies of ULFA

ULFA's operational strategies have evolved significantly over the decades, reflecting their adaptability and resilience amidst changing circumstances. In the early 1980s, ULFA's initial operations involved acts of sabotage, such as the pipeline bombings in 1981, which aimed to disrupt infrastructure and draw attention to their cause. During this period, the group sought training and weapons from separatist groups in neighbouring states like Manipur and Nagaland, making multiple trips to Dimapur to establish contact with the National Socialist Council of Nagaland (NSCN). Initially unsuccessful, ULFA eventually connected with the NSCN and received guidance on establishing a constitution and manifesto, with members training at NSCN camps in Myanmar to learn guerrilla warfare and the importance of alliances (Bhattacharya, 2023).

To finance their activities, ULFA relied on robberies, including the looting of tea garden treasuries and coal depots, while also exploring legitimate business ventures and government contracts. The group expanded its recruitment efforts throughout the Brahmaputra Valley,

attracting members from various districts and solidifying their presence in Assamese communities. They adopted a flag and developed a constitution, initially avoiding explicit calls for independence to prevent immediate government retaliation (Bhattacharya, 2023).

In the late 1980s, ULFA openly declared their objective to "liberate" Assam from India through armed rebellion. They sought international support, particularly from Bangladesh and militant groups in Punjab, although these efforts were largely unsuccessful. ULFA secured training from the Kachin Independence Army (KIA) in Kachin, aiming to gain combat experience, establish foreign bases, and procure weapons. They continued financing their operations through bank robberies and contributions from sympathisers within the Assam government, establishing a formal structure with political and armed wings organised along regional and district lines. ULFA created a parallel government in parts of Assam, enforcing their own rules and punishments to undermine Indian authority, including banning alcohol sales and enforcing traditional dress codes (Bhattacharya, 2023).

The group's social initiatives and the perceived failures of the Assam government garnered significant public support in the late 1980s. However, challenges arose in the 1990s as Indian military offensives like Operation Bajrang forced ULFA to abandon camps and adapt strategies. Internal divisions and a lack of long-term planning hindered their ability to effectively counter the army's operations. ULFA shifted focus to establishing bases in neighbouring countries like Bangladesh and Bhutan, relying on extortion to fund operations and engaging in high-profile abductions to generate publicity and bargain for the release of imprisoned members. They also carried out secret killings and attacks on political opponents to silence dissent and maintain control, seeking to exploit international events like the Kargil War to gain support from Pakistan's ISI (Bhattacharya, 2023).

Entering the 2000s, ULFA experienced a decline in public support due to increasingly violent tactics and the emergence of rival militant groups. Security forces pressured their foreign bases, including through Operation All Clear in Bhutan. Despite continuing bombings and targeted attacks in Assam, ULFA struggled to regain its former strength and influence. The organisation underwent multiple structural changes to address internal divisions and adapt to new challenges, but these often led to further confusion and instability within its ranks. ULFA's operational strategies have thus transitioned from early sabotage acts to open rebellion and parallel governance, followed by a decline in popularity and a return to more clandestine and violent tactics, underscored by internal discord and a lack of broad-based support beyond specific Assamese communities (Bhattacharya, 2023).

Funding and External Support

ULFA’s external support network was shaped by a complex web of alliances and strategic interests, particularly as Indian military pressure intensified. Initially, ULFA’s pursuit of external support in the 1980s was pragmatic, driven by the need for arms, training, and safe havens. The group forged ties with the Kachin Independence Army (KIA) in Myanmar, leveraging shared ethnic connections, this was facilitated by shared ethnic ties, with some ULFA cadres emphasising their Mongoloid heritage to gain favour with the Kachin and gaining access to training and arms (Mahanta, 2013). By the 1990s, ULFA received significant support from Pakistan's Inter-Services Intelligence (ISI). Paresh Baruah, one of ULFA’s key leaders, publicly acknowledged receiving training and financial assistance from the ISI. ULFA delegations visited Pakistan, which helped cement ties with Pakistani intelligence. Notably, during the Kargil War, ULFA is alleged to have provided the ISI with intelligence on Indian Army positions. These ties with Pakistan persisted well into the 2000s, reinforcing ULFA’s ability to operate with external support (Bhattacharya, 2023).

As Indian counter-insurgency efforts ramped up in the 1990s, ULFA sought sanctuary in countries like Bhutan and Bangladesh. Bhutan initially provided refuge in its dense jungles, but this proved short-lived when Bhutan launched a military operation in 2003 under Indian pressure, dismantling ULFA's camps. In contrast, Bangladesh became a more stable ally for ULFA, offering safe havens, training camps, and arms supplies, facilitated by the country's Directorate General of Forces Intelligence (DGFI). Bangladesh's involvement was part of a broader strategic calculation, using ULFA as leverage against India, especially as anti-Indian sentiments grew within certain political factions (Mahanta, 2013). However, ULFA's reliance on external actors, particularly Bangladesh, had unintended negative consequences. The group's association with Bangladesh, viewed by many in Assam as a source of illegal immigration, alienated ULFA's local support base.

Moreover, as ULFA became increasingly involved in arms trafficking, their nationalist mission was diluted. The 2004 Chittagong arms case, where a large cache of weapons destined for ULFA was seized, exposed their deep entanglement in illegal arms trade networks. This transformation into a profit-driven enterprise, along with their involvement in attacks alongside Islamist groups, further distanced ULFA from its original goals and eroded public sympathy in Assam (Mahanta, 2013).

ULFA's external support network has been integral to its operations, with various neighbouring countries and international actors playing key roles in sustaining the organisation's insurgency. In the early 1980s, ULFA sought weapons and training from separatist groups in Manipur and Nagaland. They successfully established contact with the National Socialist Council of Nagaland (NSCN), which provided crucial advice on formalising ULFA with a constitution and

manifesto. ULFA members were trained at NSCN camps in Myanmar, where they gained expertise in armed rebellion and sustained insurgency operations. This experience highlighted the importance of establishing foreign bases and alliances with other insurgent groups (Bhattacharya, 2023).

ULFA's relationship with China has largely been characterised by limited direct support, despite repeated efforts to secure assistance. In the 1960s and 1970s, ULFA viewed China as a potential ally, inspired by its support for other regional insurgent groups like the Naga National Council (NNC), Mizo National Front (MNF), and People's Liberation Army (PLA). However, these aspirations did not materialise into significant aid (Bhattacharya, 2023).

One notable example of ULFA's attempts occurred in 1986, when an ULFA delegation tried to enter China via Nepal to seek support, leaving a memorandum for the Chinese Communist Party. However, they were denied entry at the Chinese border, symbolising an early failure in securing direct Chinese involvement. Meanwhile, the PLA of Manipur had a stronger presence in northern Myanmar's Kachin region, where they were supported by the Kachin Independence Army (KIA), possibly with indirect backing from China, further suggesting that China continued to influence insurgent groups in Northeast India through indirect means (Bhattacharya, 2023).

In the 1990s, Paresh Baruah, one of ULFA's key leaders, allegedly made contact with Chinese intelligence while in Kachin, Myanmar. Although his requests for assistance were rejected, he is believed to have cultivated ties in Ruili, a city in Yunnan province known for business and arms dealing, indicating ongoing efforts to build a relationship with China. Additionally, in the 2000s, rumours spread among Manipuri insurgent groups that China might renew support if

they could form a large alliance, though no concrete evidence of this materialised. There were also reports of two Chinese intelligence officers visiting an ULFA camp in Myanmar's Sagaing region during the same period, interacting with insurgent leaders and touring the area, hinting at potential Chinese interest in these groups (Bhattacharya, 2023). By the 2010s, it was speculated that Paresh Baruah had moved to China, possibly to Yunnan provinces. Overall, while ULFA sought Chinese backing and some indirect contacts were made, definitive proof of sustained or direct Chinese support remains elusive. China's role, if any, seems to have been limited to indirect engagement, primarily through its relationships with other insurgent organisations in the region (Bhattacharya, 2023).

Implications to India's Internal Security

ULFA's activities significantly impacted India's internal security, particularly in Assam, by creating an environment of fear, instability, and social disruption. The group employed violent tactics, including bombings, killings, and abductions, targeting a wide range of individuals such as government officials, security forces, political activists, and civilians. Between 1986 and 1990, ULFA was believed to be responsible for at least 113 deaths, including those of Congress party members and government employees. These acts of violence led to a breakdown of law and order, creating widespread insecurity and undermining public safety (Bhattacharya, 2023).

A significant aspect of ULFA's operations was its reliance on extortion to finance its insurgency. Businesses, tea estates, and local traders were frequently coerced into paying large sums under threat of violence. This atmosphere of intimidation discouraged investment and stifled economic growth in Assam, as the business community became wary of further engagement. ULFA also conducted robberies, including looting tea garden treasuries and

attempting bank heists, further destabilising the financial ecosystem of the region (Bhattacharya, 2023).

In addition to its violent tactics, ULFA sought to undermine the Indian government's authority by attempting to establish a parallel government in Assam. The group imposed its own rules, collected taxes, and even tried to control local administration. This effort to supplant the Indian state's authority fueled separatist sentiment and created a formidable challenge to government control over the region (Bhattacharya, 2023).

From a security standpoint, ULFA's use of guerrilla warfare, its network of camps in neighbouring countries, and its ability to draw support from segments of the local population posed significant obstacles to Indian security forces. The group's access to weapons and funding, along with its resilience and ability to evade capture, made it difficult for counter-insurgency operations to effectively neutralise their threat (Bhattacharya, 2023). Moreover, ULFA's widespread activities contributed to an erosion of public trust in the Indian government's capacity to provide security and maintain order. This lack of faith in the government further empowered ULFA, making the insurgency more difficult to contain. Overall, ULFA's operations severely disrupted internal security, challenged the authority of the Indian state, stunted economic development, and heightened social discord. Despite some government successes in countering the insurgency, ULFA's external support and exploitation of internal divisions presented ongoing challenges to restoring peace and stability in Assam (Bhattacharya, 2023).

Policy Recommendations

Drawing lessons from ULFA's activities and the Indian government's response offers critical insights into managing and mitigating future insurgencies. ULFA's rise was fueled by socio-economic disparities, political alienation, and ethnic grievances. To prevent similar movements, it is essential to address the underlying causes that insurgents exploit. Inclusive development initiatives must prioritise infrastructure, education, and healthcare in marginalised regions. Programs aimed at providing vocational training and employment opportunities to the youth can prevent them from becoming susceptible to recruitment by militant groups. Furthermore, fostering inter-community dialogue is vital to defuse ethnic tensions that insurgencies like ULFA have historically used to their advantage.

