



AXIA IAS ACADEMY



EDITORIAL ANALYSIS



AUGUST 23



**CONSISTENT
COMPREHENSIVE
AND CREDIBLE**



**UNIQUE AND BEST IN
QUALITY**

- 1. INDIA'S GCC REVOLUTION (THE SUNDAY STATESMAN)**
- 2. Can India build a military-industrial complex? Yes (THE SUNDAY GUARDIAN)**
- 3. Countering extremism is the first condition of prosperity (THE SUNDAY GUARDIAN)**
- 4. The right to hack: How states are rewriting cyber defence (THE SUNDAY GUARDIAN)**



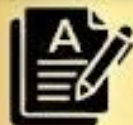
AXIA IAS ACADEMY

UPSC CSE CLASSES

RISE ABOVE THE REST



EXPERT
FACULTY &
GUIDANCE



COMPREHENSIVE
SYLLABUS
COVERAGE



STRATEGIC
TEST SERIES &
MENTORSHIP

ADMISSIONS OPEN

- Prelims + Mains + Interview
- Current Affairs Focus
- Personalized Attention
- Online & Offline Batches



WEBSITE: axiaiasacademy.com



CONTACT: +91 6002-417488



India's GCC Revolution

Now is the time for a comprehensive national policy for the GCCs. The current budget proposed one to guide states in promoting GCCs, particularly in Tier-II cities, with emphasis on talent, infrastructure, building regulation, and collaboration with industry. Of course, six cities cannot carry India's GCCs forever, and hence this focus on Tier-II cities is welcome, but for that the necessary infrastructure must be created to make them GCC-ready.

India has never lacked talent. When India offered no opportunities, they went abroad to work with MNCs. Now that opportunities exist within the country, American and European MNCs are employing our English-speaking engineers, scientists, IT professionals, accountants, and auditors at a fraction of the cost they would have to pay in their own countries. Even then, they are among our best-paid employees. This is transforming our employment and economic landscape, a point often missed by our policymakers who dismiss it as a "domestic brain drain." It has led to runaway growth in a few cities like Bangalore, Hyderabad, Chennai, Pune, etc., where MNCs now own huge offices with thousands of employees who could work across time zones and deliver software and business processes to their headquarters thousands of miles away. These are their Global Capability Centres (GCCs). These GCCs, once back offices for MNCs, have evolved and matured over the years. They now design products, develop intellectual property, manage global technology platforms, conduct research, manage cyber security, develop and deploy agentic AI models, and take decisions for their parent companies. They can transform India from an exporter of services to a global innovation hub if we can get our policies correct. As per the Nasscom Eminent GCC Landscape 2025, India had 1,107 GCCs operating through 127 countries and March 2025, employing 2.36 million people and generating \$96 billion in revenue. The number of GCCs has risen 12 per cent since FY 2023. As a result, the consultancy firm's estimate puts the FY 2025 revenue higher at \$104 bn, or 4.4 per cent of GDP and employment at 6.2 million.

More than 900 companies from the Fortune Global 2000 list now operate GCCs in India. They continue to technology operations, and product engineering about 39 per cent them are operating as "For-profit Hubs", with end-to-end ownership of products, platforms, and intellectual properties, while another 61 per cent are functioning as "Transformation



Hubs" for MNCs that handle all their AI-led operations and perform strategically important functions that directly concern their global business.

GCCs are embedding India into the global value chain, turning it into a major player in the global digital transformation market, estimated between \$1 to \$2 tn, growing annually at around 10 per cent. What China did to manufacturing for the world, India is now doing in services, courtesy the GCCs.

Thirteen GCCs operating in India belong to Accenture, Capgemini, IBM, JP Morgan, Amazon, Infosys, Microsoft, Deloitte, EY, Google, etc. New companies are joining every month - in early 2025, when the oil giant Chevron opened its GCC in Bangalore, it was the 117-year-old company's biggest investment in technology outside North America. The Economic Survey 2025-26 reports that sectors accounted for 51.6 per cent of GDP in the first half of FY 2025-26 while services GVA grew by around 9.3 per cent. Services exports reached an all-time high of \$385.6 billion in FY 2024-25. Services exports have reached around 30 per cent of GDP in the first half of FY 2025-26. A significant part of this growth is owing to the GCCs.

Interestingly, all this has happened without much government intervention or encouragement. Policy makers must now frame a comprehensive policy to attract more GCCs and to use them to transform the core sectors of the economy. Their parent companies are the world's biggest spenders on R&D in areas where India is a laggard. GCCs can channel global R&D investment, technology and expertise into the country to create high end engineering and research while creating spillovers for Indian universities and start-ups.

Geographically, the GCCs remain highly concentrated, with 90 per cent of them located in six cities: Bangalore, Hyderabad, Chennai, Pune, Mumbai and Delhi NCR. With more than 900 centres, Bangalore accounts for almost 40 per cent of GCC activities, followed by roughly 20 per cent each for Hyderabad and Pune.

The government must now encourage them to spread to Kolkata and Tier II cities like Bhubaneswar, Gandhinagar, etc., which can offer overall operating cost advantages of 25-30 per cent compared with traditional Tier I hubs, reduce congestion in Bangalore and other large cities, spread high products to employment to new regions, and include local innovation ecosystems. But it would require public investments in urban infrastructure, airports, high-speed

digital connectivity, and high-quality educational infrastructure in these cities. Structurally also, GCCs are transforming from cost arbitrage to innovation arbitrage. Early GCCs were primarily designed as back offices of MNCs to exploit the advantage of India's large, low-skilled talent. Now they are using the highly specialised talent widely available here that is difficult to reproduce elsewhere at comparable scale and cost.

The Engineering R&D-GCCs have grown 1.5 times faster than the overall GCC sector, indicating a structural shift towards high-value activities. NASSCOM reports that nearly 90 per cent of R&D now operates in intellectual centres, while more than half have evolved into portfolio or transformation hubs. India has developed a pool of more than 120,000 AI/ML professionals associated with GCCs and over 165 dedicated AI/ML centres of excellence. With about 28 per cent of the global STEM workforce and 23 per cent of global software engineering talent, India is a major player in the GCC ecosystem, poised for a large expansion.

GCCs are also building our AI ecosystem, a crucial step towards bridging the massive gap that today exists between India and the US/China. The 2025 GCC Pulse Survey by EY Young & Rubicam (EY) found that 83 per cent of Indian GCCs were investing in generative AI, while 38 per cent were already investing in agentic AI, and another 29 per cent planned to do so within a year. GenAI spend increased from 37 to 43 per cent during the year, while 81 per cent of GCCs were upskilling their internal teams in GenAI. Other than AI, the focus is also on healthcare, pharmaceuticals, automotive, aerospace, and semiconductors.

EY reports that 23 of the world's top 50 life-sciences companies have established GCCs in India. This diversification creates a massive cluster of global technological capabilities into India, which imports specialised knowledge to Indian engineers and scientists, which then subsequently diffuses into Indian broader start-up and industrial ecosystem, raising productivity and attracting more global corporations into India. Nasscom Eminent reported that Indian engineering R&D-GCCs were growing 1.5 times faster than the overall R&D sector, indicating increasing public investments in and focus on a complete ecosystem change

up the value chain. India can emerge as the world's leading AI hiring market within the GCC ecosystem. Data already suggests a paradigm shift of Indian GCCs from delivery towards global ownership. AI would accelerate this transformation through the process of creative destruction in which the old model and its practitioners would perish, but in the process, GCCs might become the principal drivers of MNCs bringing state-of-the-art AI technology and investments into India. IPWT data show that cumulative FDI equity inflows into IT between April 2020 and September 2023 were about \$197 billion, equivalent to 10 per cent of total FDI equity inflows over this period.

Now is the time for a comprehensive national policy for the GCCs. The current budget proposed one to guide states in promoting GCCs, particularly in Tier II cities, with emphasis on talent, infrastructure, building regulation, and collaboration with industry. Of course, six cities cannot carry India's GCCs forever, and hence this focus on Tier II cities is welcome, but for that the necessary infrastructure must be created to make them GCC-ready.

A GCC Advisory Committee under MoITV subsequently discussed six broad pillars: fiscal support, regulatory ease, talent, infrastructure, branding, emerging hubs, innovation and technology leadership, and a future-ready talent ecosystem. These cannot be achieved unless we have a National GCC Mission, jointly led by the Centre and states whose objective would be industry-linked advanced skill building, creating GCC-ready Tier II cities, incentivising R&D and intellectual property creation, and facilitating systematic GCC-university startup partnerships.

Rather than simply maintaining the number of centres, its goal should be quality-adjusted growth, measured by the number of patents, R&D expenditure, global products developed, startup partnerships formed, export revenue earned and high skilled jobs created. There is a huge shortage of talent to precisely the areas the GCCs need it most: advanced AI, semiconductor design, chemically quantum computing, cloud architecture, product development, and research leadership.

A 2026 PwC EYCC study found that 11 per cent of GCC leaders reported their global headquarter considering shifting GCCs to alternative locations because of talent constraints. The problem is the absence of linkage between our higher education ecosystem and broader industry requirements. To address this, the government must re-think its industry designed programmes in these areas and encourage the GCCs, through fiscal or other incentives, to establish joint laboratories with IITs, IIMs, and universities to promote GCC-university startup networks.

Government may also provide selective performance-based targeted fiscal incentives and establish an agency GCC single-window clearance mechanism for everything connected with their operations to improve regulatory ease across the entire GCC lifecycle. The question is no longer whether India will equitably benefit from this, or whether it will. The global innovation hub will have to be placed

BY NALIN K. K. NALIN K. K.

- **Key Terms and Conceptual Framework**

- **Global Capability Centres (GCCs):** Strategic, specialized offshore client-owned units established by multinational corporations (MNCs) to handle complex operations, ranging from end-to-end product design, intellectual property (IP) development, and global cybersecurity to frontier artificial intelligence (AI) and enterprise leadership. *Example:* Rather than merely managing customer billing, an automotive MNC's Indian GCC engineers the autonomous navigation algorithms and battery management firmware for its worldwide electric vehicle fleet.
- **Cost Arbitrage vs. Innovation Arbitrage:**
 - *Cost Arbitrage:* Relocating operational workflows to lower-wage destinations solely to cut labor costs (the legacy IT/Business Process Outsourcing model).
 - *Innovation Arbitrage:* Capitalizing on dense ecosystems of elite scientific, mathematical, and software talent to invent new business paradigms, secure patents, and accelerate high-value global R&D at scale.
- **Portfolio Hubs:** Advanced capability units that exercise complete lifecycle ownership over core products, digital platforms, and intellectual assets, functioning as independent strategic business entities rather than support arms.
- **Transformation Hubs:** Elite organizational nodes explicitly tasked with driving global digital transformations across a corporation, leveraging agentic AI and automated workflows to reinvent strategic enterprise processes.
- **Creative Destruction in Knowledge Services:** A Schumpeterian economic process whereby advanced cognitive automation and generative/agentic AI dismantle legacy manual IT maintenance jobs while simultaneously generating higher-order roles in architecture, machine learning (ML) operations, and deep-tech innovation.
- **Triple Helix Model:** An innovation framework based on symbiotic institutional collaboration among government policymakers, academic research institutions, and private industry to commercialize cutting-edge R&D and build industry-aligned human capital.
- **Engineering Research & Development (ER&D):** High-end engineering activities dedicated to designing physical hardware, embedded software, complex systems, and industrial platforms, representing the frontier of manufacturing-technology integration.

