

Security

16 June 2020 22:45

Syllabus:

Linkages between development and spread of extremism.

Role of external state and non-state actors in creating challenges to internal security.

Challenges to internal security through communication networks, role of media and social networking sites in internal security challenges, basics of cyber security; money-laundering and its prevention

Security challenges and their management in border areas; linkages of organized crime with terrorism

Various Security forces and agencies and their mandate

SHREYA SHREE
AIR 71 - CSE 2021

Intelligence Architecture

21 June 2021 17:15

HUMINT - Human Intelligence - interpersonal contact for intel gathering

SIGINT - Signals Intelligence

IMINT - Imagery Intelligence

MASINT - Measurement and Signature Intelligence

Present structure

- IB - 1887 - reports to MHA; responsible for domestic intelligence, internal security, counter intelligence
- R&AW - 1968 - wing of Cabinet Secretariat
- NTRO - National Technical Research Organisation - 2004 - under NSA, part of PMO
- DRI Directorate of Revenue Intelligence 1957 - falls under FinMin - for anti-smuggling intelligence
- Apex: NSCS National Security Council Secretariat, headed by NSA - 1998
- Joint Intelligence Committee JIC - 2018 - to aggregate, analyse all intel from various agencies
- Overlap due to design, natural consequence of activities
- Mostly evolved as a result of failures and crisis mgmt rather than overarching strategy

Shortcomings

ORF Recommendations

- 3 pillars of reform in national security innovation strategy
 - o People
 - o Paisa (money)
 - o Processes
- Tripartite partnership b/w govt, pvt sector & Academia
- Elements
 - o Govt as investor - intelligence agencies as venture capitalists
 - Eg Q-Tel is CIA's venture arm; Mossad incubator
 - o Rapid experimentation - better leverage existing funding platforms
 - Eg IDEX Innovations for Defence Excellence
 - o Create Future Technologies Unit
 - o Establish a Digital Academy - to train serving intelligence officers
 - o Technology Fellows Programmes
 - Lateral entry for young technical talent
 - CIA & FBI: Cybersecurity Talent Initiative
 - UK - GCHQ has cyber programme for high school students
 - o R&D Charter for intelligence community
 - o INT R&D lab/ Science Park - focused on SIGINT w/in leading engg university
 - o International alliances w/ focus on development exercises
 - o Dedicated unit on OSINT Open Source Intelligence -- made possible by commercial sensors, internet
 - o Healthy competition b/w pvt sector & DPSUs/ DRDO - break near monopoly of the present
 - o Clear method of security clearances for private citizens - to build an industrial base

- Greater participation of private sector in technology assessment
 - For evaluation of new tech, obtain pricing for development
 - Imp for framing of Request for Information (RFI)/ RFP Request for Proposal
- Separate budget for R&D exclusively for Indian private sector
 - Compel foreign OEMs Original Equipment Manufacturers to bring along Indian SMEs/ startups

Kargil Review Committee 1999

Naresh Chandra Committee

Recommendations of IDSA Task Force (2012) -- yet to be implemented

- Legal
 - Legislations for charters, functions, duties of intelligence organisations
 - Legal basis for different tiers of accountability - executive, financial, legislative
- Recruitment, deputation, promotion, training
 - Open, separate direct recruitment mechanisms for different intelligence agencies - possibly using UPSC
 - Deputation slots to induct experts from military, SnT streams
 - Outsource to meet specialised needs
 - Improve training modules, specialised training for analysts
 - Improve quality of trainers, bring in military trainers
 - Review present system of ACRs in intelligence agencies to eliminated subjectivity; bring about better objectivity
 - Review in situ promotions to improve morale at middle, mid-senior levels
- Analysis & operations
 - Improve training in tools of modern prescriptive work
 - Improve quality of supervision in operational branches of intelligence agencies, reverse drift in operational work, discard useless & profligate sources
 - Bring better financial probity in intelligence operations
 - Introduce concept of social welfare safeguards for assets who rendered valuable service for national security but became casualties on the job
- Tech upgrade
 - Enhance in-house tech R&D capabilities; esp signal decryption, cryptography
 - Examine feasibility of outsourcing relevant tasks to experts for improving output
 - Fast track equipment procurement processes, innovative asso of financial experts at suitably high levels
 - Upgrade OSINT Open Source Intelligence capabilities; use advanced commercial search engines
 - Upgrade offensive as well as defensive capabilities in cyber warfare
- Relations b/w intelligence agencies & MEA
 - Bring in system of inter-changeability b/w various agencies and connected ministries
 - Institutionalise covert assignments for external intelligence in consultation w/ MEA to improve cooperation
 - Regular interaction b/w heads of intelligence agencies and Secy of concerned Ministries + area desk officers
 - Resume posting of Joint Secretary level Foreign Service officer in external intelligence for better coordination and liaison
- Coordination of intelligence
 - Appoint a National Intelligence Coordinator/ Director of National Intelligence
 - OR NSA may function independently under Min of National Security

- Accountability
 - o Strengthen financial accountability -- CAG/ NSA
 - o In camera audit of Secret Service Funds
 - o Separate intelligence ombudsman for IB, R&AW, NTRO
 - o Enhance staff support by posting intelligence professionals in external processing units serving Cabinet Secretariat
 - o Examine Minister for National Security & Intelligence w/ admin auth on all intelligence agencies
 - o Parliamentary Accountability Committee for oversight of intelligence agencies through legislation

SHREYA SHREE
AIR 71 - CSE 2021

Development & Extremism

20 June 2020 18:10

Radicalisation

--- UAPA, NIA, FICN, FATF

- Social and psychological process of incrementally experienced commitment to extremist political and religious ideologies
- Not necessarily violent

ISIS has attracted youth fm states like Gujarat, Maha, Kerala

- Few compared to western ctries

Types:

- Right-wing extremism:
 - o Violent defence of racial, ethnic, pseudo-national id
 - o Radical hostility towards state auth, minorities, immigrants, left-wing political groups
 - o Eg. Mob lynching, cow vigilantism, assassinations of rationalists (Narendra Dabholkar, Govind Pansare, Gauri Lankesh)
- Left-wing extremism
 - o Anti-capitalist demands
 - o Transformation of political systems
 - o Incl Anarchist, Maoist, Trotskyist, Marxist-Leninist groups
 - o Use of violence
- Politico-religious extremism
 - o Political interpretation of religion
 - o Violent means to defend a religious id fm perceived attack

Strategies for de-radicalisation

- Extremism counselling hotline for 'vulnerable & indoctrinated youth'
 - o Eg Austria
- Community outreach
 - o US's counter radicalisation program
- Detection of potential, existing recruits + remedial action
- Big data analytics to gather intel
- Appealing through religious leaders
- Vyayam shala in minority schools
- Teaching all religious texts in minority schools, academic knowledge of what Quran really teaches, values of democracy, NCC training
- Islamic education through internet or present counter narrative
- Reach out to minorities through empathetic policing, teaching urdu in schools, develop minority areas as smart urban clusters

Approach in India:

- Underestimation of threat
- No official policy on radicalisation, de-radicalisation
 - o 4 aspects: individual, family, religion, psychology
 - o Lasting change in individual's belief system
 - o View it as rehabilitative, reformative, preventive approach
- Security centric perspective - undermines
- K'taka: imparting knowledge of liberal Islam; database of mosques & madrasas
- Maha: identify, reduce feeling of communalism w/in force

Challenges in formulating policy

- Aims only those who undergo radicalisation, not those who have overstepped law under influence of radical doctrine
- Marginalised/ neglected sections - little trust in law enforcement agencies
 - o Block attempts constructive dialogues
- Isolated policies w/o comprehensive fw: weak, slow intel gathering, action
- Only dealing w/ superficial aspects

Way forward

- Recognition of problem
- Based on objectively researched conclusions w/ strong evidence
- Centre must develop umbrella of legal fw - coordinate states
- Don't limit to specific communities/ source of radicalisation
- Meaningful research
- Use tech
- Community outreach
- Involve civil society
- Choke funding
- Prevent politicisation of religion

Case study:

- [Philippine govt recruiting Muslims into army to counter terrorism thru mixture of religious, security approaches](#)

Extremism

- Violent extremist ideologies have found fertile ground in fragile communities characterised by little access to devt
- Understood as constituting view far fm those of the majority population
- Not necessarily illegal; do not automatically lead to violence or harm

Left Wing Extremism LWE

- Roots: leftist/ communist political movements, labour & agrarian unrest, tribal revolts during various phases of colonial rule
- No change on ground after indep
- Prophecy of leaders:
 - political indep of India fm Brit -> change of exploiters;
 - socio-economic struct would remain same
 - Armed revolution needed to end exploitation
- Naxalbari uprising 1967-72
 - Charu Majumdar
 - Failed; marked beginning of violent LWE movement
 - No nationalist image -> excessive id w/ China
 - Over-optimistic evaluation of possibility of advancing rapidly
 - Under-estimation of state's strength
 - No mass support
- Post-Charu phase 1970s -2004
 - Polemics -> groups divided
 - 'Liberation' party 1975 - Vinod Mishra
 - o 1st Naxal leader to recognise futility of armed rebellion against Indian govt
 - o Rectification movement
 - Mass mobilisation, electoral politics

- CPI (M) - 2004- ___
 - Maoist insurgency doctrine: glorification of extreme left ideology
 - o Legitimisation of violence to overwhelm existing socio-economic, political struct



- Strategy:
 - o 3 distinctive phases
 - Organisation, consolidation, preservation of regional base areas in isolated terrain
 - Progressive expansion
 - Destruction of enemy - conventional battles

Issues

- Forest Laws
 - o Forest Conservation Act, 1980
- Land fragmentation + other factors
 - o 40% rural hhs - no land/ < 0.5 acre
 - o No land reforms
 - o Exploitation of tenants
 - o Evasion of land ceiling laws (by traditional elites)
 - o Existence of special land tenures
 - o Encroachment on CPRs Common Property Resources
 - Community pastures, watershed drainages, village tanks
 - o Non-regularisation of traditional land rights
 - o Poor implementation of prohibition of land transfer to non-tribal areas in 5th Schedule areas
 - o Non-regularisation of traditional land rights
- SEZs
 - o Inadequate compensation
- Displacement due to development projects
 - o Forced evictions
- Unemployment, non-implementation of minimum wages
- Environmental degradation
- Tourism
- Social exclusion
 - o Denial of dignity
 - o Continued practice of untouchability in various forms in some areas
 - o Poor implementation of special laws
 - Prevention of atrocities
 - Protection of civil rights
 - Abolition of bonded labour
- Governance
 - o Corruption
 - o Poor provision of essential public services
 - o Incompetent public personnel + absenteeism

- Misuse of powers by police
- Perversion of electoral politics
- Unsatisfactory working of local govt

Govt efforts

- 'Police' & 'Public Order' - state subjects
- Lack of coordination among states, centre
- **Dvpmnt efforts**
 - Clear, hold and develop strategy
 - Integrated Action Plan IAP
 - By planning commission for 82 LWE affected, backward distts
 - Construction of school, buildings, anganwadi centre, drinking water facilities, rural road, panchayat, community halls, playground etc
 - PMRDF PM Rural Dvpmnt Fellowship
 - Min of Rural Dvpmnt
 - Capacity building for qualified young professionals to carry out grass root dvpmnt
 - PESA Act 1996 - Panchayat (Extension to Scheduled Areas)
 - Surrender cum Rehabilitation Scheme
 - RRP - I & II - for Road Connectivity Project
 - LWE Mobile Tower Project
 - PESA implementation
 - Skill development - Pradhan Mantri Kaushal Vikas Yojana
- **Security Measures**
 - SAMADHAN - 2017
 - Against Maoist
 - S - smart leadership
 - A - aggressive strategy
 - M - motivation
 - A - actionable intelligence
 - D - dashboard-based KPIs Key Performance Indicators & KRAs Key Result Areas
 - H - harnessing technology
 - A - action plan for each theatre
 - N - no access to financing
 - CAPFs, CoBRA Commando Battalions for Resolute Action
 - CIAT Counter Insurgency & Anti Terrorism schools
 - MPF modernisation of police forces, fortified police stations
 - Reimbursement of SREs Security Related Expenditures
 - Intelligence sharing, community policing & civic action programmes
 - GIS Mapping, unified command
 - Operation Green Hunt
 - Central India, since 2009
 - CG, Jharkhand, Andhra, Maha
 - Central CoBRA force + state police
 - Salwa Judum
 - = Peace March/ Purification Hunt in Gondi
 - Anti-insurgency militia
 - 2006 - people's resistance movement against Naxalites
 - SC: illegal, unconstitutional; violation of human rights