Strengthening border security is another crucial lesson. ULFA's ability to maintain safe havens and secure logistical support from neighbouring countries such as Bangladesh and Myanmar underscores the need for robust border management. Advanced surveillance technologies, coupled with increased troop deployment along sensitive borders, can help curb cross-border insurgency activities. Diplomatic engagement with neighbouring nations is equally important. Collaborative operations, such as Operation All Clear with Bhutan, have proven effective in dismantling insurgent networks and should be replicated where feasible.

The Indian government's counter-insurgency strategy against ULFA highlights the importance of modernising security forces. Training personnel in guerrilla warfare tactics, improving inter-agency coordination, and utilising technological advancements like drones for surveillance are critical to enhancing operational effectiveness. However, military action alone is insufficient; integrating community policing into counter-insurgency efforts can build trust with local populations and weaken insurgent influence.

Addressing the financial networks of insurgent groups is also key. ULFA financed its operations through extortion, robberies, and external support, making it vital to monitor financial transactions and disrupt funding channels. Collaborating with businesses and creating secure environments can reduce the prevalence of extortion, while intelligence operations can dismantle external funding networks.

The role of external actors, such as Pakistan's ISI and suspected Chinese influence in ULFA's case, highlights the need for vigilance in managing geopolitical factors. Strengthened intelligence-sharing with allies, leveraging international pressure on neighbors, and monitoring regional dynamics can counter external interference. Simultaneously, robust governance and transparency at the local level can strengthen public trust, reducing the space for insurgents to gain support.

Ultimately, the ULFA insurgency underscores the importance of a balanced approach that combines military, political, and socio-economic strategies. Anticipating and addressing grievances early, fostering development, and maintaining vigilance against external manipulation can help India effectively counter future insurgencies and maintain internal stability.

Conclusion

The activities of ULFA have had significant and long-lasting effects on India's internal security, particularly in the northeastern state of Assam. Through a combination of violence, extortion, and attempts to establish a parallel government, ULFA has challenged the authority of the Indian state and created widespread instability. The group's violent tactics, including bombings

and targeted killings, led to a breakdown in law and order, fostering an atmosphere of fear and insecurity. Extortion from businesses and local traders further disrupted the region's economy, discouraging investment and growth. ULFA's reliance on external support, especially from entities like Pakistan's ISI and insurgent groups in neighbouring countries such as Myanmar and Bangladesh, compounded the difficulties faced by Indian security forces. This external backing, along with ULFA's guerrilla tactics and strong local networks, posed formidable challenges to India's counter-insurgency operations. Despite efforts to restore peace, ULFA's capacity to exploit internal divisions and access external resources made the insurgency difficult to contain.

To improve its approach to security in the future, the Indian government must prioritise strengthening border security to prevent the movement of insurgents across international borders. It is also crucial to address the root causes of insurgency, such as socio-economic marginalisation and ethnic tensions, through development initiatives that improve infrastructure, education, and healthcare in insurgency-prone regions. Engaging local communities in peacebuilding efforts and ensuring that security forces respect human rights can help restore public trust in the government's ability to provide safety and governance.

By combining military, economic, and diplomatic strategies, India can better address not only the insurgency in Assam but also other internal security challenges across the country. The lessons learned from ULFA's insurgency underscore the importance of a comprehensive, long-term approach that addresses both the immediate security concerns and the underlying issues that fuel insurgencies.

References

- *Bhattacharyya, R. (2023). ULFA: The Mirage of Dawn. Harper Collins.*
- *Dutta, A. R. (2014). Civil Society's Engagement with ULFA in Assam: A Historical Exploration. Studies in Indian Politics, 2(1), 43–54. https://doi.org/10.1177/2321023014526089*
- *Mahanta, N. G. (2013). Confronting the State: ULFA's Quest for Sovereignty.*
- *Khanikar, S. (2018). State, Violence, and Legitimacy in India. Oxford University Press.*
- *Waterman, A. (2022). The shadow of 'the boys:' rebel governance without territorial control in Assam's ULFA insurgency. Small Wars and Insurgencies, 34(1), 279–304. https://doi.org/10.1080/09592318.2022.2120324*

Adaptations and Evolution in Violent Non-State Actors' Tactical and Strategic Behaviours and Decision-Making

Mohit Gajbhiye

Introduction

VNSAs evolve their tactics to survive and adapt to hostile environments and in the face of security forces pressure. These groups, ranging from terrorist organizations to insurgent militias, leverage various adaptive strategies to sustain their operations and achieve their goals despite facing considerable opposition from state and international security forces. Understanding the mechanisms behind their adaptability is crucial for developing effective counter-terrorism measures.

This research delves into the dynamic processes of VNSA adaptation, exploring the interplay of internal and external factors that drive their evolution. By examining the intricate relationships between VNSAs and their support networks, technological advancements, and counterterrorism pressures, this study aims to shed light on the complexities of VNSA behaviour. Through an interdisciplinary approach, this research seeks to enhance our comprehension of how these actors modify their tactics and strategies, thereby informing more robust and adaptive security responses.

Literature Review

The study of Violent Non-State Actors (VNSAs) has gained prominence in recent years due to their increasing role in shaping global, regional, and domestic security environments. These actors—ranging from terrorist groups to cartels and insurgents—have consistently demonstrated tactical flexibility and strategic evolution in response to counterterrorism measures, technological shifts, and changes in geopolitical dynamics.

Evolution and Typologies of VNSAs

Scholars such as Ludvík (2023) and Vasseur et al. (2022) categorize VNSAs into several typologies—terrorists, insurgents, mafias, cartels, and mercenaries—each with unique drivers and operational structures. This typology is critical to understanding the variation in behavior, adaptability, and impact. For instance, the ideological fervor of groups like ISIS contrasts with the profit-oriented motivations of drug cartels, necessitating tailored analytical frameworks.

Adaptability under Pressure

The RAND Corporation (Johnston et al., 2023; Vasseur et al., 2022) emphasizes how counterterrorism pressure acts as a stimulus for innovation among VNSAs. ISIS, for example, evolved from a territorially fixed organization to a decentralized, digitally enabled insurgency following territorial losses. Similarly, insurgent groups like the Taliban adapted through cross-border sanctuaries and state sponsorship (Khan & Syed, 2021), illustrating a hybrid model of survival and expansion.

Technological Integration and Cyber Capabilities

Recent research (Abro et al., 2022; Al-Rawi, 2018) points to the extensive integration of emerging technologies into VNSA operations. From the use of encrypted messaging platforms (e.g., Telegram, Rocket.Chat) to cyberattacks and drone warfare, VNSAs now possess capabilities that rival some state actors. ISIS's virtual caliphate, as discussed by Bloom and Daymon (2018), shows how propaganda, gamification, and recruitment have moved online.

Recruitment and Propaganda through Digital Platforms

Studies by Dauber et al. (2019), Kang (2014), and Erelle (2015) illustrate how social media and communication apps are instrumental in shaping the psychological and ideological apparatus of

VNSAs. These platforms are leveraged to build virtual communities, spread radical ideologies, and coordinate attacks—often in ways that evade state surveillance.

Case Studies from India

The evolution of local armed civilian groups like Salwa Judum and Village Defence Committees (now VDGs) in India presents a unique domestic perspective. While these groups were state-supported to counter insurgents, their drift toward vigilantism and communal violence (HRW, 2008; Singh, 2022) complicates their role as counter-VNSA tools. Their transformation also reveals how civilian militarization can mimic or mirror VNSA tactics under state sanction.

Knowledge Gaps

While much has been written about the emergence and ideology of VNSAs, fewer studies explore their strategic adaptability across multiple domains (e.g., operational, technological, transnational). This paper addresses this gap by offering a comparative, multi-domain analysis of how VNSAs evolve and what this means for future security paradigms.

Methodology

This research employs a qualitative, case-study based, interdisciplinary approach grounded in conflict studies, counterterrorism policy, and security studies. It integrates theoretical insights with real-world examples to explore how VNSAs evolve under pressure.

1. Research Objectives

- To identify the core drivers behind VNSA adaptation (state sponsorship, technology, support networks).
- To map how these actors change tactics in response to counterterrorism.

- To assess the implications of such adaptations for national and international security.

2. Research Design

- A descriptive and analytical design is adopted, focusing on the strategic behavior and tactical evolution of selected VNSAs over time. The analysis is framed through:
- Case studies
- Technology impact mapping
- Organizational behavior analysis

3. Data Collection

- Primary Sources:
- Open-source intelligence (OSINT)
- Government documents (e.g., Indian Supreme Court rulings, security reports)
- Transcripts and speeches by terror leaders or security analysts
- Secondary Sources:
- Peer-reviewed journals (e.g., Terrorism and Political Violence, Asian Survey)
- Books and white papers (RAND, Human Rights Watch, UN reports)
- Reputable news media (e.g., New Yorker, CNN, The Print)

4. Case Studies Used

- Global: ISIS and its post-caliphate transformation.
- Domestic (India):
- Salwa Judum as a state-aligned VNSA
- Village Defence Guards (VDGs) and their evolving role
- Comparative: Taliban’s operational endurance via external sanctuaries.

5. Analytical Tools

- Thematic Content Analysis: Identifying recurring themes in adaptation (e.g., tech use, ideological shifts).
- SWOT-style Mapping: Used for evaluating each VNSA's strength, vulnerability, and opportunity.
- Platform-based Analysis: Evaluating specific digital platforms (e.g., Telegram, Discord) for their utility in radicalization.

6. Limitations

- Lack of classified counterintelligence data restricts direct operational insights.
- Rapidly evolving technology outpaces literature, making some findings time-sensitive.
- Ethical and legal barriers prevent direct fieldwork on VNSA recruitment or propaganda methods.

Division of VNSAs

Violent Non-State Actors (VNSAs) are diverse groups that operate outside the control of any state, often using violence to achieve their goals. Understanding the different types of VNSAs is essential for developing effective strategies to counter their threats. Here, we discuss various types of VNSAs, including terrorists, mafias, insurgents, cartels, and mercenaries, along with specific examples.

Terrorists

Terrorist groups aim to achieve political, religious, or ideological objectives through the use of violence and terror. They often target civilians to spread fear and coerce governments into meeting their demands. Examples include:

- *Al-Qaeda*: Founded by Osama bin Laden, Al-Qaeda orchestrated the September 11 attacks and has been involved in numerous terrorist activities worldwide.
- *ISIS (Islamic State of Iraq and Syria)*: Initially an offshoot of Al-Qaeda, ISIS declared a caliphate in 2014 and captured large territories in Iraq and Syria before being significantly weakened by international military efforts.