- **Core Thematic Pillars and Substantive Analysis**

- The structural evolution of India's services paradigm marks a decisive shift from routine outsourcing to the strategic command centers of global commerce.
 - **Macroeconomic Anchor of Growth:** Services account for 53.6% of Indian GDP (H1 FY2025-26), with services Gross Value Added (GVA) expanding at 9.3% and total services exports reaching a record \$387.6 billion in FY2024-25 (~10% of GDP). GCCs serve as a primary engine of this structural expansion, expanding from \$98 billion in FY2021 to projected revenues of \$164 billion (4.4% of national GDP) and employing 4.2 million high-skilled professionals by FY2026.
 - **Ascent up the Global Value Chain (GVC):** Over 500 Forbes Global 2000 corporations maintain Indian centers. Indian operations now function beyond operational support: 39% operate as autonomous "Portfolio Hubs" with end-to-end ownership of intellectual property, and 5% operate as high-level "Transformation Hubs" governing multinational AI deployments. ER&D GCCs are expanding 1.3 times faster than the broader sector, turning India into a core driver of the \$1 trillion to \$2 trillion global digital transformation market.
 - **The AI and High-Tech Frontier:** India houses 28% of the world's STEM workforce, 23% of global software engineering talent, more than 120,000 specialized AI/ML engineers within GCCs, and over 185 dedicated AI/ML Centres of Excellence (CoEs). Up to 83% of Indian GCCs actively invest in Generative AI, and 58% invest in autonomous Agentic AI architectures, closing the bilateral high-tech gap with leading digital economies.
 - **Spatial Concentration and the Tier-II Imperative:** Nearly 90% of all capability centers remain tightly clustered in six Tier-I metropolitan zones: Bengaluru (~40%), Hyderabad (~20%), Pune (~20%), Chennai, Mumbai, and Delhi-NCR. This extreme concentration strains civic infrastructure, inflates real estate overheads, and accelerates regional inequality. Relocating future expansion toward Tier-II and Tier-III cities (such as Indore, Bhubaneswar, and Guwahati) unlocks a 25–50% operating cost advantage and decentralizes modern employment opportunities.
 - **The Talent Bottleneck Paradox:** Despite an abundant aggregate workforce, an acute shortage persists in specialized domains like advanced AI, semiconductor architecture, quantum computing, cybersecurity, and frontier cloud infrastructure. This structural mismatch prompts 11% of global GCC leaders to weigh alternative overseas destinations, underscoring the urgent need to align higher education curricula with global frontier research.

- **Historical Evolution: From Brain Drain to Innovation Hub**

- **Pre-1991 (Era of Brain Drain):** Constrained domestic industrial capacity and strict state controls led premier engineering and scientific graduates to migrate abroad to work for Western multinational corporations. Domestic technology exposure was minimal, with high-skilled human capital treated largely as an export without local value capture.
 - **1990s to Early 2000s (Economic Liberalization and Cost Arbitrage):** The 1991 New Economic Policy, telecommunications deregulation, and the global Y2K remediation challenge triggered the first wave of IT outsourcing. Operations focused almost exclusively on low-end cost arbitrage, basic software maintenance, and business process outsourcing (BPO).
 - **2000s to 2015 (Rise of Global In-House Centres - GICs):** Multinationals shifted from third-party outsourcing vendors to wholly owned captive centers. Between April 2000 and September 2025, cumulative Foreign Direct Investment (FDI) inflows into the computer software and hardware sector reached \$119.7 billion, representing 16% of India's total gross FDI. GICs gradually expanded from back-office support into enterprise IT management, financial analytics, and regional service delivery.
 - **2016 to Present (The GCC Innovation Epoch):** Captive centers rebranded and restructured into Global Capability Centres, driving core intellectual property creation, applied AI, semiconductor layout design, and global organizational decisions. With national initiatives like the Digital India Mission, MeitY's GCC Advisory frameworks, and proposed State-level GCC policies, the ecosystem has moved from organic corporate clustering to structured state-level industrial policy.
-



AXIA
IAS ACADEMY
RISE ABOVE THE REST

**INDIA'S GCC REVOLUTION:
A COMPREHENSIVE
UPSC CSE ANALYSIS.**

KEY TERMS & CONCEPTS

GCC
Strategic client-owned units vis. tech-innovation



Example:
A's EV fleet algorithm designed in India

Cost vs. Innovation Arbitrage



Example:
A's EV fleet algorithm designed in India

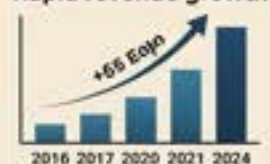
Portfolio & Transformation Hubs



Example:
A's EV algorithm designed in India

MAIN ARGUMENTS

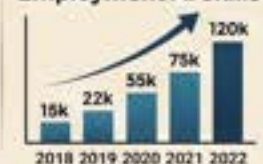
Rapid revenue growth



Rise of AI skills



Employment AI skills



"talent paradox" constraints:

- "talent's nonsimmet" constraints
- "talent paradox" to the assignment

LOGICAL FOUNDATION



Endogenous growth:
Knowledge accumulation of sctorce e-nosystem



Knowledge diffusion:
Spillover to domestic domestic ecosystem



Spatial justice principles:
Spatial justice principles to both domestic ecosystem

MULTIDIMENSIONAL ANALYSIS (GS 1-4)



Economic

- CAD Stability
- Urban Multipliers



Social

- High-income Jobs
- Urban strain



Political

- Building of Power
- Direction of social interactions



Legal

- GCC Innovation
- Stability, and Urban Multipliers



Ethical

- AI bias
- Reskilling
- Urban Alliance in situation



International

- Global economy & diosystics
- International information

SPATIAL EVOLUTION: TIER-I TO TIER-II HUS.



CURRICULAR LINKAGES

UPSC GS Paper	
Class 12	Macro/Geography
Class 12	NCERT Themes
GS 3	Economic Growth, Economic Growth, ER&D, Ennovation, Innovation
GS 4	Growth, ER&D, S&T Innovation
Essay	Essay, GVA
Optionals	Urotono Growth

HISTORICAL JOURNEY: FROM BACK-OFFICE TO STRATEGIC HUB



Brain Drain

Brain Drain
Just submissions or migrating in figures



IT/BPO Boom
Early computers, early phone computers.



GCC Innovation Epoch
Advanced robotics advanced rehotics and visualizations

CURRICULAR LINKAGES

WAY FORWARD

- 1 National GCC Mission**
 - Develop point step intertrations
 - Ractional GCC mission
- 2 Academia-GCC Links**
 - Co-funded lab with co-funded lab resources
- 3 Tier-II Infra**
 - Ploadmap to acrost with plug-and-play SEZ
- 4 IPR & Data Regime**
 - Learn-ring rconilation and inclusion

PYQ THEMES: CORE CONCEPTS TO RECALL

Concise keywords for past exams:

- Services GVA
- Human Agglomeration
- Human Capital Formation
- Human Cantnuntor
- Urban Agglomeration

axiaiascademy.com

+91 6002-417488

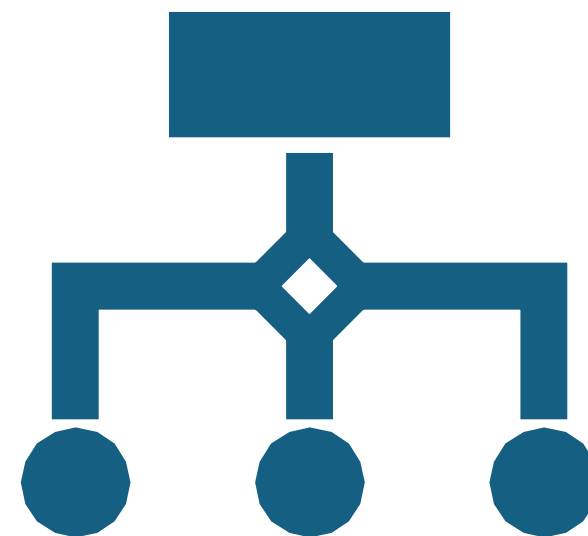
- **Logical and Philosophical Foundations**

- **From Comparative Advantage to Endogenous Growth:** Classical Ricardian trade theory posited that emerging economies should specialize in low-cost, labor-intensive tasks. The contemporary GCC paradigm validates Paul Romer's Endogenous Growth Model: economic returns are driven primarily by internal human capital formation, knowledge accumulation, and ideational spillovers, enabling emerging markets to export high-complexity non-rival software and IP designs.
- **Dialectics of Knowledge Diffusion (Agglomeration Spillovers):** When Fortune 500 corporations embed high-end laboratories within a developing economy, specialized knowledge diffuses outward. Domestic engineers, data scientists, and managers absorb international best practices and subsequently launch domestic deep-tech startups, advise domestic universities, or lead public technological missions, igniting a virtuous cycle of domestic capability building.
- **Spatial Justice and Balanced Regional Development:** The geographic concentration of high-paying knowledge jobs in select Tier-I clusters breeds severe economic dualism. Applying regional development principles (such as Gunnar Myrdal's Spread and Backwash Effects) requires public investments in Tier-II and Tier-III cities to decentralize prosperity, curb metropolitan infrastructural decay, and distribute high-income livelihoods more equitably.
- **Paradigm Shift in Talent Economics:** Reframing global corporate employment from an exploitative "brain drain" into a sovereign "brain gain" and "talent retention" dynamic. Retaining world-class engineers within domestic borders preserves domestic consumption, builds up local direct tax bases, and anchors sovereign intellectual ecosystems without requiring emigration.

Multidimensional Analysis	
Dimension	Critical Analytical Vectors
Economic	- Generates foreign exchange earnings, helping stabilize the Current Account Deficit (CAD). - Yields deep multiplier effects across commercial real estate, urban retail, aviation, and domestic services. - Shifts the macro trade mix from low-margin commodity exports toward high-margin intellectual and digital services exports.
Social	- Expands high-income white-collar employment for engineering, accounting, and life sciences graduates. - Alleviates metropolitan strain by creating formal tech corridors in emerging urban centers (e.g., Indore, Guwahati). - Deepens economic divides between specialized STEM professionals and the broader informal workforce.
Political & Governance	- Incentivizes competitive federalism as States design specialized GCC policies, single-window clearances, and fiscal subsidies. - Necessitates coordinated Center-State industrial governance across MeitY, DPIIT, and state IT departments. - Focuses municipal reforms on transit-oriented urban planning and digital public infrastructure.
Legal & Regulatory	- Requires rigorous compliance with the Digital Personal Data Protection (DPDP) Act for cross-border data flows. - Demands robust enforcement of Intellectual Property Rights (IPR) to secure proprietary enterprise algorithms. - Entails structural updates to national labor codes to support hybrid arrangements and round-the-clock global workflows.
Ethical & Epistemic	- Involves governing frontier AI models to prevent systemic algorithmic bias, data privacy breaches, and opaque decision-making. - Requires proactive structural safety nets to reskill workers displaced by agentic AI automation. - Balances corporate IP ownership against fair public and domestic academic access to frontier research.
International Relations	- Enhances India’s geotechnological standing in global critical and emerging technology supply chains (e.g., iCET). - Strengthens digital trade ties and bilateral services partnerships with North America and Europe. - Embeds India as an indispensable knowledge hub in multinational corporate architectures.

- **Curricular Linkages with NCERT Textbooks**
 - **Class 12 Macroeconomics (Chapter 6: Open Economy Macroeconomics):** Directly illustrates how services exports and cross-border invisibles balance structural merchandise trade deficits and preserve sovereign foreign exchange reserves.
 - **Class 12 Indian Economic Development (Chapter 3: Liberalisation, Privatisation and Globalisation):** Exemplifies the long-term structural outcomes of post-1991 economic reforms, tracing the shift from industrial licensing to an open, globalized, high-technology services economy.
 - **Class 12 Indian Economic Development (Chapter 5: Human Capital Formation in India):** Serves as a prime case study for how sustained public-private investments in tertiary education, STEM capability, and technical literacy yield high-productivity economic growth.
 - **Class 12 Fundamentals of Human Geography (Chapter 7: Tertiary and Quaternary Activities):** Provides theoretical definitions for quaternary (knowledge-based) and quinary (executive decision-making) economic activities, mapping directly to GCCs evolving into strategic decision centers.
 - **Class 12 India: People and Economy (Chapter 10: Geographical Perspective on Selected Issues and Problems):** Links directly to urban agglomeration dynamics, infrastructure bottlenecks in mega-cities, and the necessity of decentralized urban-industrial planning.