North East

Causes

- Immigration
- Economic underdevelopment
- Poorly developed transport, communication links

- Negligence of central govt
- Corruption among local politicians & elites
- Lang/ ethnicity/ tribal rivalry
- Control over local resources
- Governance issues
- Widespread feeling of exploitation, alienation

MAJOR INSURGENT GROUPS OPERATING IN NORTH EASTERN STATES AND DECLARED AS "UNLAWFUL ASSOCIATIONS" AND "TERRORIST ORGANIZATIONS" UNDER UNLAWFUL ACTIVITIES (PREVENTION) ACT, 1967

ASSAM		Listed/declared as -
(i)	United Liberation Front of Assam (ULFA)	Terrorist organization and unlawful association
(ii)	National Democratic Front of Bodoland (NDFB)	-do-
(iii)	Kamtapur Liberation Organization (KLO)	Terrorist organization
MANIPUR		
(i)	People's Liberation Army(PLA)	Terrorist organization and unlawful association
(ii)	United National Liberation Front(UNLF)	-do-
(iii)	Peoples' Revolutionary Party of Kangleipak (PREPAK)	-do-
(iv)	Kangleipak Communist Party (KCP)	-do-
(v)	Kanglei Yaol Kanba Lup (KYKL)	-do-
(vi)	Manipur Peoples' Liberation Front (MPLF)	-do-
(vii)	Revolutionary Peoples' Front (RPF)	-do-
(viii)	Coordination Committee Cor-com (conglomerate of six valley base UG outfits).	-do-
MEGHALAYA		
(i)	Hynniewtre National Liberation Council (HNLC)	Unlawful association
(ii)	Garo National Liberation Army (GNLA)	Terrorist organization

TRIPURA		
(i)	All Tripura Tiger Force (ATTF)	Terrorist organization and unlawful association
(ii)	National Liberation Front of Tripura (NLFT)	-do-
NAGALAND		
(i)	The National Socialist Council of Nagaland (Khaplang) [NSCN/K]	Terrorist organization and unlawful association
(ii)	National Socialist Council of Nagaland (Isak Muivah) – [NSCN(I/M)]	With ceasefire with the Government.
(iii)	National Socialist Council of Nagaland (Kitovi-Neopaokonyak) [NSCN(KN)]	
(iv)	National Socialist Council of Nagaland (Reformation) [NSCN(R)]	

Armed Ethnic Groups reasons

- Political motivation - popular support through political cause
- Availability of Arms
- Popular support base
- Terrain
- External support
 - o 2010 RAND study: w/o external support & avbl sanctuaries, no internal insurgency can thrive over a period of 10 years
- Strategy & nature of these outfits
 - o Cease fires seen as phases to re-group, recruit, finance, re-arm

Govt Initiative

- 3 conceptual parameters:
 - o Proportionate use of force
 - AFSPA

- Border surveillance incl border fencing, flood lighting on India-B'desh border
- Use of dialogue & negotiations
 - Peace process w/ states
 - Scheme for surrender-cum-rehabilitation of militants in NE
 - SRE
 - Civic action programme
 - Advertisement & publicity 'Peace Pays'
- Structural changes
 - MPF
 - Helicopter services in NE states

Needs

- Dialogue as an ongoing process to reach concrete soln w/ all stakeholders
 - Not pre-condition of complete abjuring of violence
- Coordination w/ neighbouring countries
- Political autonomy
- Governance, delivery mechanisms
- Cooperation among forces on intel sharing, investigations, operations
- Alternative conflict resolution
 - Communication
 - Mediation
 - Negotiation - conflict prevention too alongside resolution
 - Neutral fact finding
 - Neutral evaluation of grievances
 - Forum for dissent, disagreement, demonstration, discussion
 - Prevent misuse of media to fuel division

--- Bezbaruah Committee Report, NRC , [AFSPA](#), UAPA

Jammu & Kashmir Insurgency

- Conflict b/w various Kashmiri separatists, nationalists "ultras" (extremists) & Gol
- Dispute over local autonomy

2 dimensions

- External
- Internal

Difficult to resolve b'cos

- Indian territorial defensibility
- Pak state argument
- Kashmiri nationalism - making it an awkward 0-sum game

Reasons

- Rigging of 1987 assembly elections
- ISI's role
- Mujahideen influence
- Religion - only Muslim majority state in India
- Humanitarian abuses
- Poor socio-development indicators

Govt Approach

- UDAAN scheme - by MHA, NSDC National Skill Dvpmnt Corporatoin
 - To bring corporates to recruit J&K youth
- Rehabilitation policy
- Surrender policy
- Placement of special police officers for their services in the state

- Subsidised helicopter services in the state
- Scheme for providing financial assistance to families of displaced persons of PoK
- Central scheme for assistance towards damaged property during actions by CPMFs and army in J&K

Challenges

- Counter-terrorist operations with a human face.
- Rehabilitation of surrendered militants.
- Disposal/resolution of cases against terrorists for waging war against the Indian nation.
- Rehabilitation of Kashmiri Pandits and other Internally Displaced Persons (IDPs)
- Reconstruction of the state.
- Revival of Kashmiriyat and Sufism to reduce the adverse impact of fanatic jihadi ideology
- Conflict resolution.
- Role of the media.

Failure of militancy

- Extremely localised grievances
 - o Both Muslim & Kashmiri Hindus
- Failure of moderate Kashmiri leadership to emerge, no vision to espouse Kashmiri cause
- Increasing govt authority, resources
- Disillusioned youth prefer fighting on social media rather than guerilla
- World sees Kashmir as border dispute rather than ethnic terror conflict

Reqd Approach

- Amitabh Mattoo 4D
 - o Dialogue
 - o Demilitarisation
 - o Devolution
 - o Development

External state, non-state actors - internal security

20 June 2020 18:55

[TJ](#)

External State Connections

- China

- Mongoloid tribes in NE India
- close ethnic and cultural ties with the tribes in China, Tibet and Burma.
- Barring Khasis and Jaintias of Meghalaya, almost all hill tribes belong to the Tibeto-Chinese fold and to the Tibeto-Burmese family.
- affinity towards the border people of erstwhile East Pakistan and Burma that led some of these tribal groups to turn towards their own stock rather than towards the country they resided in.
- Apart from the Nagas, the Chinese also extended moral and material support to the Mizo and Meiti insurgents by arranging for their training in guerilla warfare and subversion in training centres in Yunan province of mainland China and Lhasa in Tibet.

- Bangladesh

- East Pakistan, Bangladesh since 1971, was host to many insurgent activities unleashed against India in the northeastern region.
- The anti-India operations have been largely possible because of the presence of an overwhelming illegal immigrant Bangladeshi population in the northeast. The porosity of the Indo-Bangladesh border has led to many unanticipated problems for India.
- The international terrorist groups like al Qaeda in the Indian Subcontinent (AQIS) and Islamic State of Iraq and Syria (ISIS) have lately focused their attention to the region. Bangladesh has seen a number of terrorist acts in recent times in the form of killing of secular bloggers and liberals purportedly by ISIS or local extremist groups such as Ansarullah Bangla Team (ABT) which draw their inspiration from global Islamism.
- As the extremism grows in Bangladesh, its demonstration effect may lead to increased infusion of fundamentalist ideologies on religious grounds in neighbouring Indian states as well, which may manifest in radicalisation of youth.

- Myanmar

- India shares a 1670 km long land border and a maritime border of 200 km with Myanmar.
- Some Burmese tribals belonging to the Kuki Chin Group are fighting for merger of lands inhabited by them with India.
- The Myanmar rebels ensure that drugs are brought under their protection up to the Tamu on the Indo-Myanmar border and also upto Bangladesh-Myanmar border. The Indian insurgent groups and the Bangladesh syndicates take over from these locations and thereafter push the drugs inland.
- Countries that are unfriendly towards India find an opportunity in the ongoing turmoil in the northeast and their involvement has made the problems that much more difficult to resolve. Because of geographical proximity, even smaller

countries such as Nepal and Bhutan are unable to remain immune to the developments in this region.

Non State actors

- Act of Terrorism, insurgency or extremism by any individual or a groups which has no direct or indirect linkages with any government or any government organization, is said to be done by non-state actors.
- The emergence of non-state terrorist actors and the rise of their international influence is accelerating. Much of their activity is clandestine and outside the accepted international norms. International and state-sponsored terrorism, often motivated by fundamentalist ideologies, backed by secretive but efficient financial networks, use of IT, clandestine access to chemical-biological and nuclear materials, and illicit drug trafficking, has emerged as a major threat to international stability.
- They pose threats to multi-religious, multi-ethnic and pluralistic societies. India is at the receiving end of these violent elements and is likely to remain a target of international terrorism in the future. Strategies need to be evolved to counter the threat of Weapons of Mass Destruction (WMD) terrorism as well as cyber-terrorism; the latter especially against infrastructural and economic assets such as banking, power, water and transportation sectors.
- Pakistan has been waging a proxy war against India since the 1980s. Since the Kargil War and the military coup of October 12, 1999, Pakistan's support to cross border terrorism has intensified and is expected to continue in the future. The rapid growth of Islamic fundamentalism in Pakistan is also of serious concern to India.
- Through its nexus with the Taliban and Jihadi elements, as well as its involvement in religious extremism, international terrorism and the narcotics trade, Pakistan poses a threat not only to India but to the stability of the region as well.

Threats posed by them to internal security of India:

- Bomb blasts, attacks on major establishments/public places (Akshardham, 26/11 etc.) which partially dismantles India's stability
- They bring fake currency to India and try to hit Indian economy
- They smuggle weapons, drugs (in Punjab/Northeast) in India, directly targeting the youth
- Extremist non state actors also include religious fanatics which propagate religious hatred which can led to communal tensions in the country
- They can also incite people for regionalism thus demanding their separate state which further increases secessionist tendencies
- Terrorists/insurgents are receiving weapons mainly from across the borders with the assistance of organised smuggling groups. Most of the arms are coming from Pakistan through the ISI, Pakistani based fundamentalist organisations, Afghan Mujahideen groups and the militants themselves, who bring arms from Durrah in the North West Frontier Province (NWFP).
- The smugglers have also acquired high- powered speed boats, which can land at uncharted beaches and creeks. Arms are also coming through the long and porous Indo-Nepal border. In addition, arms are being smuggled via Bangladesh and Myanmar.
- Today's terrorists, be they religious extremists, Jehadis, international cults like Aum Shinrikiyo or individual nihilists, may gain access to nuclear, biological, and chemical weapons or raw materials. NBC terrorism today has moved from the stage of far-fetched horror to a contingency that could happen tomorrow. The advances in IT and communications have made terrorism with Weapons/Materials of Mass Destruction

easier to carry out.

GCTOC Gujarat Control of Terrorism and Organised Crime Act - 2019

- anti-terrorism law
- Returned by 3 Prez; assent by Prez Kovind
- Confessions made before police officer will also be considered as evidence
 - o Rank of SP or above only
 - o Violates Art 20 - FR of an accused
- 'organised crimes' - criminal activities run for a substantial profit
 - o Economic offences: Ponzi schemes, multi-level mkting, organised betting
 - o Extortion, land grabbing, contract killings, cybercrimes, human trafficking
- Draws heavily fm MCOCA Maha Control of Organised Crime Act, 1999
 - o GCTOC doesn't contain checks on interception of communication
 - Only talks about admissibility of evidence collected thru interception
 - Violates Art 21 - Right to Privacy
 - o Defn of 'terrorist act' also covers 'intention to disturb public order'
 - Allows Patidar agitations and the likes to be described as act of terrorism
 - Not in line w/ UAPA 1967; it includes such incidents under IPC
- 180 days for auth to file charge sheet, stricter conditions for bails
 - o Usually 90 days
 - o Could encourage custodial torture
- Creation of special courts, appointment of special public prosecutors
- Arguments in favour
 - o Govt could introduce checks and balances while framing rules
 - o Provision - court can ask govt to frame rules to this effect
 - o Constitutional validity of law can be challenged on a case-specific basis
 - o Inbuilt mechanisms to limit extension of 'terrorist act' definition
 - FIR registration - rank SP or above
 - Sanction fm state govt reqd before court takes cognisance
 - o Similar provisions under TADA, POTA (both repealed now)
 - o Gujarat has border w/ Pak
 - CrPC inadequate in such cases
- Arguments against
 - o Competing interest of law & order v/s privacy
 - o Very wide definition of 'terrorist' act
- Conclusion - Existing laws like CrPC are comprehensive. Need for better training for investigators.