Insurgents

Insurgents are armed groups that aim to overthrow a government or secede from a country. They often engage in guerrilla warfare, leveraging local support and difficult terrain to challenge state forces.

- *FARC (Revolutionary Armed Forces of Colombia)*: A Marxist-Leninist guerrilla group that fought the Colombian government for over 50 years before signing a peace deal in 2016.
- *Taliban*: A fundamentalist militant group that controlled Afghanistan from 1996 to 2001 and has continued to wage an insurgency against the Afghan government and its allies.

Mafias

Mafias are organized crime syndicates involved in various illegal activities such as drug trafficking, extortion, and money laundering. They typically operate in a clandestine manner and maintain influence through violence and corruption. Examples include:

- *Yakuza*: Japanese organized crime groups involved in a range of illicit activities including drug trafficking, gambling, and human trafficking.
- *Cosa Nostra (Sicilian Mafia)*: Known for its hierarchical structure and involvement in various criminal enterprises, including drug trafficking and protection rackets.

Cartels

Cartels are large, highly organized groups primarily involved in drug trafficking. They control large territories and engage in violent confrontations with rivals and state forces to maintain their dominance.

- *Sinaloa Cartel*: One of the most powerful drug trafficking organizations in Mexico, involved in smuggling large quantities of narcotics into the United States.
- *Medellín Cartel*: A notorious Colombian drug cartel led by Pablo Escobar, which was responsible for the majority of cocaine smuggled into the United States during the 1980s.

Mercenaries

Mercenaries are individuals or groups hired to fight in conflicts for financial gain rather than ideological or political reasons. They often operate in conflict zones where state control is weak.

- *Wagner Group*: A Russian private military company involved in conflicts in Ukraine, Syria, and several African countries.
- *Executive Outcomes*: A South African private military company that operated in Angola and Sierra Leone during the 1990s.

Adapting to Evolving VNSA Threats

This article explores the drivers, impacts, and implications of VNSA adaptation in critical areas. Key drivers include counterterrorism pressures, technological advancements, internal dynamics, and external support networks. We examine the impact on security landscapes, showcasing the adaptive capabilities of VNSAs through the case studies of ISIS, Salwa Judum,

and Ranveer Sena. Finally, we propose strategies to counter these evolving threats, emphasizing robust intelligence gathering, scenario planning, and adaptable security measures. Understanding VNSA behaviour helps security agencies enhance their agility and resilience in counterterrorism efforts.

VNSA Adaptation Drivers

Violent Non-State Actors (VNSAs) have shown remarkable adaptability in response to the dynamic challenges posed by counter-terrorism efforts. Several key factors drive this adaptability, which can be grouped under the following subheadings:

1. External Support Networks

External support networks are critical in shaping the behavior and capacity of VNSAs. These networks can include:

- State Patrons: Countries that provide financial, military, or logistical support to VNSAs. For example, Iran’s support for Hezbollah in Lebanon and Syria, or Pakistan's backing of insurgent groups in Afghanistan, including the Taliban.
- Global Players: Various international actors who may indirectly support VNSAs by providing them with weapons, funds, or propaganda platforms.
- Products and Services: The provision of advanced weaponry, financial resources, and training to VNSAs. This support enables these groups to sustain their operations, develop new capabilities, and evade counter-terrorism efforts.

2. State Sponsorship

State sponsorship is one of the most significant factors influencing VNSA activities. This sponsorship is driven by:

- Political and Strategic Gains: States often support VNSAs to project power, influence regional dynamics, or counter perceived threats. For instance, Iran's support of Hezbollah serves to counterbalance Israel and Sunni Arab states.
- Provision of Resources: States provide VNSAs with essential resources such as finances, arms, and training. They may also offer physical safe havens from which VNSAs can launch operations or retreat during crackdowns.
- Impact on Counter-Terrorism: The support provided by states often hampers counter-terrorism efforts. For example, the resilience and reorganization of the Taliban are bolstered by their ability to operate from safe havens in Pakistan.

3. Transnational Networks

Transnational networks are another key adaptation driver for VNSAs. These networks include:

- Criminal and Sympathizer Networks: VNSAs often collaborate with criminal organizations, foreign fighters, and sympathizers to enhance their capabilities. These collaborations help in resource sharing, recruitment, and the exchange of tactical knowledge.
- Global Recruitment: Transnational networks enable VNSAs to recruit fighters and supporters from across the globe, increasing their manpower and reach.
- Complementary Capabilities: Network ties often influence VNSA behavior and goals, aligning them with the objectives of their sponsors or collaborators. For instance, Hezbollah’s strategic restraint in attacking Israel during low-intensity conflicts may be influenced by a desire to avoid jeopardizing its support from Iran.

4. Technological Advancements

Technological advancements play a crucial role in the adaptation of VNSAs by:

- Improving Communication: Enhanced communication technologies allow VNSAs to coordinate across vast distances, maintain operational security, and disseminate propaganda.
- Weaponization: The acquisition of advanced weapons, such as drones and improvised explosive devices (IEDs), has significantly increased the lethality and operational reach of VNSAs.
- Cyber Capabilities: Some VNSAs have developed cyber capabilities to conduct cyber-attacks, recruit online, and spread their ideology through social media platforms.

5. Limitations of External Support

While external support networks provide significant advantages, they also come with inherent weaknesses:

- Lack of Autonomy: VNSAs that rely heavily on external support may sacrifice their autonomy, becoming dependent on their sponsors for resources and legitimacy.
- Potential Alienation: Over-reliance on state sponsors or transnational networks can alienate potential supporters and deepen regional enmities, potentially limiting the VNSA's appeal and operational freedom.

External support networks, including state sponsorship and transnational ties, are key factors that shape how VNSAs operate and adapt. These networks offer critical resources, safe havens, and ideological backing, which strongly influence the goals and actions of these groups. However, reliance on these networks can also restrict VNSAs' independence and risk alienating potential supporters. To effectively counter these groups, it’s crucial to understand and address the support structures that sustain them.

Impact on Security Landscapes

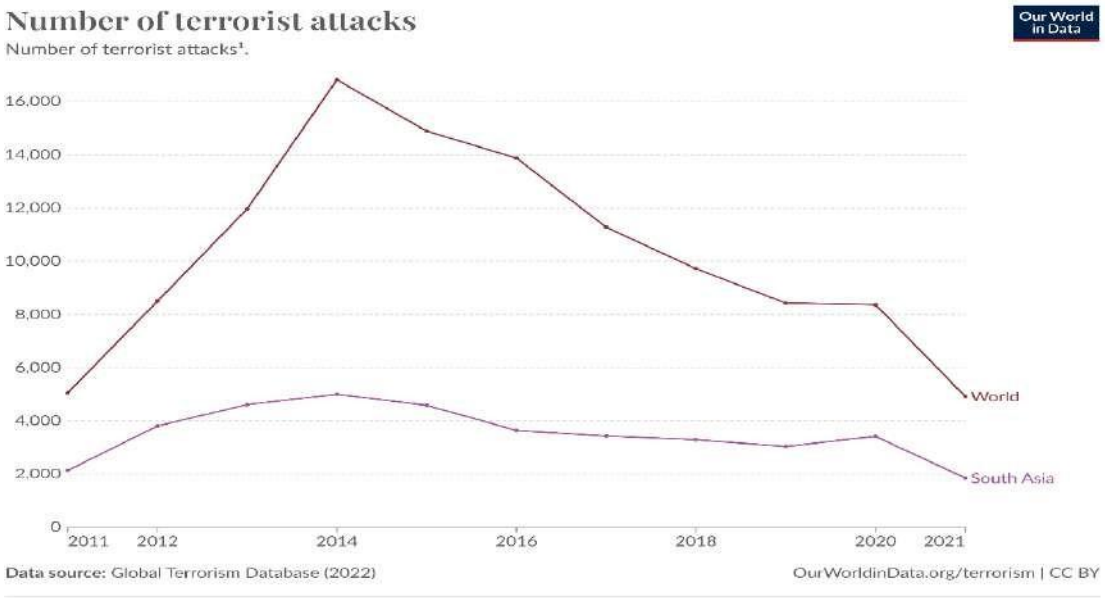
This has been a great challenge to security agencies through VNSA adaptation thus causing a reduced public trust and overstretching on available resources. each of these actors expands its methods, approaches and formations; thus, security agencies are constantly struggling to match the pace and encounter numerous challenges in thwarting threats. This not only erodes the public confidence in the capacity of the security forces to deliver safety and security but also puts huge stress on resources committed to counter-terrorism measures.

One of the prime strategically enlightening examples of the adaptive deployment of VNSA and its consequential implications for security environments is the case of the Islamic State of Iraq and Syria (ISIS). ISIS, otherwise known as Daesh, turned into one of the most dangerous terrorist organizations in the contemporary history of terrorism that proved its ability to evolve in response to the change in security technologies and countermeasures at the international level (Albadry, 2022).

Violent Non-State Actors (VNSAs) like ISIS have dramatically impacted global security landscapes through their adaptability and evolving tactics. The rise of ISIS in the wake of the Syrian civil war and the withdrawal of U.S. troops from Iraq serves as a prime example. Initially seizing large territories, ISIS used social media and online platforms to recruit globally and spread its ideology. When faced with military defeats, ISIS shifted from conventional warfare to guerrilla tactics, carrying out suicide bombings, riots, and mass attacks aimed at sowing fear and instability.

Even as ISIS lost significant ground, its decentralized leadership and global network allowed it to maintain influence and continue its operations. Security agencies, while attempting to counter these threats, found their resources strained, struggling to keep pace with ISIS's adaptability. This has led to more cooperative international counterterrorism measures,

including intelligence-sharing and joint operations. Despite ongoing efforts, ISIS remains a global threat, underscoring the challenge VNSAs pose in today's security environment. However, over the past decade, there appears to be a decline in terrorist events, as indicated by the graphical trends derived from data provided by the Global Terrorism Database and the World Bank from the year 2011 to 2021.



The adaptive nature of groups like ISIS, coupled with their effective use of modern technology and propaganda, continues to be a pressing issue for security agencies worldwide.

In India there exist some VNSAs in the past that had impacted and challenged Indian Security systems.

Salwa Judum

Salwa Judum, launched in 2005 in Chhattisgarh, India, aimed to counter the Naxalite-Maoist insurgency, which sought to overthrow the Indian government through armed struggle. This state-backed militia, composed of local tribal villagers, was armed and trained to defend their communities and gather intelligence. However, Salwa Judum's actions includes forced

displacement, violence against civilians, and extrajudicial killings. Entire villages, suspected of aiding the Maoists, were targeted, displacing thousands into overcrowded camps under dire conditions. These actions deepened distrust in the government, escalated violence, and overstretched security forces. In 2011, the Supreme Court deemed Salwa Judum unconstitutional, citing its violation of citizens' rights and the counterproductive nature of arming civilians.