- **Linkages with the UPSC CSE Syllabus**
 - **General Studies Paper 1 (Society, Urbanization, and Geography):**
 - *Urbanization Challenges:* Metropolitan congestion, internal labor migration, and the spatial planning of Tier-II counter-magnet cities.
 - *Social Empowerment:* Changes in demographic dividend utilization and the expansion of the high-income middle class.
 - **General Studies Paper 2 (Governance, Public Policy, and Ease of Doing Business):**
 - *Government Interventions:* Formulating a National GCC Policy, MeitY's six-pillar development framework, and performance-based incentive structures.
 - *Regulatory Architecture:* Simplifying single-window clearance mechanisms, labor compliance, and cross-border digital trade frameworks.
 - **General Studies Paper 3 (Economy, Science & Technology, and Industrial Growth):**
 - *Economic Development & Employment:* Services sector contributions to GDP, export diversification, and high-productivity job creation.
 - *Science, Technology & Innovation:* Deep-tech adoption, Generative and Agentic AI deployment, ER&D expansion, and domestic IP generation.
 - *Infrastructure:* Digital public goods, high-speed connectivity, tech parks, and commercial real estate assets.
 - **General Studies Paper 4 (Ethics, Integrity, and Aptitude):**
 - *Technological Ethics:* Ethical parameters of automated decision systems, algorithm accountability, and workforce displacement due to cognitive automation.



- **Way Forward and Policy Roadmap**

- **Launch a Dedicated National GCC Mission:** Establish an institutionalized Union-State task force across MeitY, DPIIT, and state IT departments. This mission should implement standard operating procedures, unified single-window digital clearance systems, and performance-linked fiscal benefits tied to domestic patent registrations and global product launches.
- **Operationalize the Triple Helix Framework in Higher Education:** Address the talent bottleneck by mandating joint curriculum design between leading universities (IITs, IISERs, central universities) and capability centers. Co-finance industry-led research laboratories, institute deep-tech fellowships in quantum computing, semiconductor architecture, and advanced AI, and incentivize private R&D grants.
- **Build Infrastructure in Tier-II and Tier-III Cities:** Develop high-grade, plug-and-play Special Economic Zones (SEZs) and technology parks in emerging hubs such as Indore, Bhubaneswar, Coimbatore, and Guwahati. Offer sub-lease fiscal incentives, municipal property tax rebates, and high-speed digital connectivity to lower corporate migration barriers and relieve pressure on Tier-I metros.
- **Modernize the Intellectual Property and Data Regime:** Strengthen domestic patent examination infrastructure to cut approval times for enterprise software and algorithms. Align cross-border transfer approvals under the DPDP Act with international data standards to maintain legal certainty for multinational portfolios.
- **Catalyze GCC-Startup-University Innovation Flywheels:** Provide structured tax incentives for capability centers that mentor, incubate, or acquire domestic deep-tech startups. Establishing shared sandboxes and open innovation ecosystems allows MNC technology and domain expertise to spill over into domestic industrial sectors.



Mains

- **2024 (GS Paper 3):** "The shift from low-end IT outsourcing to high-value Engineering Research and Development (ER&D) and Artificial Intelligence represents the coming of age of India's knowledge economy." Analyze the structural drivers and policy imperatives of this transition.
- **2022 (GS Paper 3):** "Economic growth in recent decades has been predominantly driven by the services sector, yet manufacturing remains essential for inclusive job creation." Critically evaluate the role of high-skill services versus labor-intensive industrialization in India's long-term development.
- **2020 (GS Paper 1):** "Account for the spatial concentration of information technology and high-tech industries in specific metropolitan clusters in India. What measures are required to foster balanced regional industrialization in Tier-II and Tier-III cities?"
- **2017 (GS Paper 3):** "Stemming the 'Brain Drain' and converting it into 'Brain Gain' requires an institutional ecosystem that bridges academia, government, and industry." Discuss in the context of emerging technology ecosystems in India.

Assam Public Service Commission (APSC) & State PSC Focus

Prelims

- **APSC CCE (Prelims):** With reference to the development of the IT and services sector in Northeast India, consider the following:
 - The 'Tech City' initiative near Guwahati aims to position Assam as a regional hub for IT/ITeS and electronics manufacturing.
 - Guwahati has emerged as an expanding Tier-II destination for high-tech services due to its strategic connectivity and talent base.
 - *Which of the statements given above is/are correct?*

Mains

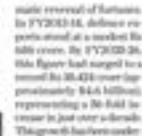
- **APSC CCE (GS Paper 3):** "Tier-II cities in Eastern and North-Eastern India, particularly Guwahati, hold significant potential to capitalize on the decentralization of Global Capability Centres (GCCs)." Discuss the infrastructure, policy, and educational reforms necessary for Assam to attract high-value technological investments.
- **APSC CCE (GS Paper 5 - Assam Section):** "Examine the potential of the services and high-technology sectors in transforming Assam's economic landscape, moving beyond traditional agriculture and resource extraction."



agreement to sell 100,000 tons of rice to Vietnam, making a significant expansion of the defense footprint in Southeast Asia.

Indonesia has also signed a cooperation agreement on the Comprehensive Indonesia System sharing Prince Sultan's new MoD's rail, shore and air defense systems. Indonesia is now sending defense expert staff across ASEAN. Once these agreements are reached, the United States and Indonesia will become the second certified

**DIPLOMACY THROUGH
DEFENCE**



planted by the Government of
Malawi, 1980. (Malawi, 1980)

The policy architecture supporting this transformation includes the Defense Acquisition Procedure (DAP) positive indigenization lists, and the establishment of free-defense industrial corridors. The private sector has emerged as a critical driver, contributing its US\$600 million (46.4%) of defense exports in FY2005-06, while Defense Public Sector Undertakings (DPSUs) accounted for the remaining 34.5%. Roughly 140 Indian companies are

repeated in some cases for
convenience, with the repeat
factor in brackets.

ing explicit and platform such as BlackBerry, Windows, Apple, etc. devices.

	2004-2005	2005-2006
Production	1,000,000 tons	1,000,000 tons
Consumption	1,000,000 tons	1,000,000 tons

[illegible]

various principles, jointly developed by India's Defense Research and Development Organization (DRDO) and

Source: U.S. Census Bureau, *U.S. Economic Outlook*, 1992.

at nearly Mach 2.8 (three times the speed of sound) and has become one of the fastest accelerators in the

2004

AN INDIAN MILITARY-INDUSTRIAL COMPLEX

India's emergence as a dominant regional power has created significant for its global standing. Historically, India's status as the world's largest arms importer has provided it with considerable economic and diplomatic leverage by increasing this dynamic. New Delhi is becoming it is a reliable security partner for many nations, and is now a leading provider of advanced technology to friendly nations. This transformation enhances India's credibility as a global security power, and is becoming a highly technologically valued by states seeking alliance with it.

The region that deals with

© 2006 The Authors
Journal compilation © 2006 Blackwell Publishing Ltd

the Philippines, for instance, has deepened bilateral ties and positioned India as a counterbalance to China's growing assertiveness in the South China Sea. Similarly, the Vietnam and Indonesia agreements also signal India's willingness

support. MAMAV's activities in strengthening their coastal defenses, aligning with New Zealand's Act-Last Policy and initiatives of a few, Japan, and Indonesia look Pacific. These transactions are not merely commercial; they show strategic investments in long-term partnerships, creating interdependencies that enhance India's diplomatic influence.

Moreover, defense exports enable India to project power through its technology transfer and capacity building. Unlike traditional aid or diplomatic overtures, defense sales create enduring relationships, providing

in mutual security interests. Countries that border India's northern frontiers are stabilised only in India's strategic interest. Instability along these frontiers is a danger to India's internal security to consider her own. This is particularly evident in India's growing defence ties with Armenia, which has emerged as a significant buyer of Indian weapons amid its troubles with Azerbaijan and Pakistan.

The *Neophila salicicola*, as the name of this effort.

India's defence export strategy is increasingly linked to its broader diplomatic objectives. By supplying advanced systems like BrahMos, New Delhi is signalling its readiness to support partners in deterring aggression and maintaining regional stability. This approach harmonises with countries wary of over-reliance on traditional suppliers like the US or the UK, both of which come with political strings attached. India, by

conditions, making it an attractive option for authors

The diversification of Israeli export basins beyond missiles to include naval systems (which now account for nearly 50% of defence exports), artillery guns, radars, and aircraft, will further underscore its growing capabilities. This breadth enables Israel to cater to a wider range of security needs, from maritime domains to access to low-tier defence, enhancing its appeal as a comprehensive defence partner.

DeBorja's expatriation serves as a total first dispensing time with her origins, for she left Egypt, the birthplace of her culture, to live in a new environment.



© 2014 Pearson Education, Inc. or its affiliate(s). All rights reserved.



1001



© 2013 Pearson Education, Inc.

- **Key Terms and Explanations**

- **Atmanirbhar Bharat in Defence:** A strategic shift from being an import-dependent buyer to an indigenous designer, developer, and producer of military hardware. Rather than pursuing autarky (complete isolation), it emphasizes building resilient domestic supply chains, integrating Indian micro, small, and medium enterprises (MSMEs), and retaining intellectual property within the country.
- **Positive Indigenisation Lists (PILs):** Policy instruments notified by the Ministry of Defence that place phased import bans on specific military platforms, weapon systems, sub-assemblies, and components. Once an item is listed and its deadline passes, the armed forces can procure it solely from domestic manufacturers.
- **Defence Acquisition Procedure (DAP) 2020:** The overarching regulatory rulebook governing military procurement in India. It accords the highest procurement priority to the **Buy (Indian-IDDM)** category—*Indigenously Designed, Developed, and Manufactured*—mandating at least 50% indigenous content.
- **Strategic Autonomy:** The capacity of a sovereign nation to formulate and execute national security and foreign policy decisions based entirely on its own national interests, free from foreign political coercion, technological sanctions, or diplomatic leverage.
- **Net Security Provider:** A state that actively stabilizes its regional maritime and continental neighborhood by providing capacity-building support, disaster relief, joint patrolling, and military hardware to friendly foreign nations, rather than merely securing its own physical borders.
- **Defence Industrial Corridors (DICs):** Dedicated geographic clusters (currently established in Uttar Pradesh and Tamil Nadu) designed to create an integrated ecosystem linking aerospace and defence public sector undertakings, private conglomerates, MSMEs, incubation hubs, and academic institutions.
- **Supersonic vs. Subsonic Cruise Missiles:** Subsonic missiles (like the American Tomahawk or Indian Nirbhay) fly below the speed of sound ($< \text{Mach } 0.8$), prioritizing range and fuel efficiency. Supersonic missiles (like the BrahMos) fly at speeds near Mach 2.8 to Mach 3, using sheer kinetic energy and compressed reaction times to evade modern shipborne radar and point-defence interceptors.
- **Defence Lines of Credit (LoC):** Concessional, government-backed sovereign financing extended by New Delhi to friendly nations (such as Vietnam, Mauritius, or Armenia), enabling them to procure Indian-made defence equipment without immediate balance-of-payments strain.