[Adverse List](#)

UAPA Unlawful Activities Prevention Act (1967, 2019 amendment)

- an upgrade on the Terrorist and Disruptive Activities (Prevention) Act TADA (lapsed in 1995) and the Prevention of Terrorism Act – POTA (repealed in 2004) was passed in 1967
- special procedures to handle terrorist activities, among other unlawful activities.
- death penalty and life imprisonment as highest punishments
- **2019 Amendment**
 - o Government can now designate individuals as terrorists on certain grounds provided in Act.

- Earlier only organisations could be declared as such
 - Not designating individuals as terrorists, would give them an opportunity to circumvent the law and regroup under different name
- empowers the Director General of NIA to grant approval of seizure or attachment of property when the case is investigated by NIA
 - Earlier required consent of State Police -> delays
- empowers the officers of the NIA, of the rank of Inspector or above, to investigate cases of terrorism
 - This will help solve the human resource crunch in the NIA.
- 2021 Delhi HC Rulings
 - Terrorist activity can NOT be broadly defined to include ordinary penal offences; extent and reach must travel beyond the effect of an ordinary crime
 - First instance of a court calling out alleged misuse of UAPA against individuals
- Criticism
 - Experiences of Anti-terror laws in India such as POTA and TADA reveals that they are often misused and abused.
 - could also be used against political opponents and civil society activists who speak against the government and brand them as “terrorists.”
 - Critics argue that the law, especially after 2019 amendment gives unfettered powers to investigating agencies.
 - Some experts feel that it is against the federal structure, given that ‘Police’ is a state subject under 7th schedule of the Indian Constitution.
 - Regular bail subject to satisfaction of the judge that no prima facie case exists
 - Dilatory trial procedures -> lengthy periods of pre-trial incarceration for accused
 - 180 days to file a chargesheet -- too long
- Stats:
 - NCRB: 4231 cases under UAPA b/w 2016, 2019
 - Low rate of acquittals (good)
 - High pendency rates- bad
 - 83% at level of police investigations
 - 95.5% at level of trials
 - 33% rise in cases filed under UAPA b/w 2013 and 2019 (NCRB)

Mob Lynching

- Took US 100 yrs to approve a bill to make lynching a federal crime
 - 200+ anti-lynching bills since 1918
 - 2018: Justice for Victims of Lynching Act - unanimous approval
- Hate lynching:
 - Terrorises entire community
 - Performative acts -> small numbers, yet instil intense fear
- Modern tech
 - Video widely circulated
 - Celebrated as acts of nationalist valour
 - Pervasive sense of every day normalised for targeted minority communities
 - -> ultimate act of terror
- SC: sought explanation from Union, state govts
- Significant statutes:
 - UP Law Commission - draft anti-lynching law
 - Manipur govt introduced ordinance 2017
 - Both hold police guilty for dereliction of duty

- Exercising lawful auth vested in them
- Protection to victim of lynching
- Failure to act upon apprehended lynching
- Refusing to record any info related to lynching cases
- UPLC also holds DM guilty
- Both lay down official duties to protect victims, witnesses
- UPLC - right to compensation
- Prevention of Communal & Targeted Violence (Access to Justice & Reparations) Bill
 - Recommends creation of new crime - lynching
- Challenges
 - Most perpetrators go unpunished (99% in US)
 - Madhya Pradesh Cow Progeny Slaughter Prevention Act, 2004
 - Limited scope
 - No inclusion of dereliction of duty, protect victim rights, secure compensation
 - Rajasthan tabled anti-lynching bill
 - Doesn't contain dereliction of duty, victim rights

MPISA Maharashtra Protection of Internal Security Act, 2016

- Maha 1st state to have own law for internal security
- Not discussed in legislative assembly (?)

Afa

Challenges to internal security

20 June 2020 18:56

Challenges to internal security through communication networks, role of media and social networking sites in internal security challenges, basics of cyber security; money-laundering and its prevention

Internal Security Acts

- Official Secrets Act 1923
- Criminal Law Amendment Act 1961
- Enemy Property Rules 2015
- Explosive substances act 1908
- Arms (amendment) act 2019
- Young persons (harmful publications) Act, 1956
- Special protection group Act 1988
- Sikh gurdwaras amendment act, 2016

NHRC

Bureau of police research and development

National integration council

Narcotics control bureau

Mutual legal assistance in criminal matters - revised guidelines

Police Modernisation umbrella Scheme MPF

Cyber - I4C Indian Cyber Crime Coordination Centre

- National Cybercrime Threat Analytics Unit
- Cybercrime Ecosystem Mgmt Unit
- National Cybercrime Reporting Portal
- Platform for Joint Cybercrime Investigation Team
- National Cybercrime Training Centre
- National Cybercrime Research and Innovation centre
- National Cybercrime Forensic Lab Ecosystem

CCPWC Cybercrime Prevention against Women & Children Scheme

Communication Network

- Part of **Critical Information Infrastructure**: "The computer resource, the incapacitation or destruction of which, shall have debilitating impact on national security, economy, public health or safety
- Critical Infra: Those facilities, systems, or functions, whose incapacity or destruction would cause a debilitating impact on national security, governance, economy and social well-being of a nation
- Crucial for connectivity of other critical infra
 - o Eg. Energy, transportation, banking & finance, telecom, defence, space, law enforcement, security & intel, sensitive govt org, public health,

- water ss, critical mfg, e-governance
- Threats
 - Through the network
 - To the network
- Applications
 - Vital + auxiliary functions in critical infra sectors
 - Voice, data communication
 - Financial sector - ATM, etc -> financial stability
 - Flash crash of NYSE 2000
 - Fake twitter post - hacked acc (Homo Deus)
 - Connects infra systems, subsystems & constituents
 - Smart Grid power sector
 - Smart cities
 - Wired network- optical fiber
 - Wireless - 4G, 5G, WiFi
 - Satellite network
 - Machine to machine connectivity
 - Networks - MAN, WAN, PAN, HAN
 - Dedicated resources for critical communication
 - Automation in industrial, mfg facilities
 - E-governance - Digital India, e-Governance Plan, e-Kranti
- Threats
 - Natural
 - Human induced
 - Insiders
 - Economic, military or adversary nation states
 - Long-term operations incl espionage, data/ credentials theft, execution & monitoring attacks
 - Criminal syndicates to terrorist outfits
- Possible targets
 - Devices: routers, switches, firewalls, mobile phones, database, DNS servers
 - Web portals, protocols, ports & communication channels
 - Satellite network communication systems
 - Network applications such as cloud based services
 - SCADA Supervisory Control and Data Acquisition - gathers, analyses real time data
- Terrorists and non-state actors
 - Obj: instigate terror in victims, onlookers
 - Great access to HR w/ good knowledge due to radicalisation among youths
 - Eg ISIS, LeT have own secured communication apps for smartphones
 - w/ support of adversarial states
- Nation states
 - Potent threat
 - Large resources at disposal
 - Lucrative threat in the absence of globally agreed norms/ legal measures
 - APTs Advanced Persistent Threats
 - State-sponsored campaigns against CII esp communication network
 - Sophisticated, targeted, prolonged
 - Wide variety of techniques
 - SQL injection, malware, spyware, phishing, spam
 - Designed to remain undetected/ hidden fm admin - for years
 - Eg.

- USCYBERCOMM - US Cyber Command - has offensive capabilities
- South Korea - Cyber Warfare Command - 2009 - response to North Korea's cyber warfare units
- Brit GCHQ Govt Comm HQ has started preparing cyber force
- China - 2010 - response to US Cyber Command
- Need to secure!
 - Basis of digital ecosystem
 - National security
 - Chain of commands in security agencies
 - Sharing gathered intel - horizontal, vertical
 - Growing interdependencies
 - Power reqd by all
 - Power requires transportation
 - Protecting digital sovereignty
 - Individual control over data that can be gathered, distributed, used, saved about them
 - Building confidence on digital technology
 - Digi-locker etc
- Challenges
 - External sourcing of equipment and tech
 - Chinese devices - 60% of total telecom equipment imports
 - Could have back-window
 - IEEMA Indian Electrical and Electronics Mfg Association - concern of security threat in critical power infra
 - Evolving nature of threats
 - Involvement of state and non-state actors
 - Inadequate understanding of interdependencies
 - Structural challenges
 - Federalism
 - Cyber security not mentioned in 7th Schedule
 - States oppose central govt initiatives - eg. NATGRID
 - Coordination among security agencies
 - Lack of national security architecture
 - Private sector ownership & operation of significant part of info infra
 - Security can't be left to pvt sector alone
 - Lack of incentive to improve cybersecurity
 - Poor enforcement of regulations
- Developments
 - Data Protection Bill
 - Legal amendments to deal w/ cyber terrorism threats added thru IT (Amendment) Act, 2008
 - National Telecom Policy 2012 - target for domestic production of telecom equipment to meet 60-80% domestic dd by 2020
 - Measures to have equipment free fm vulnerability, viz. Mandatory local certification
 - NCIIPC National Critical Info Infra Protection Centre
 - Under NTRO National Technical Research Org
 - Nodal agency for CII protection
 - Id of all CII elements
 - Strategic leadership, coherence across govt
 - Coordinating, sharing monitoring, collecting, analysis, forecasting national level threat to CII
 - Policy guidance, expertise sharing, situational awareness
- Way forward:
 - Foster trust , confidence
 - Address tech, policy, legal dimensions
 - Move beyond traditional roles as regulators

Media and Social Networking

- Broad classification
 - o Print media
 - Newspapers, magazines, books & brochures, billboards, etc
 - o Electronic media
 - News sites, social networking sites, mass SMS schemes, television, internet, radio, cinema, etc
 - o New age media
 - Mobile phones, computers, internet, e-Books
- Role:
 - o Inform and educate people objectively, impartially and in an unbiased manner about security threats and challenges
 - o Unbiased reporting with the restraints of self regulations
 - o Promotion of the principles of healthy democracy
 - o Respect for the Constitutional Provisions
 - o To build a bridge between people and governments at the national level
 - o Uphold fairness, justice, national unity and international cooperation
 - o Inform, educate, entertain, publicize and most importantly correct the excesses in any society.
 - o Highlight the trouble spots in the society and press the government and public to devise suitable mechanisms to eliminate them
 - o Shape the perceptions of government, influence public opinion, promote democracy, good governance as well as influence peoples' behavior and support people- oriented policies
- Distinction b/w **facts, opinions and speculation** has been blurred
- Media as a threat to internal security
 - o Wider perspective of national security issues absent
 - o Self-restraint absent
 - o Over-analysis distorts national security perspectives
 - o Anchors lack political and strategic maturity to discuss national security issues
 - o Cut out development of contrary views and perspectives by imposing commercial breaks
- Measures to tackle the threat
 - o Accuracy
 - o Neutrality, impartiality and objectivity
 - o Ensure crime and violence are not glorified
 - o Privacy
 - o National security - use of terminology, maps mandated by law; refrain fm encouraging secessionist interests but broadcast instances of breach of national security in public interest -- not to be confused w/ endangering national security
 - o Superstition and occultism
 - o Sting operations - as last resort

India's National Security Issues and Indian Media Record:

“

* **India's Nuclear Weapons Test 1998:** The Indian media went berserk in politicising the issue. It chimed that there were no national security threats in evidence justifying it. Within seven months the Kargil War took place.

* **Pakistani Proxy War in J&K:** The media has been totally irresponsible. India's strategic sensitivities are constantly ignored and there is a competition to adopt extreme liberalist views. One theme often stressed is of Kashmiri alienation. Had that been so, Pakistan by now would have inflicted a Bangladesh on India.

* **Kargil War:** Instead of marshalling the nation into a cohesive force, the Indian media playing partisan political roles at the height of the war, were busy stoking controversies as to how it happened.

* **Agra Summit:** The summit had more to do with India's national security interests than political diplomacy. The Indian Media went berserk in focusing and projecting General Musharraf's view point than advancing India's interests. What a comparison to the Pakistani journalists who utilised India's electronic media space to defend and advance their country's interests.

* **India's Military Mobilisation December 2001:** Pakistan did not have to use ISI to spy on India's mobilisation efforts and moves of its strategic formations. The Indian media was doing the job.