Village Defence Guards

The Village Defence Committees (VDCs), now restructured as Village Defence Guards (VDGs) under the 2022 Village Defence Guard Scheme, represent a unique dynamic in Jammu and Kashmir's counterinsurgency efforts. Established to bolster local defense capabilities against insurgent threats, these groups have historically served as a force multiplier for the state in remote areas where security forces have limited reach. However, their actions have occasionally led to controversies, particularly when their activities veered into vigilantism or instances of communal violence. Concerns about misuse of state-provided arms and the lack of robust oversight have raised questions about the balance between their intended defensive role and their potential for creating localized unrest.

The restructuring into VDGs aimed to address these issues by formalizing their operations, enhancing accountability, and ensuring their activities align with state objectives. Yet, the empowerment of these groups has also sparked apprehensions about exacerbating communal tensions in an already fragile region. Instances of weapon misuse and allegations of targeting specific communities underline the importance of strict oversight. While the VDGs have been instrumental in countering insurgent activities, their long-term impact on the region's sociopolitical fabric depends on careful management to prevent them from becoming sources of instability rather than security.

Emerging Technologies Implications for VNSAs and Terrorists

1. Enhancing Radicalization and Recruitment

Emerging technologies are transforming the way terrorists and violent non-state actors (VNSAs) reach new audiences, radicalize followers, and recruit operatives. With the proliferation of online platforms, extremist groups can spread their messages globally, forming virtual communities and recruiting supporters in previously unreachable regions. Advanced tools such as video manipulation and AI-assisted deepfake technology enable these groups to produce and distribute convincing propaganda. By creating fake videos or using altered images, terrorists can fuel misinformation, provoke violence, and sustain ideological movements.

For instance, militant groups in India's Jammu and Kashmir have employed fake videos and images to incite violence and coordinate activities. With the blending of augmented and virtual reality (AR/VR), terrorist leaders could even use avatars of well-known figures to spread extremist messages and mobilize followers. These technologies make it easier for radicalizers to influence vulnerable populations and enhance the reach of their violent narratives.

2. Augmenting Planning, Training, and Plotting

Technological advancements have also revolutionized how terrorists plan and train for attacks. Using AR/VR environments, terrorist groups can create virtual simulations of potential targets, allowing operatives to practice attack scenarios in safe, controlled settings. This enables them to plan complex operations, rehearse routes, establish contingency plans, and ensure coordinated actions without revealing their actual intentions. For example, with adequate reconnaissance, terrorists can simulate attacks on key locations and prepare for various outcomes. They can also use anonymity tools to protect their identities while operating in these

virtual environments. Moreover, augmented reality could enable terrorists to create virtual training camps where experienced operatives mentor recruits from different parts of the world, thus maintaining global networks even when separated by physical distance. The impact of these technologies on desensitizing violence is further magnified by the use of increasingly realistic first-person shooter games, which can condition attackers to carry out real-life acts of violence with more ease and precision.

3. New Attack Methods Using Emerging Technologies

Emerging technologies are providing terrorists with advanced tools for precise and efficient attacks. AI and machine learning enable better target identification, faster decision-making, and enhanced drone operations, including swarms that can evade defenses and autonomously target individuals or groups. Autonomous vehicles add to these threats, as they can be weaponized for ramming attacks while masking the attacker's identity. The growing reliance on the Internet of Things (IoT) also introduces critical vulnerabilities. Terrorists can leverage AI-driven cyberattacks to exploit infrastructure, such as power grids or water facilities. For example, malware flagged by the Cybersecurity and Infrastructure Security Agency (CISA) highlights the risk of sabotaging utilities, emphasizing how terrorists are increasingly able to exploit both physical and digital systems for large-scale disruption.

EMERGING TECHNOLOGY REFERENCE GUIDE			
	Radicalization	**Plotting**	**Attacks**
Artificial Intelligence	AI coupled with machine learning could enable extremists to refine their targeting of people susceptible to radicalization and recruitment.	Focused pattern recognition could facilitate target identification and pre-attack surveillance.	AI could process sensory inputs from various sources to inform attack methods. Facial recognition and pattern-of-life analysis could allow for more targeted attacks.
Autonomous Vehicles	Terrorists might increase their pool of potential attackers by encouraging supporters to conduct attacks using autonomous vehicles—such as UAS or self-driving cars—potentially removing a barrier to entry for extremists hesitant to conduct in-person attacks.	Plotters could use autonomous vehicles to gather data about potential targets and escape routes. Use of live-feed video surveillance might enable terrorists to better anticipate and plan for attack contingencies.	Attackers could use autonomous vehicles to conduct vehicle-ramming attacks and deliver improvised explosive devices to targets.

Cyber	Advancements in terrorist cyber use could enable more targeted radicalization efforts. Proliferation of increasingly secure encrypted messaging systems and cryptocurrency could aid in terrorist recruitment and fundraising.	More widespread access to advanced cyber capabilities on personal mobile devices could help terrorists with surveillance and reconnaissance as well as with attack planning and logistics. Terrorists may increasingly use encryption technology to conceal their online activities, including in regions where cyber capabilities are historically less available.	Internet–connected critical infrastructure and medical devices could be more vulnerable to attack. Cyber-attacks to infiltrate or disrupt software or hardware used by first responders could disrupt response efforts.
Internet of Things	Internet-connected devices, such as wearable fitness trackers, vehicle systems, and smart home appliances, might be vulnerable to	Terrorists might hack into devices connected to the Internet of Things to gain more information about potential targets.	Virtual attacks could cripple vital services or be used to disrupt responses to terrorist attacks by targeting first responders' software and

	exploitation. If compromised, such data could highlight user vulnerabilities that terrorists could employ to refine recruitment efforts.		communications. Smart devices used by first responders, if disabled, could complicate response efforts.
Deepfakes	Terrorists could use deepfake videos to manufacture content for radicalization and recruitment efforts. Extremists could share doctored video content to try to discredit counter messaging or propagate violent extremist narratives.	Terrorists could use deepfakes to gain unauthorized access to physical or virtual environments or to spread disinformation before an attack.	Terrorist could use deepfake technology to produce and disseminate content during or after an attack to try to disrupt responses or discredit public information networks.
Social media	More widespread access to encrypted social media apps could continue to facilitate terrorists' radicalization	Social media could be used by terrorists to call supporters to action, share operational instructions, or conduct	Terrorists could conduct cyber-attacks targeting social media platforms to remove or tamper with accounts

	and recruitment efforts that are difficult to detect.	misinformation campaigns.	or spread false information.
Augmented and Virtual Reality (AR/VR)	Terrorists could use AR/VR to provide environments for rapport-building during radicalization and recruitment. Virtual parlors may provide more intimate platforms for discussing terrorism than traditional online messaging platforms.	AR/VR environments could enable realistic training and mission rehearsals. Terrorists could use virtual landscapes to practice attacks and plan for contingencies. Terrorists could use AR/VR platforms for weapons and equipment training, enabling them to conduct attack preparations anywhere with access to these platforms.	Terrorists could use AR/VR technology in concert with autonomous vehicles for operational surveillance or attacks. Self-driving cars or drones could be used to enable attacks or enhance remote operations.

The Use of social media and Digital Platforms by VNSAs

Violent non-state actors (VNSAs), especially ISIS, have demonstrated remarkable adaptability in exploiting digital platforms for recruitment, propaganda, and planning. Their platform-

specific strategies leverage the tools and features of each medium to maximize outreach while evading scrutiny. Scholars like Dauber et al. (2019) and Bloom and Daymon, C. (2018) have highlighted the evolution of these methods, reflecting ISIS's role as a model for other groups.

Telegram

Telegram remains a cornerstone of ISIS's digital operations, primarily due to its encryption and wide reach. ISIS-linked entities like Amaq News Agency and Nashir News Agency rely on Telegram channels to share attack instructions, propaganda, and operational updates. Telegram's features allow seamless dissemination of content while providing some degree of anonymity, making it a resilient platform despite increased monitoring.

Rocket Chat

Rocket Chat emerged in 2018 as a significant tool for ISIS after territory losses in Iraq and Syria. As Dauber et al. (2019) observed, the group's ability to adapt technologies is notable. ISIS-linked groups like Halummu and Shumukh al-Islam leveraged RocketChat's self-hosting option, reducing their vulnerability to takedowns. Nashir News even guided members on installing and using the platform anonymously. With over 700 users in key channels by January 2019, Rocket Chat serves as a vital hub for communication and propaganda.

Discord

Discord, originally a gaming platform, has been co-opted by ISIS supporters for radicalization and recruitment. Pro-ISIS servers host content in multiple languages, including English, Russian, and Japanese, and share threats targeting cities like New York and Paris. As Bloom, M. and Daymon, C. (2018) emphasize, ISIS has skillfully adapted its branding, using platform-native features such as memes and emojis to attract younger audiences.

WhatsApp, Skype, and Kik

These private messaging apps are instrumental in enabling direct communication between recruiters and potential recruits. The memoir of Erelle, A. (2015) provides a vivid example of how ISIS recruiters, such as Bilel, used Skype for secure conversations and psychological manipulation. WhatsApp and Kik are similarly utilized for logistical planning and one-on-one radicalization.

Facebook, Instagram, and Twitter

Despite efforts by these platforms to curb extremist content, ISIS exploits their widespread user base to disseminate memes, videos, and targeted propaganda. Kang, J.C. (2014) highlighted ISIS's use of "Call of Duty"-themed memes promoting martyrdom, while Segall, L. (2014) documented their audacious Twitter campaigns encouraging individuals to join Jihad.

YouTube and Twitch

ISIS capitalizes on the visual appeal of video content, releasing high-quality productions like *Mujatweets*, which showcase a curated image of ISIS fighters engaging with communities. These efforts reflect what Kang, J.C. (2014) termed as "brotherhood propaganda." Twitch and Facebook Live have further enabled real-time dissemination of extremist messages and attacks, as noted by RAN (2020).

Viber and Yahoo Together

Although their presence on Viber and Yahoo Together was short-lived, ISIS briefly utilized these platforms for propaganda. The Nashir News Agency established accounts on Viber, signaling an experimental approach to new communication avenues. Similarly, Yahoo Together hosted ISIS-linked content before swift takedowns curtailed its use.