- **Main Arguments and Substantive Analysis**

- **Core Thesis:** India's transition from the world's leading arms importer to a credible defence exporter marks a profound geopolitical evolution. Military-industrial self-reliance transforms defence trade from a simple commercial enterprise into an active instrument of statecraft, deterrence, and strategic autonomy.
 - **Structural Reversal of Trade Velocity:** The expansion of defence exports—growing from ₹686 crore in FY 2013–14 to over ₹38,000 crore in FY 2025–26, with a trajectory targeting ₹50,000 crore by 2029—signals a systemic industrial transformation. Domestic manufacturing now accounts for approximately 65% of domestic military procurement, significantly reducing the traditional 65–70% import dependency.
 - **Democratization of the Manufacturing Base:** The domestic defence landscape is no longer the exclusive preserve of Defence Public Sector Undertakings (DPSUs). Private aerospace and defence entities now account for nearly 45% of total defence exports, supported by tier-2 and tier-3 MSME supplier networks.
 - **Hardware-Driven Strategic Diplomacy:** Exporting advanced systems like the BrahMos cruise missile to ASEAN members (such as the Philippines, Vietnam, and Indonesia) bolsters their coastal deterrence in the South China Sea. This aligns directly with India's **Act East Policy** and provides partner nations with a reliable, non-coercive alternative to Western or Chinese military hardware.
 - **Counter-Arguments and Structural Vulnerabilities:** Despite rapid expansion, India's share of the global arms export market remains modest (< 2%) relative to established superpowers. Key vulnerabilities persist:
 - *Critical Component Dependency:* Continued reliance on foreign suppliers for critical sub-systems, high-end semiconductors, specialized marine gas turbines, and advanced metallurgy.
 - *Joint-Venture Geopolitical Constraints:* Systems developed with foreign partners (such as Russian involvement in BrahMos) face potential friction under Western sanctions regimes like CAATSA when pitched to certain prospective buyers.
-

- **Historical Evolution of India's Defence Industrial Base**

- **Colonial Period to Independence (Pre-1947):** British-era Ordnance Factories functioned primarily as secondary repair facilities and basic ammunition manufacturers for imperial forces. India inherited no indigenous research, design, or high-technology military manufacturing infrastructure.
- **Post-Independence and the 1962 Inflection Point (1947–1962):** Early policy focused on civilian socio-economic industrialization, leaving national security dependent on off-the-shelf British and French imports. The 1962 Sino-Indian War exposed severe logistical and operational gaps, prompting the establishment of the Defence Research and Development Organisation (DRDO in 1958) and the Department of Defence Production (1962).
- **Import Substitution and Soviet Alignment (1965–1990):** Western arms embargoes during the 1965 and 1971 conflicts led New Delhi to turn toward the Soviet Union for licensed production (e.g., MiG aircraft, T-72 tanks). While this boosted domestic assembly capacity, true intellectual property and design capabilities remained foreign. In 1983, Dr. A.P.J. Abdul Kalam launched the **Integrated Guided Missile Development Programme (IGMDP)**, laying the groundwork for strategic missile systems: *Prithvi*, *Agni*, *Akash*, *Trishul*, and *Nag*.
- **Post-Pokhran II to Strategic Joint Ventures (1998–2014):** The 1998 nuclear tests and the 1999 Kargil War highlighted the dangers of international supply-chain blockades during crises. In 1998, India and Russia formed the **BrahMos Aerospace Joint Venture**, combining Russian propulsion technology with Indian guidance, software, and fire-control systems. In 2001, the defence sector opened to 26% private and foreign investment, yet procedural bottlenecks kept India as the world's largest arms importer.
- **Atmanirbhar Bharat and the Export Pivot (2014–Present):** A major structural overhaul began with the corporatization of the 200-year-old Ordnance Factory Board (OFB) into seven specialized DPSUs in 2021. The introduction of Defence Acquisition Procedure (DAP) 2020, Positive Indigenisation Lists, Defence Industrial Corridors, and the Innovations for Defence Excellence (iDEX) framework transformed the private sector into a primary driver of research, development, and exports.



AXIA
IAS ACADEMY
RISE ABOVE THE REST

INDIA'S STRATEGIC TRANSFORMATION: FROM ARMS IMPORTER TO GLOBAL DEFENCE EXPORTER

A COMPREHENSIVE ANALYSIS
FOR UPSC CSE PREPARATION

FLAGSHIP WEAPON: BRAHMOS SUPERSONIC CRUISE MISSILE

- SPEED: MACH 2.8 (Supersonic)
- COMBAT PROVEN (OP SINDOOR)
- JOINT INDO-RUSSIAN VENTURE (DRDO & NPO M)



EXPORT FOOTPRINT

Philippines: \$375M (2022/24)
Vietnam: \$620M (2026)
Indonesia: Deal (May 2026)
FUTURE: BrahMos-NG (Next Generation) (lighter, Flight tests began 2026)

PANEL 1: INDIA'S STRATEGIC PIVOT (INTRODUCTION & GEOPOLITICS)

PAST: WORLD'S
LARGEST IMPORTER



65-70% dependent

FUTURE:
EMERGING EXPORTER



<35% dependency



Net Security Provider in Indo-Pacific



Strategic Autonomy & Diplomacy through Trade

PANEL 4: GEOPOLITICAL IMPACTS & NET SECURITY PARTNER

INDOMID-PACIFIC



Maritime Domain Awareness



Counter-terrorism



Countering China/Russia dependency

BALANCED STRATEGIC PARTNERSHIPS
(e.g., ASEAN, Armenia)

PANEL 2: ATMANIRBHAR BHARAT: THE DEFENCE ECOSYSTEM

POSITIVE INDIGENISATION LISTS



DEFENCE ACQUISITION PROCEDURE (DAP) 2020



PRIVATE & DPSU SYNERGY



UPSC CSE LINKAGES & WAY FORWARD



GS PAPER LINKAGES

Target	Analysis
GS-2	Brief peak points from analysis media to unwehmonal intogranms
GS-3	Phased domestas from analysis Dond /konperison vail

GS PAPER LINKAGES

GS-3	Analysis orator denones and litoral defense
GS-4	Analysis identifiial datans/ countasdon procurements

NCERT LINKAGES

Class 12 Pol. Sci. Class 10/12 Econ/Geog

- EXPAND R&D (IDEX, TDF)
- STREAMLINE CERTIFICATION (DGQA)
- SECURE SUPPLY CHAINS (Specialty Alloys/Chips)
- GLOBAL DEFENCE DIPLOMACY & FINANCING (LoC)



- **Logical and Philosophical Base**

- **Kautilyan Realism (*Arthashastra*):** Classical Indian strategic thought posits that national sovereignty relies on the balance between **Kosa** (state treasury) and **Danda / Bala** (military power). Kautilya warned that relying on foreign powers for armaments undermines the king's capacity to protect the realm. Military strength without domestic production makes state sovereignty contingent on external goodwill.
- **Structural Realism (Waltzian and Mearsheimerian Framework):** In an anarchic international system with no supreme global authority, sovereign states must rely on *self-help* to ensure survival. Sourcing critical weapons from foreign powers creates profound strategic vulnerabilities—such as spare-part embargoes, ammunition denial, and political conditionalities during conflict. Indigenous defence production converts latent economic potential into hard, deployable security.
- **Strategic Autonomy as a Democratic Imperative:** True non-alignment is unsustainable when a country relies on external powers for over 60% of its basic military hardware. By manufacturing its own defence platforms, a nation secures the freedom to chart its foreign policy without fear of sudden supply cutoffs.
- **Constructivist Identity Transformation:** Supplying reliable military hardware shifts a country's international standing from a reactive, vulnerable consumer to a proactive, reliable security partner. Supplying coastal defence systems to smaller littoral nations builds enduring institutional, operational, and doctrinal partnerships.

- **Multidimensional Analysis**
- **Social Dimension**
 - **High-Skilled Employment and Human Capital:** The aerospace and defence ecosystem generates high-tech engineering, metallurgical, and software jobs, helping reverse brain drain and encouraging youth involvement in domestic STEM research.
 - **Regional Industrial Development:** Establishing defence corridors in non-metropolitan hubs (such as Bundelkhand in Uttar Pradesh and Coimbatore in Tamil Nadu) drives regional infrastructure improvements, technical training centers, and local auxiliary industries.
- **Political and Governance Dimension**
 - **Elimination of Intermediaries:** Promoting transparent domestic procurement procedures (via Buy-IDDMM channels) minimizes the historic influence of foreign arms brokers and opaque procurement scandals.
 - **Bipartisan Strategic Consensus:** Achieving self-reliance in national defence strengthens internal political stability and reinforces public confidence in sovereign deterrence.
- **Legal and Regulatory Dimension**
 - **Non-Proliferation Regime Alignment:** India's accession to the Missile Technology Control Regime (MTCR), the Wassenaar Arrangement, and the Australia Group provides legal clearance for exporting high-precision systems like BrahMos (with ranges calibrated under international guidelines).
 - **SCOMET Licensing Framework:** The Special Chemicals, Organisms, Materials, Equipment and Technologies (SCOMET) framework ensures that all military and dual-use exports comply strictly with international non-proliferation standards.
- **Ethical Dimension**
 - **Ethical Arms Exporter Paradigm:** India's defence exports emphasize deterrence and legitimate self-defence (aligned with Article 51 of the UN Charter), explicitly avoiding predatory sales to rogue states or non-state entities.
 - **Preserving Strategic Equilibrium:** Supplying coastal anti-ship systems to smaller nations promotes defensive deterrence against asymmetric bullying, supporting peaceful coexistence in international waters.
- **International and Geopolitical Dimension**
 - **Deterrence in the Indo-Pacific:** Equipping Southeast Asian countries with supersonic cruise missiles provides an asymmetric hedge against revisionist maritime claims, maintaining stability along vital sea lanes of communication (SLOCs).
 - **Diversified Security Partnerships:** From the South China Sea to the South Caucasus (e.g., supplying Pinaka rocket systems and Akash air-defence platforms to Armenia), defence exports build durable security ties without the ideological conditions often tied to Western or Chinese sales.
- **Economic Dimension**
 - **Capital Preservation and Forex Generation:** Replacing expensive foreign imports with domestic production saves valuable foreign exchange while generating significant export revenues.
 - **Economic Multiplier for MSMEs:** Defence platforms require intricate precision engineering. A single missile system integrates thousands of sub-components, driving sustained orders across machine-tool, precision-electronics, and advanced-metallurgy MSMEs.

Linkages with NCERT Textbooks		
Class & NCERT Textbook	Chapter Title & Theme	Conceptual Linkage to Defence Indigenisation
Class 12: Contemporary World Politics	Chapter: Security in the Contemporary World	Connects directly to traditional security concepts, balance of power, military deterrence, and national self-help in an anarchic global order.
Class 12: Contemporary World Politics	Chapter: Alternative Centres of Power	Explores India's emerging role as a regional economic and security anchor in the Indo-Pacific, strengthening institutional ties with ASEAN.
Class 12: Politics in India Since Independence	Chapter: India’s External Relations	Illustrates the evolution of Indian foreign policy from post-colonial non-alignment to pragmatic strategic autonomy and defence diplomacy.
Class 11: Indian Economic Development	Chapter: Economic Reforms Since 1991	Relevant for analyzing the transition from state-monopolized production to private-sector participation, FDI liberalization, and the Make in India initiative.
Class 10: Contemporary India - II	Chapter: Manufacturing Industries	Demonstrates how heavy manufacturing, specialized metallurgy, and engineering ecosystems provide the industrial base required for high-tech defence production.

- **Linkages with UPSC CSE Syllabus**

- **General Studies Paper II (GS-2)**

- *Bilateral, Regional, and Global Groupings and Agreements involving India:* Strategic implications of defence sales to ASEAN members, Quad partners, and regional players in West Asia and Central Asia.
- *Effect of Policies and Politics of Developed and Developing Countries on India's Interests:* Managing foreign sanctions frameworks (e.g., US CAATSA) while navigating defence joint ventures with international partners.
- *India's Act East Policy:* Using defence equipment supplies to reinforce ASEAN centrality and support a rule-based international maritime order.

- **General Studies Paper III (GS-3)**

- *Indigenisation of Technology and Developing New Technology:* The technical development of platforms like the BrahMos-NG, Tejas LCA, Akash air-defence system, and advanced artillery (ATAGS).
- *Science and Technology - Applications in Defence:* Supersonic propulsion, solid-fuel rocket motors, radar seekers, active electronically scanned arrays (AESA), and high-temperature metallurgy.
- *Security Challenges and Their Management:* Modernizing armed forces, managing two-front security challenges, and securing the Indian Ocean Region (IOR).
- *Indian Economy and Industrial Policy:* Evaluating the economic impact of Defence Industrial Corridors, private-sector defence manufacturing, and high-value export growth.

- **General Studies Paper IV (GS-4)**

- *International Ethics and Global Arms Trade:* The moral responsibilities of a rising power in exporting weapons—balancing commercial and strategic gains against regional stability and the prevention of human suffering.



- **Way Forward and Policy Recommendations**

- **Ramping Up Core R&D Expenditure:** India must increase domestic defence R&D spending from less than 1% of GDP to at least 2.5–3%. The Innovations for Defence Excellence (iDEX) initiative and the Technology Development Fund (TDF) need larger venture capital allocations to support deep-tech startups working on quantum encryption, autonomous drone swarms, hypersonic glide vehicles, and artificial intelligence.
- **Securing Critical Supply Chains and Upstream Metallurgy:** To prevent foreign supply disruptions during crises, India should build strategic domestic reserves and manufacturing capacity for raw military materials—such as aerospace-grade titanium alloys, carbon-fiber composites, specialized high-strength steel, and military-standard semiconductor chips.
- **Strengthening Lines of Credit and Defence Diplomacy:** The Ministry of External Affairs and Ministry of Defence should integrate defence export financing through the EXIM Bank. Expanding soft credit packages will allow developing countries in Africa, Latin America, and Southeast Asia to procure Indian platforms without balance-of-payments strain.
- **Modernizing Testing and Certification Infrastructure:** Private defence firms often struggle with limited access to state-owned military firing ranges and certification labs. Modernizing Directorate General of Quality Assurance (DGQA) procedures and granting private firms open, affordable access to DRDO testing ranges will significantly cut prototype-to-production timelines.
- **Sovereign Intellectual Property Protection:** Future joint ventures must prioritize complete intellectual property (IP) transfer, ensuring domestic control over source codes, guidance software, and core engineering blueprints. This prevents third-party nations from vetoing future export deals.