- Existing Regulations

- Art 19 - freedom of speech w/ suitable restrictions
- Art 105(2), 194(2) - press can publish/ report legislative pr
- Press Council Act of 1978, National Security Act 1980 - restrictions on press while reporting on sensitive/ confidential issues
- Defence of India Act, 1962 - restrained press largely
- Civil Defence Act, 1968 - govt can make rules to prohibit printing/ publication of any book, newspaper, etc
- Broadcasting Code 1962
 - Adopted by 4th Asian Broadcasting Conference
 - Highlights major principles to be followed by electronic media:
 - ensuring the objective presentation of news and fair and unbiased comment, to promote the advancement of education and culture.
 - raising and maintain high standards of decency and decorum in all programmes
 - providing programmes for the young which, by variety and content, will inculcate the principles of good citizenship.
 - promoting communal harmony, religious tolerance and international understanding.
 - treating controversial public issues in an impartial and dispassionate manner.
 - respecting human rights and dignity.
- News Broadcasting Standards Authority
 - Indep body by News Broadcasters Association
 - Consider, adjudicate upon complaints about broadcasts
- Self Regulatory Content Guidelines for Non-News and Current Affairs Television Channels

Social Media

- Participation
- Openness
- Conversation
- Community
- Connectedness

Types

- Social networks
- Blogs
- Wikis
- Forums
- Content communities
- Micro-blogging

Use by law enforcement agencies

- Use public data to gauge sentiments, predict patterns & possible flash points of disturbances, prevent & react to cyber crimes
- Build actionable intelligence to support human intelligence efforts, share across agencies
- Warning and Trend Prevision Tool
- Institutional Communication Tool
 - o Informational Superiority - state has to have advantage on adversary in IT and decision making to protect strategic interests
- Influence, propaganda and deception tool

Threats to internal security

- Terrorism - radicalisation, recruitment, communication and training tool
- Protest movements and revolution
- Criminality - support, communication, coordination tool
- Mobile phone -> instant digital camera, video
- Cyber bullying, misuse & corruption of personal info, posting material about 3rd party, w/o consent, etc
- War
 - o NATO: future conflicts will occur in more and more connected environments, which will be characterized by the use of new communication and information technologies, Social Media included
 - o Hacking of media networks by enemy countries
 - NY Times, Twitter servers by Syrian agencies

Regulations

- Sections 69, 69(a) of IT Act 2000: govt can
 - o issue directions for blocking of information for public access and to issue directions for interception or monitoring or decryption of information through any computer resource when circumstances threaten public order, defence, security, sovereignty and integrity of India, or friendly relations with other states or to prevent incitement to the commission of any cognizable offence relating to the above circumstances.
 - o Article 69 (b) of the IT Act 2000 empowers agencies of the government of India, in this case the Dept. of Electronics and Information Technology, "to authorise to monitor and collect traffic data or information through any computer resource for cyber security" for cyber incidents and breaches.
 - o Safeguards: Rules under 69 (a) of IT act 2000 (rule 7), authorizes Secretary, DeitY as a competent authority to issue directions for blocking of information for public access after examining recommendations of a committee comprising of designated officer of DeitY, Joint Secretaries of MHA, Ministry of Law and Justice, Information and Broadcasting and ICERT.

Measures

- Use of same medium by auth to provide correct info, nip rumours in the bud
 - o Underutilisation of existing tech
- SOCMINT Social Media Analysis Generated Intelligence - model to isolate

- hotspots/ subjects that go viral - use as predictive tool
- Social Media Lab by Mumbai Police - monitors relevant info fm FB, YT, Twitter, other public domain info
- More pilot projects to dev truly credible database
- Awareness that internet is not a private place
- Corporates: revised security model acc for sharing of info across social networks - unrecognised risks
- Strengthening of legislation designed to protect personal info
- Working to define, protect data ownership rights in a web based envi

Cyber Security

[telecom CA, defn etc](#)

Definitions:

- **Cyber security** means protecting information, equipment, devices computer, computer resource, communication device and information stored therein from unauthorised access, use, disclosure, disruption, modification or destruction (IT Act, 2000)
- **Cyberspace** complex environment comprising interaction between people, software and services, supported by worldwide distribution of information and communication technology devices and networks. (IT Policy 2013)
- **Cyber Threats**
 - o **Cyber Espionage** - use of computer networks to gain illicit access to confidential information, typically that held by a government or other organization
 - o **Cyber Crime** - any type of offensive manoeuvre employed by individuals or whole organizations that targets computer information systems, infrastructures, computer networks with an intention to damage or destroy targeted computer network or system
 - o **Cyber Terrorism** - violence not compulsory; must be serious enough to create panic by attacking critical systems/ infra
 - o **Cyber Warfare** - The use of computer technology to disrupt the activities of a state or organization, especially the deliberate attacking of information systems for strategic or military purpose

Importance of cyberspace

- Key component in formulation, execution of public policies
- Processes, stores sensitive & critical data
- Could lead to disruption of many public services - railways, defense systems, communication system, banking, other fin insti
- States devping cyberattack capabilities
- Ind vulnerable to cybercrimes due to proliferation of internet based services - online bank frauds, surveillance, profiling, violation of privacy

Challenges

- Diffused and intangible threat
- Difficult to locate the attacker; can be misled
- Absence of any geographical cooperation
- Need of international cooperation
- Rapidly evolving tech
- Non-existence of fool-proof security architecture
- Human element in cybersecurity: due to own mistakes
 - o Stuxnet - physical intro of infected USB into Iran's nuclear facilities
 - o 2016 Cyber-heist of \$950mn fm B'desh - gullible/ complicit bankers handed over SWIFT codes to hackers

Cybersecurity in India

- NCRB:
 - o 6% annual rise b/w 2015-16
 - o 350% increase in no of cases b/w 2011-14
 - o Most attacks fm US, Turkey, China, Brazil, Pakistan, Algeria, Turkey, Europe, UAE
- Recent instances
 - o Wannacry Ransomware attack 2017
 - o Legion attack hacking social media acc of famous personalities
 - o Leakage of Aadhaar data
 - o Leakage of debit card data fm private bank in 2016
 - o 2019: power plant (?)
 - o More!!

Legal Framework

- **National Cybersecurity Policy 2013**
 - o 24x7 NCIIPC National Critical Info Infra Protection Centre
 - o 5lakh strong cyber security professionals taskforce in 5 yrs
 - o Fiscal schemes for businesses to adopt std security practices
 - o Testing labs to regularly check safety of equipments
 - o CERT-In designated nodal agency - cyber security related matters
 - State CERT bodies to do this at resp level
 - o **Open Standards** for Cyber Security
 - o Dynamic legal fw
 - o Wider use of PKI Public Key Infra for govt services
 - o Infosec professionals to assist e-Governance, etc
 - o Concerns
 - Only defensive & response measures
 - No mention of need to develop offensive capacity
 - Lack of proper implementation, esp 5 lakh professionals
 - Inadequate for balancing cybersecurity needs w/ need to protect civil liberties of citizens (esp privacy)
- **IT Act, 2000 (2008 Amendment)**
 - o Regulates use of computer systems, networks, data
 - Publicizing sexually explicit material in electronic form
 - Video voyeurism
 - Cyber terrorism
 - Breach of confidentiality
 - Leakage of data by intermediary
 - E-commerce frauds
 - o Statutory reco to electronic contracts & deals w/ electronic authentication, digital signs, cybercrimes, liability of network service providers, etc
 - o Creation of Cyber Appellate Tribunal (merged w/ **TDSAT**)

Criminal Offences	Subsection
Sending offensive messages, including attachments, through communications service	66A
Dishonestly receiving stolen computer resource or communication device	66B
Identity theft	66C
Cheating by personating	66D
Violation of privacy	66E
Cyber terrorism: defined as causing denial of service, illegal access, introducing a virus in any of the critical information infrastructure of the country defined u/s 70 with the intent to threaten the unity, integrity, security or sovereignty of India or strike terror in the people or any section of the people; or gaining illegal access to data or database that is restricted for reasons of the security of state or friendly relations with foreign states.	66F
Publishing or transmitting of material containing sexually explicit act in electronic form	67A
Publishing or transmitting of material depicting children in sexually explicit act	67B
Preservation and retention of information by intermediaries as may be specified for such duration and in such manner and format as the central government may prescribe.	67C

- Issues
 - Doesn't address confidential information, data issue of corporates
 - 'spam' not mentioned anywhere
 - Max damage compensation capped at Rs. 5 crore - too little
 - Doesn't address jurisdictional issues
- **National Telecom Policy 2012**
 - Adequate measures by TSPs
 - TSPs must assist law enforcement agencies
 - Regulatory measures to ensure only safe-to-connect devices are inducted on network

Institutional Framework

- **NATGRID**
 - Integrated intelligence grid
 - Connects databases of core security agencies of Govt
 - Collect comprehensive patterns of intel, readily accessible
 - After 2008 Mumbai attacks
 - Accessible to 11 agencies - RAW, IB, CBI, CBDDT, CBEC, ED, FIU, etc
 - Challenge: lack of compatibility w/ datasets in regional Igs
- **National Cybersecurity Coordination Centre NCCC**
 - Cyberspace intelligence agency
 - Security, electronic surveillance
 - Concern: encroach on privacy
- **CERT-In India's Computer Emergency Response Team**
 - Mandated under IT Amendment Act 2008
 - Referral agency for responding to computer security incidents as & when they occur
- **CERT-Fin**
 - On reco of FSDC Financial Stability and Development Council
 - To tackle threats related to financial sector
- **NCIIPC National Critical Info Infrastructure Protection Centre**
 - National nodal agency
 - Protect, identify critical information infrastructure elements
 - Develop, execute national and international cooperation strategies for protection of CII
- **I4C Indian Cyber-crime Coordination Centre & Cyber Warrior Police Force**
 - Under CIS Cyber and Information Security Division of MHA
 - Cyber threats, child pornography, online stalking
- **Cyber Swachhata Kendra CSK**
 - By MeITy under Digital India initiative
 - Botnet cleaning, malware analysis centre
 - Coordinate w/ ISPs, industry
 - Tools

- M Kavach - anti-virus for smartphones, tablets
- USB Pratirodh - USB protector to clean external storage devices
- AppSamvid - whitelisting tool for desktop
- Browser JSGuard - block malicious JavaScript, HTML files
- Free Bot Removal Tool
- [Ground Zero Summit](#)

Other Measures

- Digital Army Programme
 - Dedicated cloud to digitize, automate procedures for Indian Army
 - Similar to Meghraj
- Cooperation w/ other cties

Challenges to Cybersecurity in India

- Structural
 - Rapid gr
 - Openness, connectivity by design; not ensuring security against unauth access
- Administrative
 - Lack of best practices, statutory backing
 - Yet to id, implement measures to protect CII
 - Appointment of National Cyber Security Coordinator (2014) not supplemented by liaison officers in states
- HR related
 - Understaffing in CERT-In
 - Attitudinal apathy of users
- Procedural
 - Lack of awareness in local police - IT Act 2000, IPC, etc
 - Push for cashless w/o capacity, awareness building on security of devices/ txns
 - Current IT Act inadequate to protect citizens' data in smart cities - huge volumes

Way forward

- Cyber command - armed forces + DRDO + experts
- Perception mgmt and social networks
- Capacity building, investment in R&D
- Legal aspects - needs trained personnel
 - Understanding use of cyberspace as 'force'
 - UN Charter implications
 - Negotiating int'l laws and treaties
- PPP models for CII
- Mech for info sharing and coordination b/w govt CERT-In & pvt sector thru Security Information Sharing and Analysis Centres
- Regulatory mechanism for protection of pvt sector CII, incentives for adherence to norms
- NASSCOM + govt - promote startups
- Int'l best practices
 - Tallinn Manual - laws applicable to cyber crimes, followed by dvped nations

Global Cyber Strategy

- UNGA regularly passes resolutions on info security

Need

- Stability of int'l & national security
- Social media - new medium for strategic communication bypassing national boundaries, authorities
- Global data transmission infra critically depends on undersea cables - highly vulnerable to accidents

Key Components

- No harm to National critical infrastructures
- ensure secure, stable and reliable functioning of the Internet
- Evolve common understanding of Internet security issues
- sovereign rights of national governments to make national policies on ICT consistent with international norms.
- Encourage global culture of cyber security based on trust and security
- The digital divide should be overcome.
- International cooperation should be strengthened.
- PPP should be encouraged.
- CIA (Confidentiality – Integrity – Availability) of information systems
- Balance between the need to maintain law and order and fundamental human rights should be maintained.
- obligations on states not to take any overt or clandestine measures which would result in cyber warfare.
- define what the use of force in cyberspace means and in what circumstances such force can be used, if at all.
- How would a state react if it is subjected to cyber attacks by a state, or a non-state actor, or by a combination of the two?