Gaming Platforms

Gaming platforms and MMOs (Massive Multiplayer Online games) have become unconventional yet effective spaces for recruitment. As Dauber et al. (2019) observed, ISIS's use of gaming metaphors, such as the *Call of Duty* meme “THIS IS OUR CALL OF DUTY AND WE RESPAWN IN JANNAH [Paradise],” underscores their ability to resonate with younger, tech-savvy audiences. Recruiters use gaming chats to identify targets and initiate private conversations.

ISIS and other VNSAs have transformed the digital landscape into a battleground for their ideological campaigns. Their innovative use of platforms like Telegram, Rocket Chat, and Discord highlights a strategic approach to evading detection and maintaining influence. As Al-Rawi, A. (2018) and Segall, L. (2014) point out, the response from tech companies is critical in disrupting these operations. Effective countermeasures require a combination of technological innovation, policy enforcement, and international cooperation to combat the persistent digital threat posed by these groups.

Countering Evolving Threats by VNSAs

Violent non-state actors (VNSAs) like ISIS pose significant and ever-changing security threats, necessitating multifaceted and dynamic approaches by security agencies. These strategies must combine robust intelligence gathering, scenario planning, adaptable security measures, and a future-oriented focus on leadership, emerging technologies, and international cooperation.

Effective Strategies for Countering Evolving Threats

1. Robust Intelligence Gathering

Efficient intelligence gathering forms the backbone of counterterrorism efforts. As highlighted by Dorak, O.J. (2021), timely and accurate intelligence about VNSAs' intentions, capabilities, and activities is indispensable.

- Human Intelligence (HUMINT): Utilizing personnel to gather intelligence.
- Signals Intelligence (SIGINT): Interception of communications using electronic means.
- Imagery Intelligence (IMINT): Analysis of images to derive actionable intelligence.
- Open-Source Intelligence (OSINT): Monitoring social media and online platforms.

Advanced methodologies such as data mining, pattern matching, and network analysis help uncover and dismantle plots before their execution. Intelligence-sharing networks among nations are crucial to countering globally active VNSAs like ISIS.

2. Scenario Planning

Scenario planning, as described by Norouzi, N., Fani, M. and Ziarani, Z.K. (2020), involves identifying potential threats and crafting strategies to counter them. This approach includes simulating attacks and operational models to evaluate readiness, improve communication channels, and develop backup strategies. By allocating resources to high-risk areas and using risk-reward assessments, security agencies can enhance their preparedness for evolving threats.

3. Adaptable Security Measures

Adaptability is key to combating VNSAs, whose tactics evolve constantly (Hummel, K., 2021). Proactive measures include:

- Employing layered security techniques, such as physical barriers, access controls, and surveillance systems.

- Using advanced tools like biometric scanners, UAVs, and explosive detection systems for real-time threat identification.
- Enhancing training for security personnel in crisis management, counterterrorism, and inter-agency coordination (Utete, R., 2021).

Way Forward

1. Leadership Dynamics and Organizational Behaviour

Researching leadership roles within VNSAs, as suggested by Karakuş and Ak (2022), can illuminate how leaders influence ideology, recruitment, and operations. Understanding leadership vulnerabilities can aid in destabilizing these groups by targeting hierarchical structures and undermining cohesion.

2. Emerging Technologies

Modern technologies like artificial intelligence, machine learning, and autonomous systems hold immense potential for tracking, identifying, and disrupting VNSA operations. However, research should also address ethical, legal, and societal concerns associated with counterterrorism technologies. Studying how VNSAs exploit social media can aid in designing anti-extremism policies.

3. International Cooperation

Addressing global threats requires collaboration among nations, regional organizations, and NGOs. Future research should focus on the efficacy of frameworks like the United Nations Global Counter-Terrorism Strategy and the dynamics of geopolitical relations in fostering or hindering international cooperation. Enhanced information exchange, joint training programs, and coordinated actions are essential to combating transnational VNSA threats.

Countering evolving threats from VNSAs requires a comprehensive approach combining intelligence, adaptability, and collaboration. Security agencies must prioritize timely intelligence, scenario planning, technological advancements, and international cooperation. Future research into leadership, emerging technologies, and global partnerships is vital to enhance security and maintain global peace.

Conclusion

In conclusion, Violent Non-State Actors (VNSAs) demonstrate significant adaptability in response to counterterrorism pressures and environmental challenges. Factors such as external support networks, state sponsorship, transnational collaborations, and technological advancements enable these groups to sustain operations and evolve strategies. This adaptability, evident in their use of digital platforms, weaponized technologies, and decentralized leadership, underscores the complexity of addressing VNSA threats. Trends from the Global Terrorism Database and World Bank suggest a decline in terrorist events over the last decade, reflecting progress yet demanding continued vigilance and innovation in countermeasures.

Addressing VNSAs effectively requires a multidimensional approach integrating timely intelligence, technological advancements, and international cooperation. Future efforts should prioritize understanding VNSA decision-making, leadership dynamics, and exploitation of emerging technologies to develop pre-emptive and adaptive strategies. Strengthened global collaboration and robust security frameworks are essential to counter the persistent threats posed by VNSAs while ensuring sustained global peace and stability.

References

- *Albarry, H. (2022). The protection of civilians in Northwest Syria: How is the responsibility to protect reflected in the knowledge, attitudes, and behaviours of non-state armed groups? (Master's thesis, Hasan Kalyoncu Üniversitesi).*
- *Johnston, T., Mueller, E. E., Chindea, I. A., Byrne, H. J., Vest, N., Clarke, C. P., Garg, A., & Shatz, H. J. (2023). Countering violent nonstate actor financing: Revenue sources, financing strategies, and tools of disruption. RAND Arroyo Center.*
- *Khan, I., & Syed, K. H. (2021). Afghanistan under the shadows of Taliban and implications for Pakistan and regional security. Pakistan Social Sciences Review, 5(4).*
- *Schulze, K. E., Jones, S. G., & de Bretton-Gordon, H. (n.d.). The Taliban and the struggle for Afghanistan.*
- *Ludvík, Z. (2023). Violent non-state actors: The politics of territorial governance. Rowman & Littlefield.*
- *Vasseur, M., Serena, C. C., Clarke, C. P., Chindea, I. A., Mueller, E. E., & Vest, N. (2022). Understanding and reducing the ability of violent nonstate actors to adapt to change. RAND.*
- *Shamshad, M., & Arshad, F. (2021). Iran's strategic approach towards the Israel- Hezbollah conflict. Perennial Journal of History, 2(2), 237–253.*
- *Albadry, A. S. (2022). Terrorism and its impact on the right of human in development: A study case of ISIS (Daesh) in Iraq. Political Sciences Journal, (63).*
- *Congress.gov. (2024). ISIS post-caliphate: Threat implications for America and the West. Retrieved from https://www.congress.gov/event/115th-congress/houseevent/108344/text*

- *Kibusia, J. K. (2020). Contribution of the multiagency approach to security in the fight against terrorism in Kenya: A case of disciplined forces (Doctoral dissertation, Africa Nazarene University).*
- *Dorak, O. J. (2021). Tactical intelligence: Disrupting the terrorist attack cycle by analysing terrorists' intelligence operations.*
- *Norouzi, N., Fani, M., & Ziarani, Z. K. (2020). The fall of oil age: A scenario planning approach over the last peak oil of human history by 2040. Journal of Petroleum Science and Engineering, 188, 106827.*
- *Hummel, K. (2021). Commentary: Placing terrorism in a violent non-state actor framework for the Great Power Competition era. Combating Terrorism Center at West Point. Retrieved from https://ctc.westpoint.edu*
- *Abro, G. E. M., Zulkifli, S. A. B., Masood, R. J., Asirvadam, V. S., & Laouiti, A. (2022). Comprehensive review of UAV detection, security, and communication advancements to prevent threats. Drones, 6(10), 284.*
- *Utete, R. (2021). Capacity building as a strategic tool for employment equity implementation in the financial sector. SA Journal of Human Resource Management, 19, 10.*
- *Karakuş, M., & Ak, Ö. (2022). Pornification of the cyberspace during intrastate conflicts: VNSAs, recruitment strategies, and the changing role of women in the turbulence of violence. In Fighting for Empowerment in an Age of Violence (pp. 189–210). IGI Global.*
- *Supreme Court of India. (2011). Judgment on Salwa Judum. Retrieved from https://www.supremecourtofindia.nic.in*

- *Human Rights Watch. (2008). Being neutral is our biggest crime: Government, vigilante, and Naxalite abuses in India's Chhattisgarh state. Retrieved from https://www.hrw.org*
- *Chand, S. (2009). The Naxalite movement in India: Origin and impact. Asian Survey, 49(3), 465–488.*
- *Kang, J. C. (2014, September 18). ISIS's call of duty. The New Yorker. Retrieved from https://www.newyorker.com/tech/annals-of-technology/isis-video-game*
- *National Counterterrorism Center. (n.d.). Emerging technologies may heighten terrorist threats: First responders toolbox. Retrieved from https://www.odni.gov*
- *Miller, C. J. (2021). Violent non-state actors and the evolving threat of terrorism (Master's thesis). Portland State University. Retrieved from https://pdxscholar.library.pdx.edu*
- *Newman, L. H. (2022, February 24). Terrorist groups prey on unsuspecting chat apps. Wired. Retrieved from https://www.wired.com/story/terrorist-groups-prey-on-unsuspecting-chat-apps/*
- *Erelle, A. (2015). In the skin of a jihadist: A young journalist enters the ISIS recruitment network. Harper Collins.*
- *Dauber, C. E., Robinson, M. D., Baslious, J. J., & Blair, A. G. (2019, June). Call of duty: Jihad--How the video game motif has migrated downstream from Islamic State propagandistic videos. Perspectives on Terrorism, 13(3), 17–31.*
- *Bloom, M., & Daymon, C. (2018, April). Assessing the future threat: ISIS's virtual caliphate. Foreign Policy Research Institute, 372–388.*
- *Segall, L. (2014, September 30). ISIS recruiting tactics: Apple pie and video games. CNN Business. Retrieved from https://money.cnn.com/2014/09/30/technology/isis-recruiting/*

- *Al-Rawi, A. (2018). Video games, terrorism, and ISIS's Jihad 3.0. Terrorism and Political Violence, 30(4), 740–760.*
- *Human Rights Watch. (2008). "Being Neutral Is Our Biggest Crime": Government, Vigilante, and Naxalite Abuses in India's Chhattisgarh State. Human Rights Watch. Retrieved from https://www.hrw.org/report/2008/07/14/being-neutral-our-biggest-crime/government-vigilante-and-naxalite-abuses-indias*
- *Singh, R. (2022). VDCs to VDGs: The transformation of civilian defence groups in Jammu and Kashmir. The Print. Retrieved from https://theprint.in*
- *Dawn. (2023). Misuse of armed civilian groups in conflict zones: Lessons from the Village Defence Committees. Dawn. Retrieved from https://www.dawn.com*

Evaluating the Role and Risks of Lethal Autonomous Weapons Systems in Modern Warfare: Ethical, Technical, and Strategic Perspectives

Rajas Ashish Purandare

Introduction

In modern times, we have seen a shift from conventional warfare to non-conventional technological warfare. We have moved from soldiers fighting on the ground to drones and robots replacing “the boots on the ground,” thereby limiting human intervention and increasing the use of modern technology. There is no denying that modern forms of high-intensity conflict are akin to traditional state-to-state combat. But it is not a pinpointed throwback to 20th-century 'trench and tank warfare.'