- **UPSC Civil Services Mains Examination**

- **GS Paper 3 (2023):** "The dynamic nature of external threats demands a robust domestic defence industrial ecosystem. Analyze the role of the 'Make in India' initiative in transforming India's defence capabilities from import-dependent to self-reliant."
- **GS Paper 3 (2019):** "How is the Government of India protecting the country from local and international cyber and military threats through indigenous initiatives? Discuss the significance of the Integrated Guided Missile Development Programme (IGMDP) in this context."
- **GS Paper 2 (2022):** "'India's Act East Policy is gaining a clear defence and security dimension.' In the light of this statement, analyze the strategic implications of India exporting advanced military hardware to ASEAN nations."
- **GS Paper 3 (2018):** "Defence acquisition procedures in India have often faced systemic delays. How do the newly introduced procurement reforms aim to streamline procurement and encourage private sector participation?"

- **Assam Public Service Commission (APSC) Relevant Questions**

- **APSC CCE Mains (GS 3):** "Discuss the strategic importance of the Atmanirbhar Bharat initiative in the defence sector. How can high-value defence exports elevate India's position as a net security provider in the Indian Ocean Region?"
- **APSC CCE Mains (GS 5 - Assam/Act East):** "Assam and the North-Eastern region serve as India's gateway to ASEAN. Explain how India's expanding economic and defence engagements under the Act East Policy contribute to the geopolitical stability of the wider region."



Countering extremism is the first condition of prosperity

The International Monetary Fund estimates that armed conflict cuts a country's growth by roughly two percentage points for every year it lasts, and that fragile states grow more slowly long after fighting stops.



RAJESH MEHTA

The human cost of terrorism is well understood. The quieter question is macro-economic: whether a state that keeps radicalisation at bay ends up richer and its people better off. It does, by margins wide enough to change how governments think about spending on peace.

Order is the ground on which prosperity is built. When organized extremism takes hold, it raises the cost of every everyday economic decision. The choice to invest, visit, hire, or build now comes with added risk due to the possibility of violence. This risk results in lost investment, fewer tourists,

and missed opportunities for growth year after year.

The International Monetary Fund estimates that armed conflict cuts a country's growth by roughly two percentage points for every year it lasts, and that fragile states grow more slowly long after fighting stops. The burden is regressive.

If extremism is a tax, look at countries of different faiths and systems that cleared out the violence and see what grew once it was gone.

The United Arab Emirates proscribed a violent extremist organisation in 2014, then built an architecture of tolerance: the Anti-Discrimination and Anti-Hatred Law in 2015, a Ministry of Tolerance in 2016, the Document on Human Fraternity in 2019, and normalisation with Israel through the Abraham Accords in 2020. By 2025, foreign investment had hit a record of some 48 billion dollars, non-oil activity roughly four-fifths of the economy, and the country

had become the world's leading destination for migrating millionaires.

Singapore is the cleanest comparator. After disrupting a plot to bomb foreign missions in 2001, it did not stop at detention. A rehabilitation programme returned most of those held to ordinary life, with only isolated reoffending, while mixed housing and the Maintenance of Religious Harmony Act reinforced social and religious harmony. Singapore now records among the highest incomes per person on earth and ranks among the most trusted places to hold capital. Neutralise the threat, repair the society that produced it, and confidence pays a long dividend.

The same lesson holds in Northern Ireland, where a conflict ran three decades and killed roughly 3,700 people until the ceasefires of 1994 and Good Friday Agreement of 1998. As killings fell, house prices rose fastest where violence had been worst. Overseas

visitors roughly doubled to about three million, and financial-sector employment grew around 36% between 1998 and 2022, the strongest of any UK region.

The opposite is clear. Pakistan's government put the cumulative economic cost of terrorism at around 127 billion dollars between 2001 and 2018. In Sri Lanka, coordinated bombings killed more than 250 people in one morning in 2019; arrivals fell by more than 70% the following month, with tourism supplying close to a sixth of foreign-exchange earnings. One attack priced itself into the national accounts within weeks. Where extremism captures the state, as in Afghanistan after 2021, output collapses, falling about a quarter as poverty climbed toward three in four.

For India, the lesson is close to home, and must always separate violent actors from communities they must never be conflated with. The Kashmir Valley's economy, on the best

available estimate, would be more than half as large again without the long insurgency.

The sharpest evidence is recent. Valley tourism reached a record in 2024, then collapsed in 2025 after the April attack at Pahalgam, in which 26 people, most tourists, were killed: arrivals fell to roughly a third of the previous year's total. It is proof that a single attack can undo years of patient gains.

India is betting its next phase of growth on connectivity that only pays off in a calm neighbourhood: the India-Middle East-Europe Economic Corridor and I2U2 grouping to its west, and the International North-South Transport Corridor and Chabahar port running through Iran towards Central Asia and Russia. Every route assumes regional stability, making countering extremism a precondition for growth India is planning, not merely a shield for what it has built.

The pattern is consistent enough to state as principle. Extremism is a tax, and some countries have decided to stop paying it. Removing organised violence does not guarantee prosperity. It lifts the ceiling and opens the room, turning a country from a place outsiders price for risk into one they price for opportunity. Tolerance and coexistence persuade the investor, visitor and skilled family that peace will hold.

One qualification remains: poverty and grievance can themselves feed extremism, so the arrow runs both ways, and no serious analysis would claim proven causation. But the natural experiments, prices and arrivals moving as violence begins and ends, run substantially from violence to loss. That is why the price of hate, like the dividend of peace, shows up on every balance sheet.

** Rajesh Mehta is an international affairs expert working on innovation and public policy.*

• Key Terms and Explanations

- **The Peace Dividend:** The tangible economic benefit accrued when a society transitions away from conflict or internal instability. By reducing spending on state defense and internal policing, resources are reallocated toward productive capital investments like infrastructure, education, and healthcare, while reducing the baseline risk premium for foreign and domestic investors.
- **The Regressive Tax of Extremism:** The implicit cost imposed by violence on an economy. It acts regressively because low-income households and micro-enterprises bear the brunt of localized disruptions, sudden curfews, inflation, and capital flight, lacking the liquidity or geographic mobility that wealthier entities possess to hedge against instability.
- **Fragile States and the Conflict Trap:** A systemic loop identified in development economics where institutional weakness permits radicalization and violent insurrection, which in turn destroys physical infrastructure, fractures societal trust, and shrinks fiscal revenue. The resulting underdevelopment entrenches further instability.
- **Architecture of Tolerance:** A proactive policy doctrine that treats social harmony as foundational state infrastructure rather than a passive cultural aspiration. It combines institutional, legal, and educational mechanisms—such as anti-discrimination statutes, mixed public housing, interfaith dialogue frameworks, and deradicalization programs—to dismantle communal fissures before they turn violent.
- **Sovereign Risk Premium:** The extra yield or return demanded by international investors to compensate for the political, legal, and physical risks of deploying capital in a specific jurisdiction. Sustained social instability increases this premium, suppressing capital inflows and raising sovereign borrowing costs.
- **Geo-Economic Connectivity Corridors (e.g., IMEC, INSTC, I2U2):** Multi-modal trade and transit networks designed to integrate disparate regional economies. Their viability rests entirely on guaranteed transit stability; a single node compromised by regional or domestic extremism degrades the utility of the entire trade corridor.



- **Main Arguments and Conceptual Foundations**
- The relationship between internal stability and economic output rests on four core pillars:
 - **Security is a Macroeconomic Precondition:** Growth cannot be sustained through monetary or fiscal stimuli alone if baseline public safety and predictability are absent. Violence elevates transaction costs, inflates supply-chain friction, and forces economic agents into defensive asset allocation.
 - **The Long Hysteresis of Conflict:** Conflict inflicts damage that outlasts active violence. The International Monetary Fund (IMF) projects that armed conflict subtracts roughly two percentage points from annual GDP growth, leaving post-conflict zones to grow at structurally depressed rates due to broken institutional trust and destroyed human capital.
 - **Evidence from International Transitions:**
 - *United Arab Emirates:* Codified legal penalties against hate speech and discrimination, alongside institutional normalization, transforming the country into a top destination for foreign direct investment and global talent migration.
 - *Singapore:* Integrated early detention with community-based rehabilitation, ethnic integration quotas in public housing, and legal mandates on religious harmony, yielding sustained trust ratings and high per capita income.
 - *Northern Ireland:* The 1998 Good Friday Agreement precipitated an immediate rebound in real estate value across previously high-violence zones, a doubling of overseas visitors, and above-average financial services job growth.
 - **The Cost of Radical Capture and Destabilization:**
 - *Pakistan:* Suffered over \$120 billion in direct and indirect losses from sustained terrorism, deterring long-term foreign investment and straining state finances.
 - *Sri Lanka:* The 2019 Easter Sunday bombings showed how a single day of coordinated violence can immediately compress tourist arrivals by more than 70%, destabilizing foreign exchange reserves.
 - *Afghanistan:* Post-2021 institutional capture by hardline elements triggered an immediate one-quarter contraction in GDP and deep poverty.
 - **Asymmetric Vulnerability in Regional Development:** Localized violence yields non-linear economic shocks. A single security breach in vulnerable economic sectors—such as hospitality or seasonal tourism—can erase years of accumulated investor confidence and employment gains.
 - **The Geopolitical Corridors Argument:** Contemporary mega-projects (such as the India-Middle East-Europe Economic Corridor or the International North-South Transport Corridor) depend on regional stability. Countering domestic and neighborhood radicalization is not merely an internal defense mandate, but an offensive economic strategy necessary to unlock cross-border trade dividends.

- **Historical Evolution of the Issue**

- The modern understanding of social stability as an economic engine has evolved across distinct historical phases:
 - **Pre-Independence Era (Colonial Divides and Economic Fragmentation):** Colonial powers frequently relied on communal partitioning and identity-based divisions to sustain administrative control. This fractured domestic market integration, diverted native revenue to imperial defense budgets, and stifled the emergence of an integrated national economic space.
 - **Post-Colonial and Cold War Era (Kinetic Counter-Insurgency):** Developing post-colonial nations treated insurgencies and extremism primarily as kinetic law-and-order challenges. State responses relied on militarized suppression, often overlooking how economic marginalization, sub-regional neglect, and communal friction fed ongoing insurgent recruitment.
 - **Post-9/11 Era (Securitization of Capital and Global Anti-Terror Frameworks):** The Financial Action Task Force (FATF) and the United Nations Security Council (UNSC Resolutions 1267 and 1373) formalized the financial cost of harboring or failing to control extremist elements. Jurisdictions facing grey-listing or black-listing saw automated drops in foreign credit lines, heightened borrowing costs, and severe trade friction.
 - **The 2010s (Shift Toward Soft Deradicalization and Institutional Harmony):** Governments shifted from purely punitive counter-terrorism toward deradicalization, economic rehabilitation, and codified tolerance policies. Case studies across Southeast Asia and the Middle East showed that legal enforcement against incitement paired with social safety nets yielded immediate stability dividends.
 - **Present Day (Geo-Economic Corridors and Connectivity Imperatives):** As nations pivot toward transcontinental transit networks and regional value chains, localized instability threatens cross-border infrastructure. Ensuring social cohesion is now viewed as an essential driver of sovereign competitiveness.

THE MACROECONOMIC POWER OF TOLERANCE & ORDER: UNLOCKING INDIA'S PEACE DIVIDEND

Peace is a precondition. Tolerance and coexistence persuade investors. Tolerance lifts the ceiling.