Pros

- Isolationist approach: no benefits of arising opportunities
- Treaties & conventions under development -> India can proactively engage in drafting them

Cons

- Tech control regimes undermining national sovereign interests of India - eg space, missile
- Biased in favour of major int'l players
 - o Eg European Convention on Cybercrime
- Need to develop own cyber capabilities to a level beyond ambit of control regimes

Global Initiatives

- **Budapest Convention 2001**
 - o **Only binding multilateral treaty** on cyber security that addresses Internet, computer crime
 - o Deals w/ copyright, computer related fraud, child pornography, violations of network security
 - o Focus on harmonising national laws, improving investigative techniques of legal auth, increase int'l cooperation
 - o Not signed by developing countries (incl India) -
 - developed countries drafted w/o consulting
 - India pushing for convention under UN framework
 - Contains provisions conflicting w/ our sovereignty
 - Provisions to override our Copyright Act
- **Ground Zero Summit**
 - o Largest collaboration platform in Asia for Cyber Security experts & researchers
 - o By MEA
 - o Corporate, PSUs, govt depts, security & defence establishments

- By IIC Indian Infosec Consortium - indep not-for-profit org
- **ICANN Internet Corporation for Assigned Names and Numbers**
 - Non-profit public benefit corporation
 - Global multi-stakeholder org
 - Coordinates Internet DNS, IP addresses, ASN Autonomous System Numbers, etc
 - Int'l, community driven org indep of govt; started in US govt
 - Collaborates w/ companies, individs, govts
- **Global Conference on Cyber Space GCCS**
 - India hosted 5th ed in 2017
 - To estb 'rules of the road' for behaviour in cyberspace
 - Setup - Global Forum on Cyber Expertise - to enhance capacity building, share best practices

Technology as facilitator of National Security

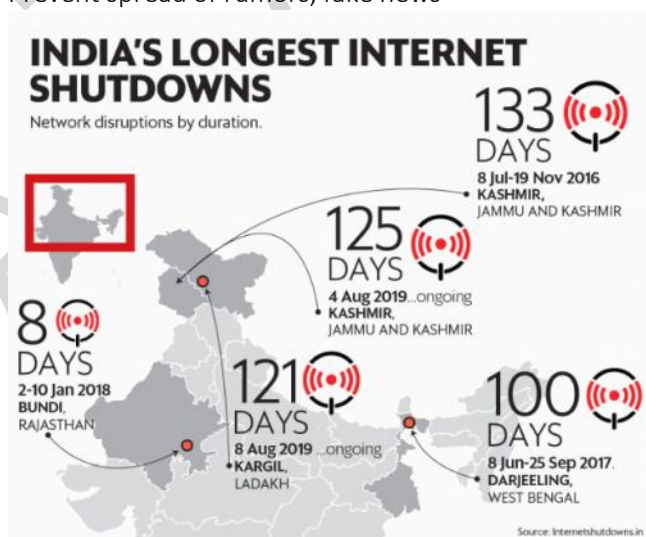
- Evidence collection: using forensic tech
- Intelligence gathering- using cyber technologies
- Surveillance- Drones, Radar, Sonar, Early warning systems
- Reconnaissance- GPS, Satellite data, autonomous vehicles
- Secure communications- encryption, cryptography
- Collaboration- NATGRID
- Nano Technologies- micro weapons, cameras, sensors, lighter ships, aircrafts, spacecrafts, etc
- Bio Technology- lighter food, lighter soldier uniform, better camouflage
- Artificial Intelligence- city surveillance using Machine Learning, Computer Vision, etc.
- Maintaining presence in Hostile environment- eg in Siachen

Internet Shutdowns

- India considered world leader in cutting off access to internet
- 134 instances in 2018; 2nd Pak - 12; total 196 globally

Why?

- To block flow of internet during civil unrest
 - About govt actions
 - End communication among activists
 - Prevent spread of rumors, fake news



How? - Legal Mechanisms

- Temporary Suspension of Telecom Services (Public Emergency or Public Safety) Rules 2017
 - o Home Dept in states; reviewed by state govt committee
 - o Centre also has powers under this; doesn't use often
- Sec 144 of CrPC
 - o DM, SDM, any exec magistrate
- Indian Telegraph Act, 1885
 - o Very infrequent use
 - o For public emergency, public safety, sovereignty & integrity of India, security of state, etc

Negatives:

- Economic cost
 - o ICRIER: \$3bn cost to economy over last 5 yrs
- Internet almost basic right in most cties
 - o SC: Right to Internet under Art 21
- No access to info, services -- could be difference b/w life & death
- UN 2016 resolution - non-binding
 - o Condemns countries that disrupt internet access to citizens

AADHAAR issues

- Positives- Easy tracking, Eliminate duplication of resources, robust social security
- Issues-
 - i. Fear of mass surveillance as AADHAR is linked to mobile numbers
 - ii. Issue of cyber security
 - iii. Financial security as AADHAR has been linked to PAN, Bank Account
 - iv. Not fool proof- illegal migrants getting aadhar
 - v. Aadhar Act has not defined National security (section 33) for which information can be revealed
 - vi. Only UID approach court, a citizen cant for a breach of his right
 - vii. Denial of social security services such as grains under NFSA due to technical reasons
- Recommendations-
 - o Concrete privacy laws- recent SC verdict which makes privacy part of Art 21 should be utilized
 - o IT laws should be modernized to handle privacy related issues by companies
 - o Include Aadhar database in the definition of CII
 - o Specialized team to deal with cyber-attacks on UID database
 - o Security testing of all Aadhaar based applications
- To overcome these challenges UIDAI has come up with Virtual ID and Limited KYC

AADHAAR ACT, 2016

- o The government has made Aadhaar mandatory for filing income tax returns; for obtaining PAN; for availing benefits under Mid-Day Meal; and also for verification of mobile phone connections.

What is Aadhaar?

- Aadhaar is a **12-digit number** issued by the **UIDAI** to the **residents of India**, however, it does **not confer any right of citizenship or domicile** in respect of an Aadhaar number holder.
- Any resident, **irrespective of age and gender** may **voluntarily enrol free of cost** to obtain Aadhaar.
- Aadhaar is **proof of identity, proof of residence and now also financial address for its residents**.
- **Data collected** includes:
 - ✓ **Demographic information required:** Name, Date of Birth, Gender, Address.

What is Aadhaar?

- Aadhaar is a **12-digit number** issued by the **UIDAI** to the **residents of India**, however, it does **not confer any right of citizenship or domicile** in respect of an Aadhaar number holder.
- Any resident, **irrespective of age and gender** may **voluntarily enrol free of cost** to obtain Aadhaar.
- Aadhaar is **proof of identity, proof of residence** and now also **financial address for its residents**.
- **Data collected** includes:
 - ✓ **Demographic information required:** Name, Date of Birth, Gender, Address, Parent/Guardian details (required for children, optional for adults), Contact details phone and email (optional)
 - ✓ **Biometric Information required:** Photo, 10 finger prints, Iris

Features and benefits of Aadhaar

- **Aadhaar has helped save government more than INR 49,000 crore in subsidies and more than 106 crore people have already been allotted Aadhaar till date.**
- **One Aadhaar:** As it contains biometrics which is **unique**, it helps in identifying fake and ghost beneficiaries in a government scheme, thereby helping in better targeting and stemming leakages.

Issues with Aadhaar

- **Privacy Issues:** Right to liberty and freedom of expression is compromised if right to privacy is not there. In the **absence of a comprehensive privacy law in India**, making Aadhaar **mandatory may lead to misuse of personal information and surveillance by the State thus taking away privacy**.
- **Release of Information:** Information of an individual can only be revealed in two cases:
 - ✓ **On the order of District Court**
 - ✓ **In the case of national security** on direction of a **"joint secretary"** (Section 33(2))
- **National security is a vague term** and these safeguards are **weaker** than those for telephone tapping as given in Telegraph Act, 1885 which allows sharing of data for **public emergency or public safety** and second, the order to share information can be issued only by Home Secretary.
- **Potential to profile individuals:** The Act does not have provisions to protect against determining of behavioural pattern and profiling of a person using big data analytics.
 - ✓ **It does not prohibit law enforcement agencies from using Aadhaar as a link across various datasets such as telephone records or air travel records**
 - ✓ **It does not prescribe maximum duration for which authentication record of an individual can be maintained.**
- **Section 57** enables the government to impose Aadhaar identification in virtually any other context that is not mentioned in the bill.
- **Cognizance of offence:** No court shall take cognizance of any offence except on a complaint made by the UIDAI. Thus, a person who is aggrieved by breach of data has no remedy at his/her disposal.
- **Discretionary powers of UIDAI:** The Act empowers UIDAI to specify other information that may be collected, **without prior approval** from Parliament.
- **No provision for public or independent Oversight:** The Act does not provide for independent oversight or limitations on surveillance.
- **Prosecution:** The Aadhaar Act does not make UIDAI liable for criminal prosecution in case of breach of data as per Section 43 of the Information Technology Act.
- **Compensation:** Unlike in western countries, the Act does not have any provision for compensation to the person whose data is compromised.
- **Authentication Failure:** In addition to wrong inclusion, exclusion of poor households, and misuse of biometric data, failure of biometric authentication stands approximately at 30 % **due to connectivity and other issues**.

Section 7 of the act says that Provided that if an Aadhaar number is not assigned to an individual, the individual shall be offered alternate and viable means of identification for delivery of subsidy, benefit, or service;

Women safety

20 June 2020 19:51

- Separate division setup under MHA in 2018
- Policy formulation, planning, coordinating, formulating, implementing projects/ schemes

CCTNS

ERSS (prev NERS)

Prison reforms

Anti-trafficking

Acid attack

Crimes against women

Devadasi system

" " children

Sc/st elderly

Zero FIR

SC, ST (prevention of atrocities) act, 2015

SHREYA SHREE
AIR 71 - CSE 2021

Organised crime & terrorism linkages

20 June 2020 18:55

[AS](#)

[TVS](#)

Terrorism

- No single universally accepted definition
- Political concept; difficult to frame a defn that excludes the state
 - o US, allies - fear - military interventions could be terrorism
- Acts committed w/ obj of seriously intimidating a population, destabilising or destroying structures of a ctry or int'l org or making a govt abstain from performing actions

Stats:

- Global Peace Index 2020
 - o India - 139/ 163 - among 25 least peaceful countries
 - o Our poor ranking due to internal conflicts, perceptions of criminality, political terror
 - o Nai Manzil scheme for Minorities - 2019 - Ministry of Minority Affairs

Causes

- Colonialism
 - o During anti-colonial struggle - due to brutal suppression, physical torture, cultural dehumanisation
 - o Eg Treaty of Sykes Picot (division of Arab lands under Ottoman b/w Brit, France - 1916)
- Fundamentalism - religion
 - o Sikh Khalistan
 - o Islam
- Organised crime and drug-trafficking
 - o Terrorist: ideological, political aims
 - o Organised crim: financial aims
 - o Same instruments
 - o Eg: Pak supplies illicit drugs in USA, funds Kashmir militancy with that money
- Increased availability, advancement in weapons
- Secessionism
 - o Emergence of micro-sovereign states after decolonisation
 - o Demands: Khalistan, Croatians in Yugoslavia, Tamils in SL
- Abetment by states
 - o UN Charter: prohibits use of force by states in reln w/ other states
 - o => proxy wars, support for military outfits
 - o Eg Pak
- Economic reasons
 - o Instability in dvping world
- Creation of USA
 - o Unilateral displays of power at WW2 end
 - o Denial of rights to Palestinians
 - o Denial of eco aid to poor nations
 - o Cold war politics
 - o Afghan mujahideen
 - o Deaf ear to India's warnings
 - o Destructive policy on Iraq

Types

- Repressive/ State Terrorism
 - o French Reign of Terror

- Revolutionary & War Terrorism
- Xeno-terrorism, Homo-terrorism
 - o Xeno: fight against foreigners for eg realignment of political bdaries
 - Not dependent on popular support
 - o Homo:
- Religion based terrorism
- Ideological - extreme right or left
- Nuclear
- Cyber
 - o Politically motivated; must instil terror
 - o v/s cyber crime
- Bio-terrorism
 - o Anthrax attack in USA
 - o Sarin gas attack in Tokyo subway
 - o Bio weapons: anthrax, smallpox
 - o Chemicals: sarin, Hydrogen cyanide, mustard agents

Steps

- Coordination
 - o NATGRID, NCTC
 - o Financial
 - Hawala, P Notes measures
 - o Border
 - CIBMS, etc
 - o Int'l
 - GCTF
 - UNSC res 2322, 1267
 - o Insti
 - NSG, NIA
 - o Laws
 - Anti hijacking
 - UAPA
 - o Offensive defence
 - Surgical strikes
 - o Cyber
 - Special: Operation Chakravayuh: IB scans web to keep tabs on radicalisation
 - o Minority schemes
 - USTTAD Upgrading the Skills and Training in Traditional Arts/ Crafts for Development
 - Nai Manzil