Disruptive technologies play an important role in defining modern military strategy and battlefield tactics and in distinguishing modern high-intensity conflict from its predecessors. The government is now dealing with near-peer foes who must have a full spectrum of capabilities, and that requires a new battle domain, like information, cyber, and space. Autonomy of various devices has experienced rapid development as well as different opportunities for incorporation. Weapons systems designed to be autonomous include many devices in manufacturing equipment, robotics, and computer science.

Some of these uses of AI Technologies are called LAWS (Lethal Autonomous Weapons Systems) and include subfields of AI like Machine Learning (ML) and computer algorithms that autonomously identify and engage a specific target without human intervention. LAWS need to be AI dependent (i.e. the weapons can be fully AI operated only or somewhere AI can support human operators).

Literature Review

The paper "India and the Challenge of Autonomous Weapons" (2016) by R. Shashank Reddy provides a comprehensive analysis of the implications of autonomous weapons and India's stance on this emerging technology. The literature review of this paper encompasses various key themes and discussions related to autonomous weapons, global perspectives, legal debates, and policy recommendations.

Reddy discusses the technological advancements that have led to the development of autonomous weapons systems. He highlights these systems' capabilities, including their ability to operate without direct human control. The author also delves into the current weapon systems that incorporate autonomous features and the potential risks associated with their use. One of the central aspects of the paper is the legal debate surrounding autonomous weapons. Reddy explores the ethical and legal implications of deploying such systems in armed conflicts. He raises questions about accountability, responsibility, and adherence to international humanitarian law in the context of autonomous weapons.

The article "Killer drones: The ‘silver bullet’ of democratic warfare?" (2016) by Frank Sauer and Niklas Schörnig explores the relationship between democracy and the military use of unmanned systems, specifically focusing on drones. The authors critically examine the reasons why democracies are leading the development of military unmanned systems and the potential consequences of this trend. They approach the topic through the lens of democratic peace theory, highlighting the distinctiveness of democracies in their behaviour towards conflict. The authors delve into the concept of democratic distinctiveness, which emerged from the democratic peace debate, to question the assumptions of democratic peacefulness.

They argue that democracies exhibit both peaceful and belligerent behaviours, challenging the traditional view of democracies as inherently peaceful.

The article discusses how democratic interests and norms, such as cost reduction, casualty avoidance, and adherence to legal norms, contribute to the appeal of unmanned systems for democracies. Bedavyasa Mohanty in his paper titled "Command and Ctrl: India’s Place in the Lethal Autonomous Weapons Regime" (2016) delves into the ongoing international discourse surrounding Lethal Autonomous Weapons Systems (LAWS), examining their compatibility with international humanitarian law.

Mohanty's analysis is twofold, aiming to identify areas of concern for India's foreign policy and national security while also emphasizing the need for careful consideration during the integration of LAWS research and development into the country's institutional framework.

The paper underscores the inevitability of LAWS development but argues that policymaking can effectively regulate their deployment. Mohanty suggests that nations, including India, should actively participate in shaping the norms governing LAWS use while simultaneously pursuing domestic production capabilities. This dual approach facilitates strategic engagement in the international discourse and enhances India's autonomy in defence technology. Overall, Mohanty's literature review provides valuable insights into the complex intersection of technology, policy, and ethics in autonomous weapons systems.

By advocating for proactive engagement and domestic capability development, the paper offers a nuanced perspective on India's role in shaping the future of LAWS and safeguarding its national interests in an evolving security landscape. In their paper "Techno-ethical Implications of Military Drones, Autonomous Weapon Systems and Lethal Robots: A Case Study of the US War on Terror" (2019), Dan Oshodin and Ayham Aloulabi delve into the profound ethical implications surrounding the use of autonomous weapons systems, particularly within the context of the US War on Terror.

The authors highlight the complex moral dilemmas inherent in the deployment of such technologies, stressing the urgent need for a comprehensive global discourse on the subject. By examining the case study of the US War on Terror, the authors underscore the real-world consequences of relying on autonomous weapons systems in military operations.

They argue that without proper oversight and regulation, the unchecked advancement and utilization of such technologies could lead to catastrophic outcomes. Moreover, they emphasize the imperative of addressing these ethical quandaries on a global scale, given the inherently interconnected nature of modern warfare and technology.

Lt. Gen. P.J.S. Pannu, in his essay "Artificial Intelligence for National Security," published in "The Power of Future Machines" in 2022, presents a thought-provoking analysis of the trajectory of artificial intelligence (AI) in the realm of national security.

He raises pertinent concerns regarding the increasing dominance of machines in human lives, citing the ubiquitous presence of smartphones and electronic devices that permeate everyday existence. This proliferation serves as a harbinger of a future where machines could potentially supersede human control. Central to Pannu's discourse is the burgeoning utilization of autonomous and remotely controlled systems by security forces, particularly in the military domain.

He forecasts a paradigm shift in warfare dynamics, with robotics emerging as a pivotal catalyst for AI-based military operations. Pannu envisions a landscape where traditional weaponry is gradually supplanted by autonomous systems, effectively mitigating risks to human life in combat scenarios.

Methodology

This research employs a mixed research method (primary and secondary) to analyse qualitative data. The study refers to published articles and research papers from various journals and databases, covering different areas ranging from international relations to defence and technology.

By combining both quantitative and qualitative methods, this approach offers a more complete understanding of the research problems. The mixed methods approach provides flexibility in data collection and analysis. While this methodological approach facilitates a comprehensive exploration of complex phenomena, conducting mixed-methods research is complex as it involves designing and executing two different methodologies simultaneously or sequentially. Gathering and analysing both qualitative and quantitative data can be challenging and necessitates meticulous planning and oversight. The synthesis of these data types into a unified narrative often presents challenges, particularly when results from each methodology exhibit substantial discrepancies.

The paper discusses Artificial Intelligence (AI), its sub-areas, ethical concerns related to AI-based tech, implications, and consequences of using such technologies. Additionally, the study provides an in-depth analysis of any available statistical data on the use of AI technology in combat scenarios.

Historical Background of LAWS

Unmanned Aerial Vehicles (UAVs), as part of LAWS (Lethal Autonomous Weapons Systems), have a military history that extends back to the interwar period. The term ‘drone’ was originally coined by U.S. Admiral William H. Stanley in the 1930s to describe remotely piloted aircraft, encapsulates a pivotal dynamic between the operator, often referred to as the ‘mothership’ and the UAV, perceived as a robotic ‘servant’ (Andrejevic, 2016: 22). This

evolution highlights the interplay of human oversight and autonomous capabilities in military applications. The origins of the UAVs can be traced back to the early 20th century specifically following Nikola Tesla's demonstration of remote-control technologies (RCT) which showcased a manipulation of a motorboat via radio waves. The innovations were subsequently adopted by military engineers in both the US and Europe.

During World War 2, the German military employed remote-controlled technologies to deploy unmanned highly explosive miniature tanks known as Goliaths to counter enemy vehicles and fortifications. Similarly, its aerial counterpart, a winged torpedo designated as Fritz was released from an operational aircraft and directed towards targets. The experimental uses of these early UAV advancements were what defined them, and their main purpose was to be disposable in war situations.

Global Trends in LAWS

The U.S. military has historically used various semi-autonomous lethal systems in combat situations. The global community has made concrete efforts to limit or eliminate the use of such weapons, as demonstrated by the Mine Ban Treaty of 1997 and the Convention on Cluster Munitions of 2008. The U.S. has also deployed semi-autonomous weapons as integral components of the air and missile defence framework.

The rapid pace of jet bombers and ballistic missiles constraints the decision-making process for human operators tasked with determining the deployment of such systems for eg – Patriot missiles. While the U.S. has achieved considerable success in various operations using these systems, they have their fair share of errors as well e.g. – the downing of an Iranian commercial airliner by Aegis Air defence force in 1998 and the shooting down of a British Tornado aircraft during the initial phase of Operation Iraqi Freedom in 2003.

Similarly, the Jaeger -C developed by GaardTech is an unmanned ground vehicle (UGV) equipped with anti-tank and anti-personnel capabilities. It is designed for reconnaissance and can silently observe targets using its autonomous image analysis function. Upon detecting a potential target, the vehicle can transition into either Goliath or Chariot mode, depending on the type of target that has been identified. In Goliath mode, it can execute a kamikaze attack to neutralize enemy vehicles. Conversely, in Chariot mode, it engages targets utilizing a concealed weapon, purportedly either a 7.62mm medium machine gun or a 6.5mm sniper rifle. The Jaeger- C comes equipped with an armour-piercing shaped charge, purportedly comparable to the 20-pound warhead found on the FGM-148 Javelin. This attribute grants a notable advantage when engaging lightly armoured tanks. Furthermore, its bulletproof platform boasts a top speed of 50 miles (80 kilometres) per hour, rendering it difficult for adversaries to evade.

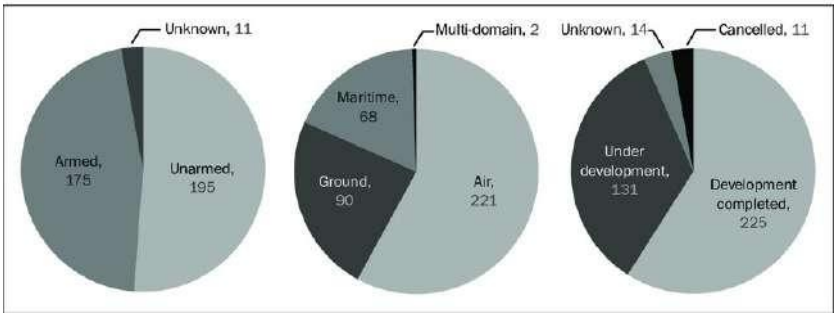
Image - Jaeger-C, Credits - https://www.gaardtech.com.au

Global AI initiatives

The summit on Responsible Use of Artificial Intelligence in the Military Domain (REAIM) took place in Seoul, South Korea, on Monday (September 9) 2024, and is part of the new global diplomacy to shape global norms on the military applications of AI. The summit was co-hosted by Kenya, the Netherlands, Singapore, and the United Kingdom.