EXTREMISM: THE REGRESSIVE TAX ON GROWTH

Human & Economic Cost

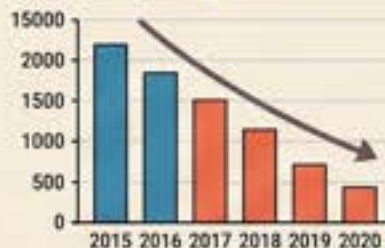


Armed conflict cuts growth by ~2% annually (IMF)



Destroyed chokes infrastrugrowth flow

Fragile states grow slowly long after



Pakistan
cumulative cost
\$127B



Sri Lanka
70% tourist drop
after bombings



Afghanistan
output collapsed
-25%

Kashmir



Economy could be 1.5x larger



Tourism halved after Pahalgam attack

ORDER

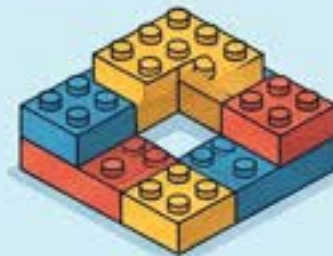
TRUST

PROSPERITY



Peace is a precondition.
Tolerance and coexistence persuade investors.
Tolerance lifts the ceiling.

Architectures of Tolerance



Record \$48B FDI (UAE)



World's leading destination for migrating millionaires (UAE)



House prices rose fastest (N. Ireland example)



Financial sector grew 36% (N. Ireland example)

INDIA'S VISION & GEOPOLITICS



Countering extremism is a PRECONDITION for planned growth, not just a shield.

- **Logical and Philosophical Foundations**

- **Hobbesian Social Contract Theory:** Thomas Hobbes observed in *Leviathan* that without an overarching civil authority ensuring collective security, there is "no place for industry, because the fruit thereof is uncertain: and consequently no culture of the earth, no navigation, nor use of the commodities." Economic activity requires a credible state guarantee of physical safety and the rule of law.
- **New Institutional Economics (Douglass North and Daron Acemoglu):** Economic development relies on formal and informal institutions that lower transaction costs and protect property rights. Extremism corrupts these institutions by introducing uncertainty, eroding contract enforcement, and replacing legal predictability with coercion.
- **The Capability Approach (Amartya Sen):** Development is the expansion of fundamental human freedoms rather than mere GDP growth. Violent extremism directly attacks core capabilities: the freedom to move safely, engage in commerce, acquire education, and live without fear. Depriving populations of these basic capabilities damages long-term human capital formation.
- **Rawlsian Pluralism and Overlapping Consensus (John Rawls):** In diverse societies, enduring stability cannot rest on the dominance of one group over another. It requires an overlapping consensus where varied cultural and religious traditions commit to shared, fair terms of social cooperation under a neutral constitutional order.

Multidimensional Analysis	
Dimension	Key Dynamics & Analytical Insights
Social	• Erosion of Social Capital: Communal radicalization destroys horizontal trust among citizens, replacing civic cooperation with insular, identity-based enclaves. • Ghettoization & Spatial Polarization: Fear forces communities into segregated living spaces, segmenting labor markets and limiting youth access to diverse economic networks.
Political	• Governance Bandwidth Crowding: Internal security emergencies divert administrative resources away from core social welfare, educational reform, and infrastructure modernization. • Erosion of Democratic Resilience: Sustained internal threats often lead to exceptional security laws, risking civil liberties and weakening democratic accountability.
Legal	• Codified Protections vs. Due Process: States face the challenge of designing effective anti-hate speech and counter-extremism laws without undermining constitutional free speech and due process. • Institutionalizing Harmony: Transitioning from ad-hoc administrative measures to clear, statute-backed frameworks (e.g., Singapore's Maintenance of Religious Harmony Act) ensures predictable enforcement.
Ethical	• The Imperative of Human Security: Ethical governance prioritizes human security—protecting individual lives, dignity, and livelihoods—over purely state-centric defense. • Non-Conflation of Communities: A critical ethical and operational duty of the state is ensuring violent actors are never conflated with the broader religious or ethnic communities they claim to represent.
International	• Sovereign Investability & Multilateral Scrutiny: Cross-border capital tracks compliance with international norms; structural failure to combat radical groups triggers FATF gray-listing and drops in sovereign credit ratings. • Vulnerability of Strategic Corridors: Multi-country connectivity platforms (such as INSTC and IMEC) rely on uninterrupted stability across every transit state to function.

- **Linkages with NCERT Textbooks**
 - **Class 11 Political Science: *Political Theory***
 - *Chapter 8 (Secularism)*: Explores the Western versus Indian models of secularism, showing how state neutrality and principled distance from religious factions safeguard inter-community trust and civil peace.
 - *Chapter 9 (Peace)*: Analyzes structural violence versus direct violence, reinforcing how sustainable economic development depends on durable, positive peace.
 - *Chapter 10 (Development)*: Discusses the social and human costs of unbalanced development, illustrating how structural marginalization can spawn local conflict.
 - **Class 12 Political Science: *Contemporary World Politics***

 - *Chapter 3 (Security in the Contemporary World)*: Distinguishes traditional military threats from non-traditional security challenges (terrorism, human rights abuses, poverty), highlighting why national defense requires human security.
 - **Class 12 Political Science: *Politics in India since Independence***
 - *Chapter 8 (Regional Aspirations)*: Details the historical trajectory of regional and identity-based movements in Punjab, the North-East, and Jammu & Kashmir, demonstrating how political accommodation and economic integration rebuild security.
 - **Class 12 Sociology: *Social Change and Development in India***
 - *Chapter 6 (Cultural Diversity and Challenges to Nation-Building)*: Examines communalism, regionalism, and casteism, outlining how social integration policies counter radical identity mobilization.
 - **Class 11 Economics: *Indian Economic Development***
 - *Chapter 5 (Human Capital Formation in India)*: Analyzes the critical inputs of education and health, showing how localized instability damages human capital accumulation and lowers long-term productivity.

- **Linkages with the UPSC CSE Syllabus**

- **General Studies Paper 1:**

- *Salient features of Indian Society, Diversity of India:* The preservation of composite culture and structural resilience against identity-based polarization.
- *Social Empowerment, Communalism, Regionalism & Secularism:* The socio-economic impacts of communal tensions and the marginalization of vulnerable groups.

- **General Studies Paper 2:**

- *Government Policies and Interventions:* Formulating evidence-based interventions for social cohesion, deradicalization, and human rights protections.
- *Role of Civil Services in a Democracy:* Administrative neutrality, community policing initiatives, and maintaining law and order during communal tension.
- *Bilateral, Regional, and Global Groupings (I2U2, INSTC, IMEC):* Strategic trade corridors and how domestic and cross-border security underwrite multilateral economic diplomacy.

- **General Studies Paper 3:**

- *Linkages between Development and Spread of Extremism:* Assessing how economic exclusion, unemployment, and regional disparities fuel radicalization, and vice versa.
- *Role of External State and Non-State Actors:* Cross-border support for domestic extremist elements and its direct impact on national output.
- *Indian Economy (Capital Investment, Infrastructure, and Employment):* How reducing the internal risk premium accelerates private capital formation, foreign direct investment, and job creation.

- **General Studies Paper 4 (Ethics, Integrity, and Aptitude):**

- *Public/Civil Service Values and Ethics in Public Administration:* Ethical imperatives of equity, absolute administrative impartiality, and non-discrimination.
- *Foundational Values for Civil Service:* Empathy, tolerance, and compassion toward weaker sections during internal security operations.



- **Way Forward**

- **Transition to an Institutional Architecture of Tolerance:**

- Move beyond reactive law enforcement by enacting comprehensive anti-discrimination legislation that penalizes hate speech, economic boycott incitement, and targeted communal intimidation.
- Establish institutional bodies dedicated to monitoring social cohesion metrics, evaluating community tensions early, and facilitating inter-faith and inter-community dialogues.

- **Adopt Evidence-Based Deradicalization and Community Rehabilitation:**

- Emulate proven rehabilitation frameworks (such as the Singapore model) that combine psychological counseling, ideological mentorship by respected community leaders, and economic reskilling.
- Scale community-oriented policing models to rebuild trust between law enforcement agencies and historically marginalized or vulnerable populations.

- **Targeted Economic Regeneration in Vulnerable Geographies:**

- Deploy targeted fiscal incentives, credit guarantee programs, and industrial corridors into post-conflict or historically volatile regions to generate youth employment.
- Build localized infrastructure resilience—specifically around vulnerable sectors like tourism, craftsmanship, and seasonal agriculture—to insulate local livelihoods from temporary security disruptions.

- **Secure National and Regional Geo-Economic Connectivity:**

- Incorporate dedicated physical and cyber security protocols into regional connectivity platforms (such as IMEC, INSTC, and domestic freight corridors) to assure institutional investors of long-term operational continuity.
- Deepen multilateral intelligence-sharing networks and financial tracking systems under the FATF umbrella to sever illicit funding lines to non-state actors.

- **Rebalance Fiscal Priorities for Long-Term Growth:**

- Systematically transition state spending from reactive internal containment and kinetic security apparatuses toward capital-forming social infrastructure: digital education, vocational academies, and modern healthcare.
- Direct the resulting peace dividend toward expanding the productive capacity of the national economy.



- **UPSC Civil Services Mains Examination**

- **2023 (GS Paper 3):** Winning the hearts and minds of the people in insurgency-affected areas is an essential step in restoring peace and order. Discuss the measures taken by the government in this direction.
- **2021 (GS Paper 3):** Analyze the multidimensional challenges posed by external state and non-state actors to the internal security of India. Also, discuss the measures required to counter these threats.
- **2020 (GS Paper 3):** For long-term economic development, internal stability and social harmony are non-negotiable prerequisites. Critically evaluate how ethnic conflicts and violent insurgencies disrupt regional economic trajectories in India.
- **2019 (GS Paper 2):** "The long-term success of connectivity corridors such as INSTC and IMEC depends as much on regional geopolitical stability as on capital investment." Examine.
- **2018 (GS Paper 3):** Left-Wing Extremism (LWE) is showing a downward trend, but still affects many parts of the country. Briefly explain the Government of India's approach to counter the LWE challenge.
- **2017 (GS Paper 1):** Distinguish between religiousness/religiosity and communalism, giving one example of how the former transforms into the latter in independent India.
- **2015 (GS Paper 4):** "A state that fails to protect tolerance and pluralism cannot hope to sustain high economic growth or ethical public administration." Comment.

- **State Public Service Commission (APSC / State PSC) Questions**

- **APSC CCE Mains (GS Paper 3):** The North-Eastern region of India has witnessed a significant decline in insurgent violence over the past decade, opening avenues for trade under the Act East Policy. Discuss the economic benefits of this peace dividend for Assam and the neighboring states.
- **APSC CCE Mains (GS Paper 2):** Social harmony and inter-ethnic peace are the foundational pillars for industrialization and foreign investment in border states. Analyze this statement in the context of Assam's developmental trajectory.

The right to hack: How states are rewriting cyber defence

As foreign states go on mobilizing private technology firms and intelligence hybrids to neutralize external threats in real time, India faces a strategic question.

OPINION

BRIJESH SINGH



Picture the moment first: state-backed hackers slip into a country's grid and the lights start to fail, or they slip into its hospitals and the machines start to falter, or they simply sit on its industrial data, hostage now, waiting on a ransom—and every citizen watching this feels the same reflex rise in it, unbidden, the oldest reflex there is, which is simply to hit back. And yet the record runs the other way, has run the other way for decades: democratic legal traditions built themselves around outlawing exactly that re-

flex, treating unauthorized intrusion into a computer system as a felony, and reserving the violence that states are permitted solely for the militaries and the police that answer to them. That old boundary, drawn after the Cold War and held for a generation, is not being debated away now; it is dissolving, quietly, almost without anyone marking the moment. Nobody is standing up in public arguing that corporations deserve some new statutory "right to hack back." What is happening instead is quieter, and more consequential—major powers reinterpreting statutes that are half a century old, issuing executive orders that fold private technology firms into state-sanctioned digital warfare.