Way out

- National Security Doctrine
- Intel sharing
- Border
- Social media
- Financial
- Smuggling
- Coordination w/ community leaders to check against home grown religious terror cells
- Offensive policies
 - o HOT Pursuit: int'l law - state has a right to pursue a vessel belonging to a foreign state which has violated any law w/in its territorial bdaries/ jurisdiction
 - Exception to fundamental principle of freedom of the high seas - the rights of vessels of all nations to navigate freely on high seas
 - news: seizure of Pak vessel w/ huge cache of heroin off Gujarat

- Surgical Strike - Strategic restraint
- Int'l
 - Intel sharing eg HSPD-6 w/ USA
 - Push for CCIT Comprehensive Convention on International Terrorism
 - Pak based terrorists in 1267
 - Harmonise laws w/ 2322

International Cooperation

- FATF
- GCTF
 - Global Counter Terrorism Forum
 - 2011 - informal, apolitical, multilateral
 - 30 members - 20 cties + EU
 - **India also member**
 - Success: facilitated talks
 - Challenge: collab low in S Asia
 - Related: **GCTF Terrorist Travel Initiative** launched at UNGA
- **CCIT** Comprehensive Convention on International Terrorism
 - Proposed treaty to criminalise all forms of int'l terrorism,
 - Deny terrorists + financiers + supporters access to funds, arms, safe havens
 - Draft proposed by India - 1996
 - Yet to be adopted at UNGA
 - Calls for:
 - Universal defn of terrorism - no good or bad
 - Ban on all groups irresp of ctry of operation
 - Prosecution of all grps, incl cross border
 - Amend domestic laws - cross-border terror: extraditable offence
 - Pak's alleged support for cross-border terrorism in S Asia
 - Concerns
 - US + allies- defn
 - Latin American cties: int'l humanitarian laws being ignored
 - OIC: could be used to target Pak, restrict self-determination right of groups in Palestine, Kashmir, etc
 - Proposed amendments to accommodate concerns:
 - 'activities of armed forces during armed conflict' - will not be governed by the present convention
 - Insertion of word 'peoples' when speaking of rights, to 'acknowledge right of self determination'
- **UN SC Resolution 2322**
 - Harmonising rules
 - Int'l database
 - Extradition, state funding
 - Role of IT
 - Mutual Legal Assistance for Extradition
 - Checking return of terrorists after ISIS is defeated
- UNSC resol 1267
 - Against al Qaeda, related terror parties
 - Individ/ org in 1267 list -> movement restriction, financial penalties, assets freeze
 - news: Masood Azhar (JeM) designated global terrorist

Deradicalization

- Operation Chakravyuha
- **Operation Veerangana**

- Naga Mothers Association
- Community Leaders
- NCC in Madarassa
- International Cooperation
- Financial and Narco Linkage
- Database
- Empowerment
 - o Economic - USTTAD, Nai Manzil
 - o Social
 - o Political
- CASE STUDY - MAHARASHTRA deradicalisation program

Urban Terror

- Threat of terrorists applied to urban envi
 - o Directed at people
 - o Directed at infra
- Why?
 - o Easy targets: dense agglomeration, mass gathering
 - o Scope for anonymity
 - o Availability of facilities
 - o Easy recruitment
 - o Attacking credibility of govt
 - o Protection fm indiscriminate counter terror operation
- Way forward
 - o Cooperation among intelligence agencies
 - o Proper surveillance to penetrate network of sleeper cells
 - o Tech to detect, alert
 - o Training of counter terror operation

Organised Crimes Linkages

Aka **Black Hole Syndrome** - terrorists, organised crime groups show convergence to gain economic, political power over a region

Types

- Financial
- Trafficking, drug abuse
 - o Golden triangle, golden crescent
- Human trafficking
 - o Beggary, prostitution
- Contract killings, kidnapping for ransom
- Digital
- Smuggling
- Fake Currency
- Illegal arms trade
 - o To NE thru B'desh

Transnational Organised Crime

1. Hierarchical structure system of command
2. MO: Physical violence
3. Group specialized in many crimes simultaneously - human trafficking, drug, money laundering, terror financing, illegal arms smuggling, etc.
4. Public officials and legitimate businessmen are corrupted or intimidated

Challenges

1. Inadequate legal structure
2. Difficulties in obtaining proofs
3. Slow pace of trials and low conviction rate
4. Lack of resources and training
5. Lack of Coordination
6. Dual Criminality
7. Criminal, political and bureaucratic Nexus

Human Trafficking

- Defn: UN incl both sex trafficking and forced labour

- **India: signatory to UNTOC**

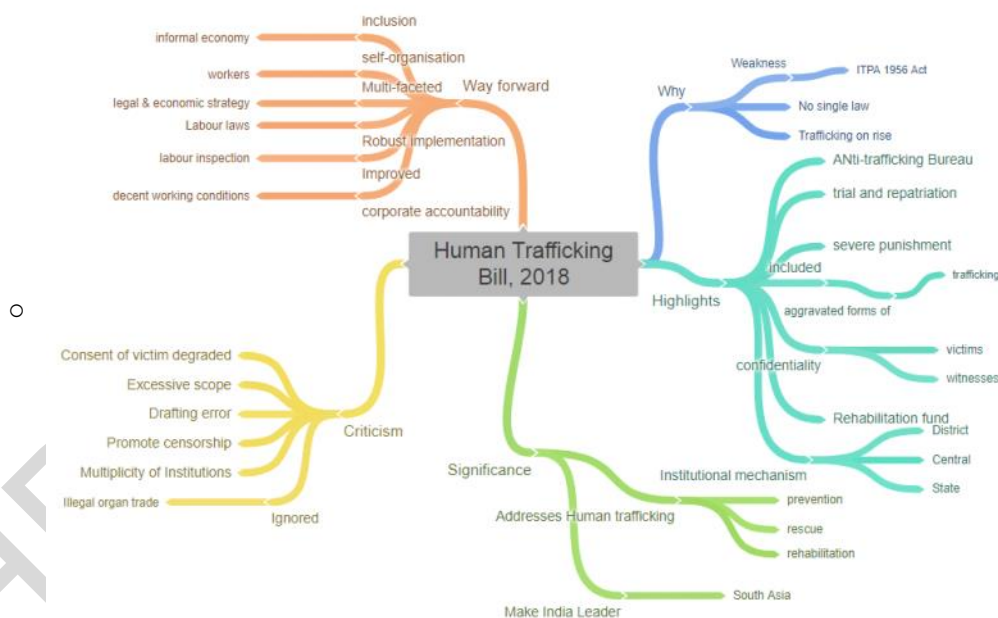
-

- Stats:

- o NCRB: human trafficking rose by ~20% in 2016 vis a vis 2015
- o Max WB, Raj; 70% female

- Constitutional, Legislative Provisions

- o Art 23(1) - prohibits trafficking in human beings
- o Human Trafficking Bill, 2018



- o ITPA 1956 Immoral Traffic (Prevention) Act - for commercial sexual exploitation
- o Substitution of Section 370 of IPC w/ 370 & 370A
 - Comprehensive measures to counter human trafficking
- o POCSO Act, 2012 Protection of children fm Sexual offences
- o Prohibition of Child Marriage Act (2006), Bonded Labour System (Abolition) Act 1976, Child Labour (prohibition and regulation) act 1986, transplantation of human organs act 1994, sec 372, 373 of IPC (buying/ selling girls for prostitution)
- o State govt legislations
- o Anti Trafficking Nodal Cell setup by MHA
- o MWCD - Ujjawala, Swadhar Program

- Factors

- o More reporting due to increased public awareness
- o Poverty -> trafficking in lure of good jobs
- o Porous int'l borders
- o FB, WA

- Collusion b/w BSF & traffickers
- Issues
 - Cross national victims victimised twice - illegal under Foreigners Act, 1946
 - Inadequate use of penal clauses
 - Delay in verification of address of victim
- Data issues
 - **World Vision** Report - prevalence data fm secondary sources DNE, no valid survey method as hidden popn
 - NCRB: parents hesitant to report/ themselves involved
 - No integrated data collection system - global data gap
- Int'l Collab
 - UNCTOC UN Convention on Transnational Organised Crime
 - SAARC Convention on Preventing and Combating Trafficking in Women and Children for Prostitution
 - Regional task force
 - AHTUs Anti Human Trafficking Units
 - Bilateral mechanism
- Measures
 - Capacity building
 - Judicial colloquium - to sensitise judicial officers, ensure speedy process
 - Accurate data to evolve effective strategies

Drug Trafficking

- **Need more!**
- UNODC UN Office on Drugs and Crime
 - India among major hubs of illicit drug trade; also transit point
 - Lies b/w two major illicit opium production region in world
 - Golden crescent (Iran - Afghanistan - Pakistan)
 - Golden triangle
 - Global trend: drug purchase on darknet using cryptocurrency (also in S Asia)
 - World Drug Report
- NDDTC National Drug Dependence Treatment Centre of AIIMS
 - Report on magnitude of substance use in India
 - Alcohol: 14.6% people; cannabis: 2.8%; sedatives (non-medical, non-prescription):1.08%
 - Treatment: inadequate availability
- National Policy on Narcotic Drugs and Psychotropic Substances 2014 (NDPS)
 1. Gradual reduction of consumption of poppy straw by addicts
 2. Use of satellite imageries for detection of illicit crop of poppy and cannabis
 3. Development of alternative means of livelihood for cultivators
 4. Allowing Private sector production of alkaloids from opium
 5. Adequate access to morphine for palliative care

Steps undertaken-

1. NDPS Act 1985
2. International UN conventions led by UNODC
3. MoUs with Thailand, Nepal, Myanmar, Joint working groups
4. National Policy on NDPS
5. Strengthening border security
6. Using technology

7. Rehabilitation of addicts

Fake Currency & terror financing

- UAPA
- TFFC Terror Funding and Fake Currency Cell
 - o Under NIA
- FCORD FICN Coordination Group
 - o By MHA w/ FinMin, RBI, Security & Intel agencies of centre & states
 - o To share intel
- MoU b/w India & B'desh
 - o Prevent smuggling, circulation of FICN
- Training programmes for Nepal, B'desh police
- Security at int'l borders
 - o New surveillance tech
 - o Additional manpower for round the clock surveillance
 - o Estb observation posts
 - o Erection of border fencing
 - o Intensive patrolling

Money Laundering

- Transformation of illegally gained money/ proceeds of crime into legitimate money, assets
- Eg: shell companies, hawala, round tripping, false invoicing, bulk cash smuggling, etc
- IMF: global money laundering ~2-5% of world GDP
- Impacts:
 - o Economic
 - Undermines legitimacy of private sector
 - Undermines integrity of financial markets
 - Loss of control of economic policy
 - Economic distortion and instability
 - Loss of revenue
 - Security threats to privatisation efforts
 - Volatility in exchange rates and interest rates due to unanticipated transfers of funds
 - Rise of economic prices
 - Affects trade and international capital flows
 - o Social
 - Increased criminality - drug trafficking, smuggling, corruption, etc
 - Decreased human devpment
 - Misallocation of resources
 - Affects trusts of local citizens in domestic fin inst
 - o Political
 - Initiates political distrust, instability
 - Criminalisation of politics
- **Legislations/ steps**
 - o FEMA
 - o PMLA 2002
 - Comprehensive legislation for money laundering; provides for confiscation of property derived fm money laundering
 - Applicable to all financial insti - banks incl RBI, mutual funds, insurance companies, financial intermediaries
 - Not effective
 - o PMLA Amendment 2012

- Adds 'reporting entity'
- Removed upper limit of fines
- Provisional attachment, confiscation of property of any person involved in such activities
- Financial Intelligence Unit - IND
 - Indep body
 - Reports to EIC Economic Intelligence Council headed by FM
- ED
 - Law enforcement, economic intelligence agency
 - Fn: investigate offences of money laundering under PMLA
- Smugglers and Foreign Exchange Manipulators (Forfeiture of Property) Act, 1976
- Narcotic Drugs and Psychotropic Substances Act, 1985

Proposals to increase effectiveness

- Make money laundering a separate criminal offence, thus separating the conviction in PMLA offence from conviction in predicate offence. ED investigates such issues.

Amendments brought-

- Disclosure of Information- false custom declaration included under PMLA
- "Proceeds of Crime" definition amended, where assets located abroad cannot be forfeited, equivalent assets within India will be taken over
- a claimant who has suffered due to ML will be compensated through confiscated assets
- Corporate Frauds included as Scheduled offence.
- Provisional attachment order powers to adjudicating authority
- Further Amendments through Finance Act 2018
 - Amendment to proceeds of crime definition to even include foreign assets to allow confiscation of assets outside the country
 - Uniformity in bail conditions irrespective of scheduled offence provisions
 - Corporate frauds included as scheduled offence
 - Compensation to claimant during trial if Special Court thinks it fit
- Mehul Chouksey, Vijay Mallya

- International:

- **FATF Reco**
 - countries should have anti-money laundering policy and should designate an authority that is responsible for such policies.
 - Enable competent authorities to confiscate property.
 - Ensure that financial institution secrecy laws don't inhibit implementation of these measures
 - Prohibit financial institutions from keeping anonymous accounts
 - Provide mutual legal assistance in relation to money laundering

Why FATF is effective while often UN is not?