This was the second iteration of the summit; the first took place in February 2023 in the Hague and was hosted by the government of the Netherlands. Although there were no dramatic outcomes at The Hague Summit, it broadened the global debate on the military dimensions of AI and brought a wider range of stakeholders into the debate. Formally, the United States issued a unilateral draft political declaration on the responsible use of AI on the last day of the Hague summit and finalised it in November 2023. Washington first published national guidelines on how US armed forces should use AI responsibly last year.

The US also simultaneously presented a resolution on the responsible use of AI at this year's UNGA, which was co-sponsored by 123 countries and unanimously passed. The UN effort focuses on broad objectives and the REAIM process is an attempt to talk about more granular issues and build a large international alliance to register new global norms on military AI.



Military systems included in the SIPRI dataset by (a) frequency of weapon systems compared with unarmed systems, (b) field of use, and (c) status of development. **Courtesy** - SIPRI dataset on autonomy in weapon systems

India took a cautious wait-and-watch approach and did not endorse the Blueprint for Action and previously did not support the Call of Action at the Hauge summit. India is still at the very beginning of the development of AI-based weapons. An AI task force was established by the Government of India in 2018 and the Defence AI Council and Defence AI Project Agency were created in 2019. The government published a list of 75 priority areas of AI in defence including

cyber security, autonomous systems, drones, data processing and analysis etc. India is also exploring options for integrating AI into its space programme and in border security operations.

Category	LAWS	Country	Key Features/Specifications
Air Weapons	**MQ-9A Reaper**	USA	Turboprop-powered, triple-redundant flight control, 7 external payload stations, remotely piloted or fully autonomous, C-130 transportable, over 90% operational availability.
	Mini Harpy	Israel	Compact loitering munition, dual ISR and strike capability, sensors for EO/IR target acquisition, small size for radar evasion, autonomous or semi-autonomous precision targeting.
Ground Vehicles	**Uran-9**	Russia	Tracked chassis, 30mm automatic cannon, anti-tank guided missiles (6km range), Shmel-M flamethrowers, autonomous and manual operation, laser warning systems, and 6km day target tracking range.
	MAARS	USA	Modular armed system, lethal and non-lethal payloads (grenades, machine guns), up to 370 lbs, 1km operational range, day/night cameras, hostile fire localization, motion detectors, and audio systems.
Navy Vehicles	**MANTAS T-Series USVs**	USA	Variants include T-4 to T-20, hydrodynamic hull, 20-60 knots speed range, multi-mission capabilities (ISR, SAR, mine warfare), SeaFlir sensors, and Teledyne sonar systems.

Analysis and Discussion -

Case Study 1 -Israel

In May 2021, during an 11-day conflict between the Israel Defence Forces (IDF) and the Palestinian groups in Gaza, the deployment of LA.W.S specifically AI-guided drone swarms by the Israeli military marked a significant development in the application of AI-based autonomous weapons in modern warfare.

Israeli troops utilised multiple drones to surveil the Gaza Strip, effectively identifying and targeting rocket launch sites operated by Hamas. This operation represents one of the first substantial instances of implementation of drone swarm technology in a real-world conflict scenario, highlighting the evolving nature of military strategies incorporating advanced technologies.

In a significant advancement, the Israel Defence Forces (IDF) deployed artificial intelligence (AI) technology to support human analysts in the examination and interpretation of vast quantities of satellite and aerial surveillance imagery. The primary objective of this initiative was to identify rocket launch sites, including those engineered for recurrent use.

This innovative application of LAWS in military operations led Israeli Military Intelligence to describe the Gaza campaign's first AI-driven war. This characterization underscores the increasing integration of AI in modern warfare, highlighting its potential to enhance situational awareness and operational efficiency.

According to reports, the Israeli military utilized artificial intelligence to deploy small groups of quadcopter drones across the southern Gaza Strip. Each drone was assigned to monitor a specific area, and if a rocket or mortar launch was detected, other armed aircraft or ground-based units were dispatched to neutralize the source of the attack.

Case Study 2 – Libya

Introduction

In 2014, Libya descended into civil war following contested election results. Although multiple actors were involved in the conflict, the primary factions were the Government of National Accord (GNA), endorsed by the United Nations (UN) and the Libyan National Army (LNA). The Struggle between these groups marked a critical phase in Libya's politics, as both vied for control and legitimacy within the country's fractured landscape.

On March 27 2020, the Libyan government under Prime Minister Faiez Serraj launched "Operation Peace Strom", aiming to repel the forces led by General Khalifa Haftar known as Haftar Armed Forces (HAF. The operation represented a significant shift in the tactical application of advanced autonomous weapons systems in modern warfare.

Deployment of Advanced Weaponry

Libya's military strategically applied technologically advanced weaponry, including Firitina T155 155mm self-propelled guns and T-122 Sakarya Sakarya multi-launch rocket systems. These systems targeted the mid-20th-century main battle tanks and heavy artillery that were staples of HAF's arsenal.

During HAF's retreat, Libya's forces deployed unmanned combat aerial vehicles (UCAVs) and LAWS systems such as STM Kargu -2, alongside additional loitering munitions. These assets enabled precision strikes against HAF's retreating units, showcasing a marked tactical advantage achieved through modern autonomous technologies. (2023. Libya, The Use of Lethal Autonomous Weapon Systems.)

Escalation and Strategic Advantage

The operation highlighted an intense increase in UAV assaults, with the United Nations (UN) documenting over 800 UAV-related attacks by HAF up to 2019, compared to the Government of National Accord (GNA) 280. By April, HAF forces had initiated a siege on Tripoli. However, the intensity of the conflict escalated when HAF deployed UAVs, which in urban combat settings, often led to civilian casualties.

International Military Support and Technological Edge

The tactical landscape shifted further following a military agreement between Turkey and the GNA. This accord facilitated an influx of UAVs to the GNA, enabling Libya's forces to launch a counteroffensive to reclaim key strategic assets. One of the most important targets was the Al-Watiya airbase, which had been under HAF control since 2014. This base, positioned just outside Tripoli, had served as a launch point for HAF airstrikes on the capital.

Tactical Outcome and Ceasefire Agreement

Employing Bayraktar TB2 drones, the GNA effectively neutralized multiple Pantsir- S1 (RS-SA-22) short-range air defence systems, which were crucial to HAF's defensive strategies. By May, the GNA had successfully regained control of the Al–Watiya airbase, marking a turning point that eventually lifted HAF's siege of Tripoli in early June 2020. Both eventually led to the formation of a unified government.

Conclusion

Operation Peace Storm underscores the transformative impact of LAWS on modern conflict dynamics. The case of Libya illustrates how access to advanced military, technology particularly UAVs and autonomous weapons, can decisively alter the course of the conflict, effectively bridging the gaps in traditional military assets and reshaping the strategic outcomes.

Table 1.6: **GNA Forces selected UAVs and loitering munitions**

Name	Type/ Country of Origin	Maximum Speed (km/h)	Endurance (hours except where specified)	Sensors/ Payload
Bayraktar TB2	MALE, Turkey	222	27	EO/IR laser designator, MAM-family of munitions
Kargu	Loitering Munition, Turkey	72	15 minutes	EO, warhead
Anka-S	MALE, Turkey	??	24	EO/IR, radar, laser-designator, MAM-family of munitions

Table 1.5: **Libyan National Army selected UAVs and loitering munitions**

Name	Type/ Country of Origin	Maximum Speed (km/h)	Endurance (hours except where specified)	Sensors/ Payload
Wing Loong I	MALE, China	280	20	EO/IR, laser designator, air-to-surface munitions
Camcopter S100 rotary UAVs	ISR UAV, Austria	240	6	EO/IR,
Mohajer-2	ISR UAV, Iran	200	2	EO/IR
Orbiter 3	Tactical ISR UAV	120	7	EO, laser designator

Courtesy-https://www.iiss.org/globalassets/media-library---content--migration/files/research-papers/armed-uninhabited-aerial-vehicles-and-the-challenges-of-autonomy.pdf

Economic Implications of LAWS

The economic impact of investing in LAWS can go far beyond their direct military applications. Significant financial resources allocated to LAWS could lead to substantial budget relocations from other sectors like Education, and healthcare, thereby obstructing economic growth and likely worsening economic inequalities.

Additionally, as governments prioritize spending there may be a corresponding decline in national income, and the opportunity costs incurred from heavy focus on LAWS could pose a barrier to broader developmental outcomes.

The deployment of LAWS may change labour market dynamics, but it has the potential to induce structural unemployment by displacing human roles within military operations. Further impact of this transition is expected to be uneven across the globe, with developed nations likely to adapt more swiftly due to the availability of more resources and better technology, leading to exacerbated economic disparities.

Ethical Concerns arising from the use of LAWS

Absence of Human Supervision and Judgment - It is one of the major drawbacks of AI-based LAWS, these automated systems running on different types of trained models lack human values like empathy, human dignity, and awareness regarding basic human rights, particularly in situations of war, also algorithms, deep learning models embedded in these systems may contain errors, these machines use a large number of datasets which may contain biases, which may present operational challenges risks, and might lead to escalation of the conflict.

Stigmatization and Public Opposition – Lethal autonomous weapons systems face strong criticism from both governmental and non-governmental organizations. The International Campaign to Stop Killer Robots (a collective initiative by various NGOs) aims to seek a ban on lethal autonomous weapons, such opposition reflects widespread societal and ethical concerns about the potential for misuse and unintended consequences of autonomous weapon systems.

Back in 1995, international protocols were put in place to prevent the use of blinding laser weapons. However, discussions about autonomous weapons have been going on since 2014, with not much progress being made.

Susceptibility To Hacking - Lethal Autonomous weapons/ Killer robots are vulnerable to cyber intrusions that can compromise their intended functions. If hacked, such systems could malfunction and potentially pose a threat to operators and allied personnel., rather than targeting adversaries as intended.

In cases where LAWS are integrated with surveillance capabilities, a security breach could allow hackers to utilize these systems for intelligence gathering against the operators or their allies. Such misuse could undermine operational secrecy and introduce significant risks to personnel rather than targeting adversaries as intended.