The legal acrobatics that make this pivot possible are worth sitting with, because they show just how unready a body of peacetime doctrine

is for a war fought in wires and packets rather than in trenches. In the United States, one legislative attempt followed another—the Active Cyber Defense Certainty Act chief among them—and each one died in Congress, killed every time by the same bipartisan fear: that letting corporations act as vigilantes online would tip, sooner or later, into something like international armed escalation. So, rather than wait on a consensus that wasn't arriving, the executive branch bypassed Capitol Hill entirely, leaning on an obscure, 40-year-old provision buried in the Computer Fraud and Abuse Act, a clause written for law-enforcement investigations; federal directives now quietly recruit vetted private contractors to carry out offensive cyber surveillance and disruptive-effects operations against foreign criminal syndicates, all of it kept, at least on paper, under federal oversight.

Strip away the modern vocabulary and what this mechanism resurrects is something much older, 18th-century privateering, ported wholesale into the digital realm. To manage the moral hazard that comes with letting corporations wage something like war-

fare, Washington has bolted on a set of commercial safeguards: participating firms are required to post million-dollar indemnity bonds, required to secure written operational sign-off before they act, and in exchange the state gets to outsource the friction, the risk, the messiness of offensive operations to private hands, while trying to keep its own diplomatic fingerprints off the outcome. But underneath the paperwork the legal foundation is exceptionally brittle; no appellate court has ever tested whether a carve-out written for ordinary law enforcement permits a private contractor to knock a foreign server offline, and the first cross-border misattribution, the first inadvertent scrap of collateral damage, will be the thing that finally drags it all into protracted litigation and foreign-policy fallout.

Across the Pacific, though, it is Japan that has undertaken the more historic shift of the two, and by some distance. For decades Tokyo was bound, tightly and without exception, by the strictly pacifist constraints written into Article 9 of its postwar Constitution—and now, against that backdrop, it has enacted the Cyber Response Capability Enhancement Act, formally authoriz-

ing civilian authorities and the police to infiltrate adversary command-and-control infrastructure abroad and neutralize it before any attack ever has the chance to fully unfold. To survive the domestic constitutional scrutiny owed to the absolute secrecy of communications, a right taken seriously in Japanese law, the drafters reached for a delicate technical fiction: state monitoring, they wrote, is strictly confined to routing metadata alone, things like IP addresses and command strings, leaving the actual content of any message untouched, sealed off, out of reach.

Except that fiction is ageing badly, and ageing faster than its drafters could ever have planned for. In a modern digital network, where machine-learning classifiers can derive full operational intent directly from nothing more than a communication pattern, the old distinction between metadata and content is collapsing, rapidly, underneath the statute's feet. Japan's attempt to build a statutory, civilian-led active-defence architecture remains genuinely unprecedented, and yet its operational viability keeps running into practical bottlenecks: Tokyo has legislated ambitious pre-emption

mandates on paper, but its national cybersecurity apparatus confronts an acute deficit of the specialized personnel needed to carry them out, exposing, plainly, a persistent and uncomfortable gulf between statutory ambition and actual state capacity.

European capitals, meanwhile, are fracturing along fault lines that contradict one another outright, each government drawing the boundary in its own place. In Germany, proposed legal revisions would empower civilian police bodies and interior-ministry agencies to strike foreign infrastructure directly, and pointedly exclude both foreign intelligence services and the military from that same authority—a choice that reads, on its face, as a deliberate act of institutional narrowing. France sits in stark contrast to all of this, maintaining a rigid institutional wall between the two functions, a wall it has held to for years: the civilian cybersecurity agency stays purely defensive, guarding its own trust with industry above all else, while offensive cyber counter-strikes are assigned, strictly and without exception, to military commands operating under the constraints of international

humanitarian law.

At the international level, multilateral consensus has stalled entirely, and shows no real sign of resuming. The United Nations' Open-Ended Working Group has tried, repeatedly, and repeatedly failed, to reach any agreed threshold for what level of digital disruption should count as an unlawful use of force under the UN Charter—a question that sounds technical and is, underneath, almost civilizational. In the absence of binding international treaties, states are left to unilaterally improvise their own thresholds, each on its own terms, and what has emerged instead of formal law is something quieter, a tenuous norm built through operational habit rather than through any treaty: national frameworks increasingly restrict authorized retaliation to the neutralization of intermediary infrastructure alone—a hijacked relay server, say, rather than the server farm behind it—rather than mounting destructive counter-strikes against a sovereign state's own networks.

For India, watching all three of these stories unfold at once—across North America, across Europe, across East Asia—the im-

plications land as genuinely urgent. New Delhi has built real, robust institutional defences: the Indian Computer Emergency Response Team on one side, a set of dedicated critical-infrastructure protection agencies on the other. And yet the Information Technology Act remains anchored to a framework that is reactive, compliance-heavy, built for reporting incidents after the fact rather than meeting them as they happen. As foreign states go on mobilizing private technology firms and intelligence hybrids to neutralize external threats in real time, India is left facing a strategic question: whether to keep relying on passive perimeter defence and post-incident reporting, or whether to construct a rigorous, constitutionally bounded active-defence framework of its own. What the global shift proves, if nothing else, is this—active cyber defence is no longer some theoretical debate; it is an operational reality, being forged right now, without international rules to hold any of it in place.

** Brijesh Singh is a senior IPS officer and an author (@brijesh-singh on X). His latest book on ancient India, "The Cloud Chariot" (Penguin) is out on stands. Views are personal.*

- **Key Terms and Conceptual Framework**

- **Active Cyber Defence (ACD) / "Hack-Back":** A proactive security posture where defenders do not merely absorb attacks behind a firewall, but actively trace, access, disrupt, or neutralize adversary digital infrastructure (such as command-and-control servers) outside their own networks before an attack culminates.
- **Digital Privateering (Letters of Marque in Cyberspace):** The sovereign practice of licensing, deputizing, or indemnifying private commercial tech firms to carry out state-sanctioned offensive or disruptive cyber operations against foreign adversaries, echoing 18th-century maritime warfare.
- **Command-and-Control (C2) Infrastructure:** A network of centralized servers, computers, or automated nodes used by threat actors to maintain communication with, manage, and deliver malicious payloads to compromised systems (botnets) inside target organizations.
- **Intermediary Infrastructure (Hop Nodes / Relay Servers):** Innocent, third-party commercial servers located in neutral jurisdictions that are hijacked by adversaries to route malicious traffic, thereby masking the true geographic and political origin of an intrusion.
- **The Metadata versus Content Legal Fiction:** A statutory distinction in wiretapping and communications law assuming that packet routing data (IP addresses, port numbers, packet sizes) can be inspected without violating the constitutional sanctity of the communication's actual substance. In machine-learning-driven environments, behavioral pattern analysis on metadata reconstructs operational intent just as invasively as reading plaintext content.
- **Use of Force in Cyberspace (Article 2(4) vs. Article 51, UN Charter):** The unresolved international threshold determining whether a non-kinetic digital disruption (e.g., shutting down an electric grid or corrupting healthcare databases) amounts to an "armed attack" justifying physical or digital self-defense under international humanitarian law.
- **Statutory Asymmetry (Passive Reporting vs. Active Pre-emption):** The structural mismatch between compliance-centric digital legislation (such as India's IT Act, 2000, which mandates reporting breaches after they occur) and the operational reality of automated, microsecond-level offensive strikes by state actors.

- **Main Arguments and Conceptual Foundations**

- **The Dissolution of the Peacetime Boundary:** For decades, democratic jurisprudence strictly criminalized unauthorized digital intrusion for non-state actors while reserving coercive violence exclusively for the sovereign military and police. This norm is disintegrating as states discover that perimeter firewalls cannot withstand persistent, state-sponsored cyber sabotage against civilian infrastructure like hospitals, power grids, and financial exchanges.
- **The Resort to Legal Acrobatics and Executive Bypasses:** Rather than crafting transparent statutory frameworks—which repeatedly stall due to domestic civil-liberties concerns—executives stretch legacy statutes. The United States repurposes law-enforcement carve-outs in the Computer Fraud and Abuse Act (CFAA) to license corporate contractors, balancing the resulting moral hazard with indemnity bonds and written mission sign-offs.
- **The Collapse of the Constitutional Metadata Shield:** Japan's bold statutory shift under the *Cyber Response Capability Enhancement Act* seeks to neutralize adversary C2 abroad while navigating Article 9's pacifism and Article 21's absolute protection of communication secrecy. However, the legal justification that authorities are "only tracking routing metadata" collapses when modern neural networks decode operational content directly from traffic metadata signatures.
- **Divergent Institutional Architectures Across Democracies:**
 - *The Civilian-Police Strike Model (Germany):* Directs offensive authorities to interior-ministry agencies and civilian police, pointedly excluding military and intelligence entities to protect post-war domestic oversight.
 - *The Rigid Institutional Wall (France):* Maintains strict institutional bifurcation—the civilian agency (ANSSI) remains purely defensive to preserve industrial trust, while offensive cyber operations remain under the military command (COMCYBER) bound by international humanitarian law.
 - *The Hybrid Outsourcing Model (United States):* Relies on vetted, commercial threat-intelligence firms operating under executive oversight to launch counter-surveillance and disruptive strikes against foreign servers.
- **Multilateral Paralysis and Norm Improvization:** The United Nations Open-Ended Working Group (UN OEWG) remains deadlocked on defining thresholds for cyber warfare. Consequently, states have unilaterally adopted a customary norm: confining authorized active defense to neutralizing compromised *intermediary infrastructure* rather than launching full counter-value strikes against the adversary state's root servers.

- **Historical Evolution of Sovereign Cyber Doctrines**

- **18th to 19th Century (The Classical Maritime Analogue):** Sovereign states routinely issued *Letters of Marque and Reprisal*, authorizing private vessel owners (privateers) to attack foreign commerce. The 1856 Declaration of Paris abolished privateering in maritime law, establishing the foundational principle that offensive cross-border coercion must remain an exclusive state monopoly.
- **1980s to Late 1990s (The Dawn of Statutory Peacetime Guardrails):** Early computerized systems prompted laws like the US Computer Fraud and Abuse Act (1986) and later India's Information Technology Act (2000). Cyberspace was treated as a civilian-commercial domain where *any* unauthorized access was classified as a felony, embedding an absolute defense-only baseline.
- **2000 to 2010 (The Rise of State-Sponsored Operations):** Events such as the 2007 cyber-attacks on Estonia and the 2010 discovery of the *Stuxnet* worm shattered the assumption that cyber threats were merely the work of isolated cybercriminals. The militarization of cyberspace began, yet democratic policy remained locked in passive defense, institutional firewalls, and reactive forensics.
- **2010 to 2020 (The Expansion of Gray-Zone Hybrid Warfare):** The weaponization of ransomware (NotPetya, WannaCry) and intrusions into power grids demonstrated that adversaries operated through criminal cutouts in the "gray zone" between war and peace. Debates over "hacking back" emerged in legislatures (such as the US Active Cyber Defense Certainty Act), but repeatedly failed over fears of vigilante-induced military escalation.
- **2020s to Present (The Shift to Institutionalized Active Defense):** Confronted by systemic threats to critical infrastructure, democratic states have moved toward pre-emptive disruption. Japan enacted the *Cyber Response Capability Enhancement Act*, European nations restructured their cyber agencies, and intelligence communities formalized partnerships with private cybersecurity giants.



AXIA IAS ACADEMY
RISE ABOVE THE REST

INDIA'S STRATEGIC CYBER QUESTION: BEYOND PASSIVE DEFENCE – UPSC CSE ANALYTICAL INFOGRAPHIC

KEY CONCEPTS IN ACTIVE CYBER DEFENCE



Active Cyber Defence (ACD)
Reactive to Proactive.
External Threat Neutralization.



Digital Privateering
Private Technology Firms
& Intelligence Hybrids:
Porting to Digital Realm.



Command-and-Control (C2) Infrastructure
Neutralizing before
attack fully unfolds.



Metadata Fiction
Old Distinction vs ML Classifiers.
derive full operational intent
directly from communication
pattern.