- **Consensus based** model without any veto unlike UN. Therefore, more acceptance
- **Naming and Shaming policy** works well in Finance as it impacts credit rating, cost of financing, etc
- Clear and **Effective guidelines with measurable compliance** so easy to identify those who are not following. Its based on technical parameters
- It scrutinizes not just laws but also implementation, eg Pakistan was put on Gray List
- APG Asia Pacific Group on Money Laundering
 - Regional affiliate of FATF
 - Placed Pak in Enhanced Expedited Follow up List (Blacklist)
- Vienna Convention - 1988
 - UN Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances

- Obligation for signatories to criminalise laundering money from drug trafficking
- 1990 Council of Europe Convention
- G-10's Basel Committee statement of principles
 - Customer due diligence for banks
 - Sharing of financial records between jurisdictions to fight terrorist financing
- IOSCO Int'l Org of Securities Commissions
- IMF
- UNODC

- **Challenges-**

1. Technology- anonymous digital transactions. Bitcoin
2. Non fulfilment of the purpose of KYC norms
3. Collusion of bank officials in frauds
4. Borderless offence
5. Tax havens-

Participatory Notes

- Overseas derivative instruments with Indian stocks as underlying assets
- Allow foreign investors to buy stocks listed on Indian exchanges without being registered
- Concern: beyond reach of Indian regulators
 - Potential for laundering, stock price manipulation
 - Major chunk invested through tax haven: Cayman Islands

Borders - security challenges, mgmt

18 June 2020 17:02

Also see later [AS borders](#)

15,106.7 km land borders

7516.6 km coastline, incl island territories 🇮🇳

Border Mgmt:

- Defending borders + protection of interests of ctry on aligning borders

Dept of Border Mgmt in MHA

- Mgmt of int'l land, coastal borders
- Strengthen border policing & guarding
- Creation of infra - roads, fencing, flood lighting
- Implementation of BADP

Issues:

- Hostile elements: access to latest tech, money, organisational strength, manoeuvrability, wide choice for theatre of action, strategic alliances
- No proper demarcation of maritime, land borders
- Artificial bdaries -> difficult terrains -> extremely porous
- Multiplicity of forces on same border -> coordination!
- Lack of infra, equipment, manpower
- Discontent among local people due to harsh anti-terrorism measures - leveraged by hostile elements
- Cross border terrorism
- Illegal migration
- Sporadic aggression on China border
- Cross border safe houses for insurgent in NE neighbours
- Smuggling - arms, explosives, narcotics, counterfeit currency
- Increase in smuggling, piracy, breach of coastal security instances

Recos:

- Use of advanced tech - satellite, aerial imagery to reduce physical deployment
- Aerial surveillance - helicopter units - to improve ability to move troops to quickly occupy defensive positions
- BSF responsible for settled borders, Indian Army for unsettled borders
- Effective control - single point control/ one-force-one-border principle
- Comprehensive long term planning for deployment of CPOs Central Police Organisation
 - o Fire-prevention approach rather than fire-fighting
- Enhancing operational effectiveness
 - o All para-military forces managing unsettled borders directly under control of army

Need for participative and multi-national integrated border mgmt system

Involvement of stakeholders:

- Community participative border mgmt, sensitive to varied cultures
- Community dvpment by Border Guarding Forces - to earn goodwill
- Enhancement of border trade
- Employment opportunities locally
- VVFs Village Volunteer Forces - helping in border mgmt

Madhukar Gupta Committee

- Replace 'linear security' by 'grid border protection' along Pak border
- Better coordination by BGF w/ local police

- Intel generation

Initiatives:

- BADP
 - o Under Dept of Border Mgmt, MHA
 - o Through state govts
 - o to meet the special development needs of the people living in remote and inaccessible areas situated near the international border
 - o to saturate the border areas with the essential infrastructure through convergence of Central/State/BADP/Local schemes and participatory approach.
- Integrated Check Post
 - o ICPs are envisaged to provide all the facilities required for smooth cross-border movement of individuals, vehicles and goods under an integrated complex.
 - o integrated 3 main border related functions
 - customs, immigration and border security
 - o Operational ICPs:
 - Attari in Punjab (Pakistan border),
 - Petrapole in West Bengal (Bangladesh border),
 - Akhaura in Tripura (Bangladesh),
 - Raxaul in Bihar (Nepal),
 - Jogbani in Bihar (Nepal),
 - Moreh in Manipur (Myanmar).
 - o "in principle" approval has been granted for the setting up (ICPs) at 10 other locations.
- LPAI Land Ports Authority of India
 - o Statutory auth
 - o Setup to oversee, regulate construction, mgmt, maintenance of ICPs
 - o Vested w/ powers on the lines of Airports Authority of India



China

3488 km long
 J&K, Himachal, Uttarakhand, Sikkim, Arunachal
 Entire bdary disputed - McMahon Line
 Guard: ITBP

Challenges:

- Smuggling

- Inadequate infra
- Border disputes
 - o Western Sector: Aksai Chin
 - 1865 Johnson Line
 - 1890 Macartney-Macdonald line
 - India uses Johnson line; China hasn't clarified their position
 - o Galwan Valley dispute 2020
 - o Eastern Sector: Arunachal Pradesh
 - Shimla Accord 1913-14
 - McMahon Line - not accepted by China as border w/ India
 - McMahon accepted as border w/ Myanmar by China
- Numerous agencies: ITBP, Special Frontier Forces, Assam Rifles, Indian Army, proposed Sikkim Scouts; Chinese side entirely by PLA, single commander of Tibet Autonomous Region
- CPEC China Pakistan Economic Corridor
- Intelligence failures
- Water disputes:
 - o China recently cut off flow of a tributary of Brahmaputra to build a dam
 - o Work on dam on another Brahmaputra tributary - to create series of artificial lakes
 - o 6 mega dams on Mekong river - effect visible in SE Asia
- o Recent border tensions in Ladakh, North Sikkim
 - o At Pangong Tso Lake area - b/w PLA and IA - at Galwan River valley
 - o Reasons:
 - o Infrastructure development by India across LAC
 - o Plans to complete feeder roads to LAC by 2022
 - o Reorganisation of J&K
 - o Growing India-US bonhomie
 - o Use of diversionary tactics by China
 - o Shadow of Doklam episode -- India's strong opposition to China not taken well by the neighbour

Initiatives

- Border Talks
 - o High level border talks 1981-87
 - o Joint Working Group 1988
 - o Agreement on Maintenance of Peace and Tranquillity along LAC 1993
 - o CBMs in Military field along LAC 1996
 - o 2 special reps to find political soln - 2003-09
 - o NSA Ajit Doval appointed Special Envoy for talks
 - No soln so far
- Construction of roads along India-China border
 - o Close to completing major upgrade of border roads,
 - o Military use road connecting airfield at Daulat Beg Oldie in northern tip of western sector with villages of Shyok, Darbuk toward south
 - o BS-DBO road reduces travel time by 40%; facilitates lateral movement of Indian forces along western sector
- Spy Cam Project
 - o Failed - high-velocity wings, frost blurs images
 - o Cameras w/ 20-25km range at 50 locations in Himachal, J&K, Sikkim, Tawang

Way Forward

- Battle ready troops at all times
- Logistics organisation
- Transfer security and surveillance to Ministry of Defence - nodal agency
- ITBP shouldn't be used by MHA for internal security duties (eg Naxals)
- Water disputes
 - o Improve diplomatic communication, greater transparency by year round sharing of data on infra dypment

- Effective, innovative frameworks of resource mgmt including all stakeholders
- De-emphasise China's role for the time being, re-strengthen relationship w/ lower riparian countries, incl B'desh
- Restore image as responsible upper riparian

Pak

3323 km

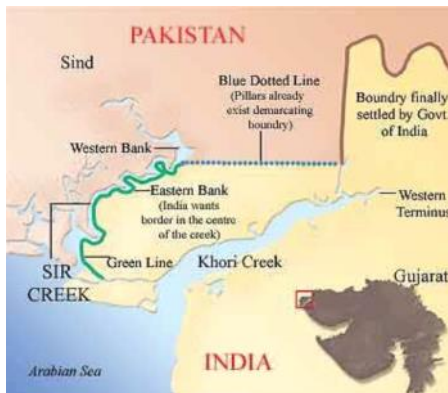
Extreme climatic conditions

3 categories

- 2308 km - Radcliff Line - Gujarat to Jammu
- 778 km - LoC/ Cease fire line - Jammu, Rajouri, Poonch, Baramula, Kupwara, Kargil, Leh - 1948, 71 wars
- 110 km - AGPL Actual Ground Position Line - NJ 9842 to Indira Col (Siachen Glacier)

Challenges

- Sir Creek



- Siachen



- River Disputes
 - Kishanganga Hydel Plant
 - Indus Water Treaty 1960!
- Cross border firing, border skirmishes, constant tension
- Repeated infiltration by Pak supported terrorists into India - proxy war
- Illegal activities - smuggling, drugs, arm trafficking, infiltration - porous borders, difficult terrain

Initiatives

- Fencing
 - Double row fenced - almost all border by 2011 - J&K, Punjab, Raj, Guj
- Use of tech **CIBMS Comprehensive Integrated Border Mgmt System**
 - 5 layered elaborate integrated setup
 - CCTV
 - Thermal imagers & NVDs

- BFSRs
- Underground monitoring sensors
- Laser barriers
- 50,000 flood lights - can be seen from space at night
- Outposts
 - 70,000 outposts, 1 ICP @ Attari, Amritsar
- Optimal utilisation of Waters of Eastern Rivers of Indus River System

Way Forward

- Prompt, appropriate compensation to border popn to stem dissatisfaction
- Study, check patterns of illegal activities
- **Task Force on Border Management (year)**
 - Under Madhav Godbole
 - Inherent problems: disputed status, artificiality, porosity
 - Recos
 - Resolve pending border disputes
 - Do NOT deploy border-guarding forces for other internal security duties
 - Estb Marine Police Force, strengthen Indian Coast Guard, setup apex insti for coordinating maritime issues
 - Accelerate dvpment of border infra, esp to wean border popn fm illegal activities

Nepal

1751 km

Uttarakhand, Uttar Pradesh, Bihar, West Bengal, Sikkim

Open border

Landlocked country, closes access to sea through India

Challenges

- Pak using open border to carry out anti-India acts - terrorists, FICN
- Fear of Maoist insurgency, links w/ Maoist groups in India
- Issue of land grabbing - by both sides
- Easy escape & illegal activities - insurgents, terrorists, hard-core criminals

Initiatives

- 25 battalions of Shashastra Seema Bal under MHA
- Bilateral talks - Home Secy level, Joint Working Group at Joint Secy level
- Border District Coordination Committee
- Construction of Indo-Nepal border roads

Bhutan

Completely demarcated except along tri-junction w/ China

Border defined by foothills

Friendship treaty w/ Bhutan - re-negotiated in 2007

Challenges

- Border dispute - at tri-junction
 - Doklam plateau - leverage to choke India's 'Chicken Neck' - Siliguri corridor
- Insurgents, criminals
 - Operation All Clear by Royal Bhutanese Army drove out Bodo, ULFA insurgents
- Smuggling
- Free movement of people & vehicles - sought by Bhutan once they enter Indian territory
- Migration - poor Indians work as construction labour in Bhutan
- Environmental concerns

Initiatives

- Deployment of forces
 - o Sashastra Seema Bal, BSF
- Bilateral cooperation
 - o Secy level bilateral mechanism: India-Bhutan Group on Border Mgmt & Security
- Road construction

Bangladesh

WB, Assam, Meghalaya, Tripura, Mizoram
 Heavily populated, cultivated upto border
 54 trans-boundary rivers

Best Examples of Border Management

- 100th CAA - issue of enclaves
- Sharing of Ganga water thru 1996 Agreement
 - o B'desh concerns over Farakka Barrage - diverts water to Hooghly
- Maritime disputes
 - o 2009: B'desh arbitral proceedings for delimitation of maritime bdary w/ India under UNCLOS - dispute settle in 2014