One of the common threats that weapons are vulnerable to is Integrity attacks; these attacks aim to mislead AI systems into making incorrect decisions. One method, known as data poisoning, involves manipulating the training data, which results in the AI learning faulty patterns. (Saltini, A. (2024). Navigating cyber vulnerabilities in AI-enabled military systems)

In military applications, such manipulations could lead to disastrous consequences, ranging from failures in accurately identifying targets to severe mishaps like misclassifying friendly forces as adversaries.

Another category of integrity attacks is known as evasion techniques, which exploits flaws in models, leading to false identification in detection systems due to even a single altered data point e.g. an attacker could modify a drone image to obscure the presence of an adversary's location or attack points. (Saltini, A. (2024). Navigating cyber vulnerabilities in AI-enabled military systems)

Another category of attacks is the availability attacks, which include denial-of-service (DoS) and ransomware, where the ultimate objective is to cripple critical systems. In the military domain, it would mean disrupting the AI systems, which are intertwined with logistics and supply chains leading to a shortage of supplies. These attacks are not limited to AI-based systems though they present a considerable amount of threat.

LAWS – The accountability gap

Legal Liability - LAWS are designed to make autonomous decisions, often without human intervention. This absence of human 'in-the-loop' protocol complicates decision-making accountability in scenarios where international law or humanitarian principles are breached. Human operators are traditionally accountable for actions taken in war, but the direct responsibility becomes unclear.

Challenges to Identify Responsible Parties – In conventional military operations, responsibility can be assigned to commanders, soldiers, generals, and other personnel involved in the decision-making process. However, with autonomous systems, it is difficult to hold any single person or entity accountable. Manufacturers, software developers, or military personnel who deploy these systems indirectly might share the responsibility, but no individual or organization can be held accountable, especially if the weapon acts unpredictably. (Simon, S. (2019).

Conceptualizing lethal autonomous weapon systems and their impact on the conduct of war - A study on the incentives, implementation and implications of weapons independent of human control.)

Double-Edged Impact for Democracies and Autocracies – For democratic countries, the accountability gap is particularly problematic due to internal and external pressures. Democratic societies may face political instability, protests, political backlash, and the importunity of transparency following incidents involving LAWS misuse.

Conversely, autocracies may face fewer internal repercussions due to their typically more centralized power structures and lower levels of public accountability.

This disparity in accountability can influence decision-making regarding the deployment of LAWS differently across various political contexts. (Simon, S. (2019). Conceptualizing lethal autonomous weapon systems and their impact on the conduct of war - A study on the incentives, implementation, and implications of weapons independent of human control.)

India's Stance on Lethal Autonomous Weapons Systems (LAWS)

India's stance on LAWS centres on a cautious, technology-neutral approach, emphasizing existing frameworks like the CCW (Convention on Certain Conventional Weapons) and Group of Governmental Experts (GGE) as sufficient for addressing LAWS.

India has been an important factor in the Group of Governmental Experts (GGE), whereas with the discussions that allowed the formulation of the eleven guiding principles on lethal autonomous weapons systems (LAWS) – it has played the role of chair. It has given India a platform to influence major dialogues and create the normative agenda that should guide the use of these emerging technologies.

India also opposed a UN General Assembly Resolution on LAWS, citing concerns about duplicative processes. India views GGE as the appropriate, established forum for advocating LAWS discussions, giving priority to GGE groundwork on LAWS and compliance with IHL (International Humanitarian Law).

As India engages in international dialogues concerning lethal autonomous weapons systems (LAWS), its advancements in these technologies could establish it as a pivotal player in shaping global norms and frameworks related to autonomous weaponry.

This involvement may encourage India to promote frameworks that align with its strategic interests. The development of indigenous LAWS could enhance India's strategic autonomy, as self-sufficiency in defence capabilities would strengthen its position within regional and global security landscapes.

Recommendations

Technical

In recent years, there has been a growing trend towards autonomy in both military and civilian technology. However, the rapid advancements in robotics and AI have led to a heightened interest in autonomous weaponry.

While these AI-based systems can be incredibly intelligent, they also present significant dangers, particularly when it comes to the potential risks to human life. As a result, serious

ethical and legal concerns surrounding their use must be addressed. There are three degrees of autonomy by which Lethal Autonomous Weapons Systems can be classified. They are as follows –

- Human-in-the-Loop
- Human-on-the-Loop
- Human -out- of- the-Loop

It is recommended that human oversight should continue to be a critical component in the operation of LAWS, at least over the next few decades. Introducing human–on–the–loop or human–in–the–loop systems can ensure ethical accountability allowing human decision-making processes during warfare scenarios.

Policy

Countries need to set ethical review boards, and the assessments made by these boards should be based on the implications of LAWS for human rights concerns, potential escalations of unintended kinds and how that will affect the mental health of combatants and civilians.

Governments may develop a standardised framework for assessing the legal and ethical implications of LAWS deployments; the criteria should be transparent and accessible, conduct a periodic audit of LAWS focusing on moral standards and operational performance. Reports should be published on a monthly or yearly basis to maintain accountability.

Before the operational deployment of these weapon systems, it is crucial to conduct comprehensive field trials to assess their effectiveness, reliability, and ethical ramifications. The data collected from these trials will be instrumental in evaluating the transition between human-in-the-loop and human-out-of-the-loop operational frameworks.

Defence Agencies can conduct red team penetration testing on LAWS to identify vulnerabilities. They may utilise the expertise of cybersecurity professionals to simulate attacks and propose mitigation strategies.

They can also form an AI and Ethics division tasked with overseeing compliance with the ethical guidelines. This division should be responsible for halting certain projects that may not be by ethical guidelines.

Approaches towards LAWS

United States

The U.S. has not instituted a ban on the development or deployment of LAWS. As per the Department of Defence Directive 3000.09, LAWS are characterised as weapons systems capable of autonomously selecting and engaging targets once activated, without human intervention.

The U.S. emphasises the necessity for retaining a degree of human oversight in operations involving these systems, advocating human control based on operational circumstances. Although there is a significant amount of international pressure for more stringent regulations or outright prohibitions.

European Union

The European Union has taken a proactive stance in discussions surrounding LAWS. Several European states have proposed a two-tier approach within the framework of the Convention on Certain Conventional Weapons (CCW).

This approach recognises that LAWS operating entirely without human control are unlawful and advocates for regulations which guarantee human oversight throughout the lifecycle of

such weapons. The EU's position reflects its compliance with international humanitarian law (IHL) and safeguarding human rights.

China

China's stance on LAWS underscores the necessity for stringent regulations regarding their development and operational parameters. China's representations in international discussions depict LAWS as fully autonomous, which, once activated, cannot be disengaged, which poses a significant threat related to adherence to International Humanitarian Law (IHL).

Moreover, China promotes a multilateral framework for addressing these challenges, emphasising the critical role of collaboration between international organisations over regulating the deployment of LAWS.

Russia

Russia has expressed interest in developing LAWS but is also engaged in discussions regarding its regulation. Russian officials have indicated that while these technologies can significantly enhance military capabilities, it is essential to establish clear guidelines to ensure compliance with existing laws pertaining to armed conflict. Russia's prominence on military readiness may result in resistance to imposing strict restrictions on the progression of these technologies.

Every nation has adopted its approach towards LAWS; these approaches vary widely based on national interests, foreign policy goals, ethical considerations, and interpretations of International Law. As discussions continue with forums like CCW, there is a constant challenge to find a balance between modernisation of technology and humanitarian principles.

Conclusion and Future Prospects

The rapid development of LAWS has led to a new perilous era in technological warfare, It is necessary to highlight significant risks associated with these weapons and accordingly need to be addressed. Over 70 countries have called for a fundamental ban on autonomous weapons systems to ensure that they comply with legal and moral standards. These nations include Argentina, Austria, Brazil, Egypt, New Zealand, Norway, Pakistan and Switzerland among other nations

(https://www.hrw.org/report/2020/08/10/stopping-killer-robots/country-positions-banning-fully-autonomous-weapons-and). China has called for a treaty, while also investing heavily in the development of LAWS.

The case studies of Gaza and Libya offer a clear perspective of the LAWS's ability to improve military effectiveness, limit human involvement on the battlefield, and the ability to act with utmost precision in complex combat scenarios.

Although it is important to note with advantages of such weapons there are potential consequences involved, such as a lack of human oversight, unintended escalations of prevailing conflict, along the security vulnerability of LAWS which makes them susceptible to cyber intrusions, leading to disastrous consequences.

This has led to extensive discussion regarding the psychological effect that would ensue from the deployment of Lethal Autonomous Weapons Systems (LAWS) both on military personnel and civilians. However, the use of LAWS could technically desensitize military people to violence, as the use of LAWS removes some human element of experience and moral judgement in combat situations.

Advocates for LAWS believe that getting the emotions out of making decisions could result in more strategic, rational, and efficient responses from the military. Critics say, however, that this

could encourage people to think of violence as a simple logistical calculation devoid of serious moral quandary.

Furthermore, the deployment of LAWS into combat contexts poses significant ethical and safety problems for civilian populations. The use of LAWS is limited in that they cannot easily be interpreted to distinguish between combatants and civilians, which can result in unintended casualties in their use. In such incidents, their psychical consequences are profoundly psychological and even entail long-lasting traumatization, an increase of fear, insecurity, and in general a general feeling of helplessness over civilian communities that feel in a constant state of vulnerability concerning autonomous, machine-driven violence.

While LAWS may offer functional advantages, their psychological implications and creative contexts for injustice impose a compelling reality check for policymakers and military defence strategists.

References

- *Malhotra, R., Sudarshan, T. N., & Sastry, M. (2023). The Power of Future Machines: Essays on Artificial Intelligence. BlueOneink Publications.*
- *Mohanty, B. (2016). Command and Ctrl: India's Place in the Lethal Autonomous Weapons Regime. ORF (Observer Research Foundation) Issue Brief, (Issue No. 143)*
- *Oshodin, D., & Aloulabi, A. (2019). Techno-ethical implications of military drones, autonomous weapon systems and lethal robots: A case study of the US war on terror.*
- *Reddy, R. S. (2016). India and the challenge of autonomous weapons.*
- *Sauer, F.G., & Schörnig, N. (2012). Killer drones: The 'silver bullet' of democratic warfare? Security Dialogue, 43, 363 - 380.*

INDIC
RESEARCHERS
FORUM

Civilisation • Security • Statesmanship

Indic Researchers Forum
Address: T-12 SMG-II, Ghaziabad
Uttar Pradesh-201005
Website: www.indicrf.org
Email Id: indicrf@gmail.com
Linkedin: Indic Researchers Forum
Twitter, Youtube & Instagram: indic_rf