MAIN ARGUMENTS: RISING REFLEX VS DISSOLVING BOUNDARY



STATE-BACKED HACKERS INFILTRATION



CRITICAL SYSTEMS FAILURE
(Hospital, Grid)



CITIZEN'S HIT BACK REFLEX



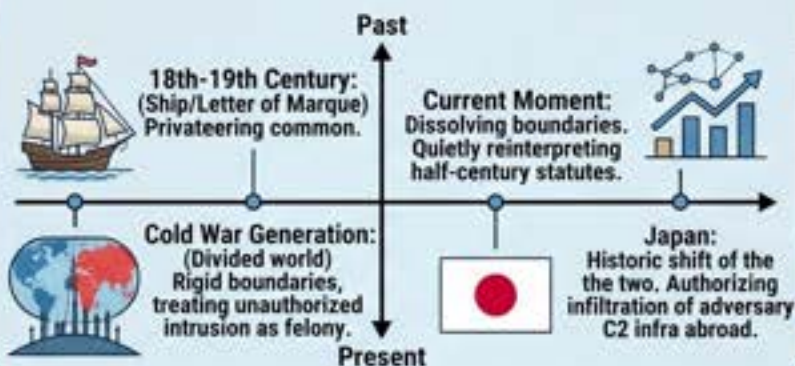
OLD BOUNDARY:
reserved violence
solely for states
& militaries.

OLD BOUNDARY:
reserved violence
solely for states &
militaries.



MAJOR POWERS REINTERPRETING STATUTES:
fold private technology
firms into state-sanctioned
warfare.

HISTORICAL EVOLUTION: A NEW ERA OF PRIVATEERING



LOGICAL & PHILOSOPHICAL BASE: CONFLICT IN WIRE AND PACKET



MULTIDIMENSIONAL ANALYSIS OF ACTIVE CYBER DEFENCE



Social
Data ransom icon,
hostage data



Political
Executive Orders fold
private firms into warfare



Legal
Reinterpreting Statutes,
untested carve-out



Ethical
Moral Hazard,
privatization of warfare



International
Multilateral Consensus
stalled, no agreed
threshold for use of force



Economic
Participating firms
million-dollar
indemnity bonds

LINKAGES FOR UPSC CSE ASPIRANTS



NCERTs:
Politics of
Global Security



GS Paper 3:
Security,
Science & Tech



GS Paper 2
Governance



GS Paper 4
Ethics



Optional Subjects:
PSIR/Law

WAY FORWARD FOR INDIA

**Transition Passive
Perimeter Defense
& Post-Incident
Reporting**

**Construct a rigorous,
constitutionally
active-defence
framework**

- Active cyber defence is no longer some theoretical debate; it is an operational Combine CERT-In & critical infrastructure agencies
- Establish international rules to hold things in place

PYQs (Previous Years' Questions)

- Sample relevant UPSC Mains questions without answers in not use cyber unnotoriety creeloss.
- What is the state cyber smotions tot pregnative summon: Active cyber defence imminent is no longer ouraire theoretical debate; it is an operational reality?
- Combine Internet & cront-infrastructure agency. Establish PISC Mains oreans rules without answers.



axiaiasacademy.com



+91 6002-417488

- **Logical and Philosophical Base**

- **Hobbesian Realism in the Digital Commons:** The international cyber domain mirrors a classic Hobbesian state of nature: an anarchic space lacking an overarching sovereign enforcer. In the absence of enforceable international treaties, states inevitably embrace offensive and pre-emptive self-help measures to ensure survival and deterrence.
 - **The Erosion of the Weberian State Monopoly:** Max Weber defined the state as the human community that successfully claims the *monopoly of the legitimate use of physical force*. Delegating active defense to private corporations fractures this monopoly, introducing profit-driven motives, corporate indemnities, and outsourced sovereign violence.
 - **The Cyber Deterrence Paradox:** In kinetic warfare, deterrence rests on visible retaliatory power. In cyberspace, demonstrating offensive capabilities burns operational zero-day vulnerabilities, while passive defense suffers an acute structural imbalance: the defender must secure every vulnerability, whereas the attacker needs to exploit only one.
 - **Just War Theory (*Jus ad Bellum* and *Jus in Bello*):** Active counter-strikes challenge classic ethical principles:
 - *Attribution and Distinction:* Inability to confirm the true perpetrator behind hijacked intermediary nodes makes discriminating between adversary infrastructure and neutral civilian systems nearly impossible.
 - *Proportionality:* Disrupting foreign routing infrastructure to stop an impending breach can cascade unpredictably into municipal civilian utilities.
- 
- 
- 
- 

Multidimensional Analysis		
Dimension	Key Structural Dynamics	Critical Strategic Vulnerabilities
Social	• Threat of cascading disruptions to civilian services (hospitals, water supplies, urban transport). • Normalization of broad domestic network surveillance under the banner of national security.	• Erosion of public trust in digital infrastructure and state-mandated digital public goods (e.g., UPI, health registries). • Chilling effect on civic digital communications and democratic dissent.
Political	• Shift of war-making powers from open parliamentary debate to closed executive councils. • Inter-agency turf battles among civilian police, intelligence services, and military commands.	• Diminished democratic accountability and parliamentary scrutiny over cross-border digital operations. • Risk of private tech corporate executives steering sovereign foreign policy decisions.
Legal	• Stretching decades-old criminal and cyber statutes to justify state-sponsored offensive intrusions. • Severe friction with constitutional privacy protections (e.g., Article 21 in India, Article 21 in Japan).	• Fragile legal foundation that remains untested in appellate and constitutional courts. • Absence of domestic statutory frameworks regulating active defense and collateral indemnities.
Ethical	• Moral hazard of corporate privateering where private vendors profit from persistent offensive states. • Unintended disruption of civilian intermediary networks in neutral sovereign third-party nations.	• Undermining the moral legitimacy of democratic states in championing a free, open, and secure internet. • Absence of ethical liability for automated algorithmic collateral damage.
International	• Complete deadlock in multilateral norm-setting bodies such as the UN OEWG and UN GGE. • Unilateral improvisation of thresholds regarding what constitutes an unlawful use of force.	• Risk of rapid, unintended escalation from cross-border misattribution into kinetic armed conflict. • Fragmentation of the global internet (Splinternet) along geopolitical security lines.



- **Linkages with NCERT Textbooks**
 - **Class 11 Political Science (*Political Theory*):**
 - *Chapter on "The State"*: Directly connects to the sovereign monopoly on coercive force and how deputizing private entities to strike foreign infrastructure challenges the classic social contract.
 - *Chapter on "Rights"*: Relevant to the ongoing conflict between state surveillance (inspecting routing metadata) and fundamental individual rights to privacy and unmonitored communication.
 - **Class 12 Political Science (*Contemporary World Politics*):**
 - *Chapter on "Security in the Contemporary World"*: Maps the shift from traditional military confrontations to non-traditional security threats, structural vulnerabilities of critical infrastructure, and asymmetrical digital warfare.
 - *Chapter on "International Organisations"*: Explains why multilateral bodies (such as the UN) struggle to build binding legal consensus among rival great powers regarding new domains of warfare.
 - **Class 12 Political Science (*Politics in India Since Independence*):**
 - *Chapter on "India's External Relations"*: Connects to strategic autonomy, national security governance, and the imperative to defend sovereign infrastructure against external state and non-state aggression.

- **Linkages with the UPSC CSE Syllabus**
 - **GS Paper 3: Internal Security & Technology (Core Focus)**
 - *Cybersecurity Basics & Architecture*: Evaluating the limits of India's current passive architecture (CERT-In, NCIIPC) against automated, state-sponsored offensive campaigns.
 - *Role of External State and Non-State Actors*: The blurring line between foreign intelligence outfits and criminal ransomware syndicates carrying out hybrid warfare.
 - *Security Challenges in Border/Digital Domains*: The transition of warfare from physical borders to trans-boundary critical information infrastructure (CII).
 - **GS Paper 2: Governance, Polity & International Relations**
 - *Executive Discretion vs. Legislative Oversight*: The institutional risk of bypassing Parliament through executive orders to execute covert digital countermeasures.
 - *Fundamental Rights (Article 21)*: Tension between active threat-monitoring and the landmark *K.S. Puttaswamy* privacy mandate regarding proportionality and legality.
 - *International Treaties & Geopolitics*: The failure of multilateral governance (UN OEWG) and India's foreign policy posture within bilateral/multilateral cyber alliances (e.g., Quad Cyber Group).
 - **GS Paper 4: Ethics and Integrity**
 - *Ethics in International Statecraft*: The morality of pre-emptive digital strikes on ambiguous attribution versus the ethical duty to defend sovereign citizens.
 - *Corporate Governance and Moral Hazard*: The ethical implications of private defense contractors profiting from state-sanctioned digital sabotage and cyber warfare.
 - **Relevant Optional Subjects:**
 - *Political Science & International Relations (PSIR)*: Concepts of Sovereignty (Bodin, Hobbes), Realism vs. Liberal Institutionalism, and non-kinetic warfare doctrines in the 21st century.
 - *Law*: Reforming the Information Technology Act, 2000; applicability of the Geneva Conventions and International Humanitarian Law (IHL) to cyber warfare.

- **Way Forward and Strategic Policy Blueprint for India**

- **Enact a Modernized Statutory Framework (Beyond IT Act, 2000):** India must move past the reactive, post-facto compliance mindset of the IT Act, 2000. Parliament should legislate a dedicated *National Cyber Security Act* that explicitly defines the legal parameters, authorizations, and judicial oversight under which active defense can be executed against external threats.
- **Adopt Clear Institutional Bifurcation:** Avoid cross-agency confusion by clearly delineating defensive and offensive functions:
 - *Civilian Sector (CERT-In & NCIIPC):* Remain purely defensive, focused on resilience, vulnerability coordination, and building trust with private industry.
 - *Strategic Command (Defence Cyber Agency & NTRO):* Retain exclusive sovereign authority to conduct pre-emptive disruption and active countermeasures abroad, strictly bound by international legal standards.
- **Create a Regulated Public-Private Partnership Framework:** Instead of covertly relying on unregulated private contractors, establish a transparent, statutory licensing protocol for vetted Indian cybersecurity firms. Mandate high indemnities, strict rules of engagement, and direct operational command by sovereign officers to prevent rogue corporate privateering.
- **Bridge the Capacity Deficit via a Cyber Reserve Cadre:** Resolve the severe shortage of specialized cyber personnel by establishing a National Cyber Reserve Force. This framework should allow top-tier private industry talent to be formally inducted for sovereign defensive and analytical duties under state disciplinary and constitutional oversight.
- **Champion Norms for Critical Infrastructure Immunity:** New Delhi should leverage its leadership in the Global South and multilateral forums (UN OEWG, G20) to push for binding international norms that declare civilian critical infrastructure (hospitals, power distribution, water systems) universally off-limits to both state and state-licensed private cyber operations.

- **UPSC Civil Services Examination (Mains)**

- **GS Paper 3 (2023):** "What are the different elements of cyber security? Keeping in view the challenges in cyber security, examine the extent to which India has successfully developed a comprehensive cyber security framework."
- **GS Paper 3 (2022):** "What are the different types of cyber crimes? What measures have been taken by the Government of India to check the menace of cyber crimes in the country?"
- **GS Paper 3 (2020):** "What is the CyberDome Project? Explain how it can be useful in controlling internet crimes in India."
- **GS Paper 3 (2017):** "Discuss the potential threats of Cyber Attack and the security framework to prevent it."
- **GS Paper 3 (2013):** "Cyberwarfare is considered by some defense analysts to be a larger threat than physical war. Discuss the vulnerabilities of our critical infrastructure to cyber warfare and the institutional mechanisms to address them."

- **State Public Service Commissions (APSC & Others)**

- **APSC CCE Mains (GS Paper 3 - 2023):** "Analyze the role of CERT-In in securing India's cyberspace. Do you think the current legal architecture under the IT Act, 2000 is adequate to tackle state-sponsored hybrid cyber warfare?"
- **APSC CCE Mains (GS Paper 3 - 2021):** "Discuss the vulnerability of critical infrastructure to cross-border cyber attacks. What measures should be adopted to strengthen Assam's state-level cyber response capabilities?"



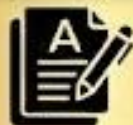
AXIA IAS ACADEMY

UPSC CSE CLASSES

RISE ABOVE THE REST



EXPERT
FACULTY &
GUIDANCE



COMPREHENSIVE
SYLLABUS
COVERAGE



STRATEGIC
TEST SERIES &
MENTORSHIP

ADMISSIONS OPEN

- Prelims + Mains + Interview
- Current Affairs Focus
- Personalized Attention
- Online & Offline Batches



WEBSITE: axiaiasacademy.com



CONTACT: +91 6002-417488