Outstanding issues

- Teesta River water dispute
- Tipaimukh Hydel Power Project on Barak R
- Illegal immigrants fm B'desh due to porous border
- Border fencing issue
 - o Riverine/ low-lying areas
 - Frequent course shifting
 - Floods uproot border pillars
 - o Population residing w/in 150 yards of border
 - o Pending land acquisition cases
 - o Protests by border population -> delay in completion
- Unauth cross-border trade despite strict trade regulations, barriers- jamdani sarees, rice, salt, diesel
- Cattle smuggling and killing of smugglers
 - o BSF given only non-lethal weapons -> attacks on BSF personnel now

Initiatives

- Deployment of force: BSF
- Fencing: barbed wire fence, improved lighting
- **Border Protection Grid**
 - o Multi-pronged, fool-proof mechanism
 - o Physical barriers, non-physical barriers, surveillance system, intelligence agencies, state police, BSF, other state & central agencies
- Road construction, border mgmt dept
- Strengthening vigilance and regulation
- Bilateral cooperation
 - o MoU on Prevention of Human trafficking, Smuggling, circulation of FICN
 - o MoU to prevent crimes at sea - b/w Coast Guards of India & B'desh
 - o Sundarban Moitry/ Alliance -- joint exercise
 - o Joint patrols, info sharing

Digression - Issues in Assam

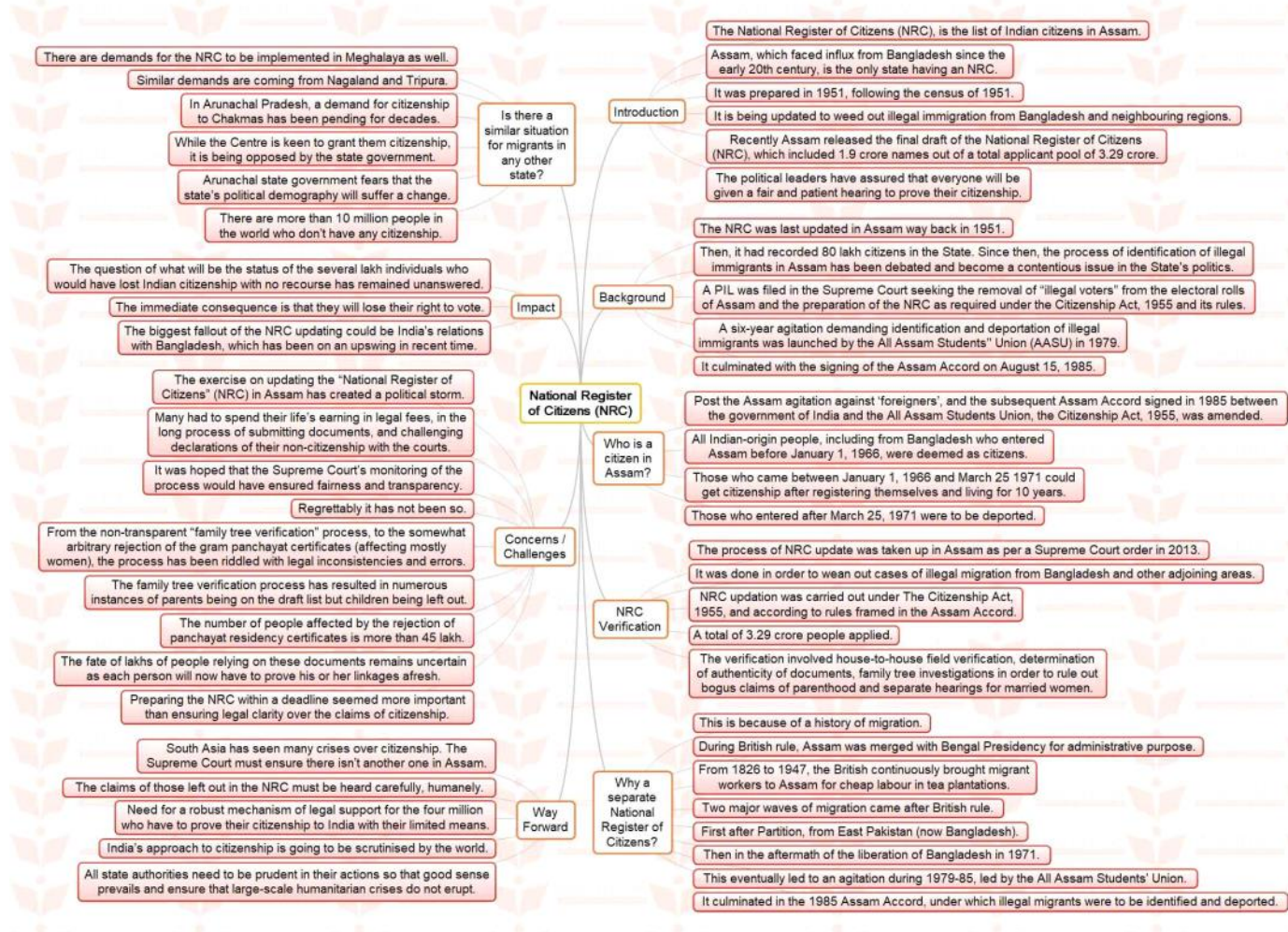
Steps:

- Sealing of Assam part of border ongoing
- Use of tech soln

- Piece-meal approach - Assam only small part of total border
- Other states not as much anti-migrant sentiment

[more on this here](#)

NRC



Myanmar

1643 km

Arunachal, Nagaland, Manipur, Mizoram

Free Movement Regime (FMR) for border tribes upto 16km across border

- Insurgents taking adv of FMR

Challenges

- Rugged terrain
- Weak vigilance - no physical barrier
- Insurgency - poorly guarded border, safe havens by tribes
- Drugs menace
 - o Edge of Drugs golden triangle
 - o Entry thru Moreh, Manipur
 - o Heroin, ephedrine, pseudo-ephedrine
 - o Trafficking of women, children
- Boundary dispute
 - o 1967 Boundary agreement - didn't crystallise on ground
 - o 2013: dispute b/w BP No. 79 to 81 - 10km long - Manipuris claimed it was several m inside Indian territory -> loss of land
- Lack of attention
- Lack of support from military junta govt in Myanmar

Initiatives

- Deployment of force: Assam Rifles
 - o 31/46 battalions for counter insurgency
 - o 15 battalions for guarding border
- Panel to study FMR
 - o Being misused for smuggling
 - o Porous borders used to mobilise cadres
 - o NSCN-K camps, bases in NSAZ
 - o China aiding this
 - o Policing difficult b'cos difficult terrain

What is Free Movement Regime (FMR)?

- The tribal communities, particularly Nagas, Singphos, Kukis, Mizos etc. claim that the boundary between India and Myanmar is inconsistent with the traditional limits of the region they inhabited and they still continue to have trans-border linkages with their kiths and kins.
- The FMR is thus an arrangement to alleviate insecurity of tribals living along India and Myanmar border.
- It permits tribes residing along the border to travel 16 km across the boundary without visa restrictions.
- While India allows Myanmarese nationals to stay 72 hours without visa, Myanmar allows stay of only 24 hours. To resolve this parallel discussions between the two governments have been going on.

Way Ahead

- Strengthen border security
 - o Either AR has ONLY border guarding mandate
 - o Or deploy BSF/ such guard force
 - o Revision of FMR, reduce permitted distance of unrestricted travel
- Issues:
 - Resentment among tribal popn on both sides
 - Eastern Nagaland in India
 - Naga Self Administered Zone in Myanmar
 - o Construction of ICP
 - o Meaningful engagement w/ Myanmar, cooperation

Sri LankaChallenges

- Katchatheevu Island - ceded in 1974
- Fishermen trespassing - strained bilateral ties

Initiatives

- Fishermen issue
 - o All big fishing trawlers being installed w/ AIS transponders
 - o Small fishing vessels - proposal to fit w/ RFID
 - o Uniform registration system for all fishing vessels
 - o Colour codes for easy id at sea - diff for diff states
 - o DATs Distress Alert Transmitters
 - o Subsidised kit of GPS, communication equipment, echo-sounder, search & rescue beacon
 - o Coastal security helpline numbers 1554 (ICG), 1093 (Marine Police)

Way Forward

- Sustainable fishing and alternate livelihood
 - o Reduce dependence on Palk Bay fishing
- Institutional mechanism
 - o Joint Working Group 2018
 - o Hotline b/w coast guards
 - o Meetings of fisheries ministers
- Joint patrolling by Indian Navy/ Coast Guard and Sri Lankan Navy

Coastal Security

7516 km

Coastline thru 9 states, 4 Uts

- Gujarat, Maha, Goa, K'taka, Kerala, Tamil Nadu, Andhra, Odisha, West Bengal
- Daman & Diu, Lakshadweep, Puducherry, A&N

Bay of Bengal

- Regional Geopolitics- Bay of Bengal is one of the largest and busiest chokepoints in the world that connects Indian Ocean and Pacific Ocean. It comprises of 22% of the global population and lies in the centre of two important economic blocks SAARC and ASEAN. The region also stays in attention due to the growing Chinese influence in the region. Almost one-quarter of world's traded goods and about 80% of energy requirement of China, South Korea and Japan flows through Strait of Malacca.
- Resource Exploration- It is rich in natural resources such as petroleum, hydrocarbons, poly metallic nodules, placer deposits of heavy metals etc. It is joined with Andaman and Nicobar Sea and Malacca straits are the link between south east and south Asia which is a major source of oil and natural gas producing area.
- Conservation- The places such as Andaman and Nicobar Islands, Palk Strait etc. are one of the high biodiversity areas which are crucial to conservation of biodiversity. The region has high potential for carbon sequestration due to presence of Mangroves (Blue Carbon).
- Maritime Security- The region has been lately very active as far as security engagements are concerned such as Malabar Exercise. The BoB is also significant to tackle crime related to human trafficking and terrorism as well.
- Development and Economic Integration- The BoB littoral states are mostly developing nations which have the lowest level of economic integration. At present less than 2% of world trade and very limited investment take place in the region
- Disaster Management – The region is highly prone to natural disasters such as cyclones. It is a strategically important area for **Disaster Risk Reduction** through monitoring and Early Warning Systems and engaging with other countries through regional exercises such as BIMSTEC DMEx 2017.

A&N Islands

- Coco Island(Myanmar) is very close to ANI and Chinese have constructed Air strip.
- 6 and 10 degree channel - more than 60k commercial vessels pass
- New Delhi established there its first and only tri-command (Army, Navy and Air Force) service in 2001- the command still faces turf wars, funding issues, and glacial decision making.
- A military presence in the Coco Islands, if truly established, would give China the edge to monitor India's naval activities with other powers in the region.
- infrastructure development on Coco Islands was completed in short order, and besides a radar station the Chinese have also built an airstrip. In contrast, India took ten years to decide to build a radar station on the nearby Narcondam Islands.
- Internet connectivity, even at the naval base in the capital Port Blair, is reported to be erratic.
- The destruction of the road by the tsunami has meant that the two groups of islands are linked only by air and sea



Challenges:

- Diverse topography - creeks, small bays, back waters, rivulets, lagoons, estuaries, swamps, mudflats, hills, rocky outcrops, sandbars, beaches, small islands
- Physically proximity of India's coast to politically volatile, economically depressed, unfriendly ctries - Sri Lanka, B'desh, Pak, Gulf ctries
- Unsettled maritime boundaries
 - o Security challenges
 - o Hinders offshore dvpment
 - Sir Creek, B'desh

Security, Threats:

- Maritime terrorism
- Piracy, armed robbery:
 - o By defn - piracy on high seas; not under ambit of coastal security
 - o Sundarbans - shallow waters - acts of violence, detention - ~to piracy
- Smuggling and trafficking
- Infiltration, illegal migration, refugee influx
 - o Led to widespread political turmoil in border states
 - o Measures: strict vigil, erection of fences, thorough checking of immigrants
 - o Strict on land -> migrants through sea - relatively lax measures
- Straying of fishermen beyond maritime boundary

Security Architecture

- **Customs Marine Organisation**
 - o On reco of Nag Chaudhari Committee
 - o Obj: suggest optimum assets reqd for anti-smuggling operations
 - o Merged w/ ICG in 1977
- **Indian Coast Guard ICG**
 - o Under Ministry of Defence
 - o Estd 1977
 - o Coast Guard Act 1978 - 4th armed force of India
 - o Ensure maritime zones' security, protect India's maritime & national interests here
- **Marine Police Force**
 - o Under Coastal Security Scheme 2005
 - o To strengthen infra for patrolling, surveillance of coastal areas
 - o Reqd to work closely w/ ICG
 - Hub and spoke concept

- Hub: ICG
- Spokes: coastal police stations
- Mandated to patrol territorial waters - 12 nautical miles

Presently

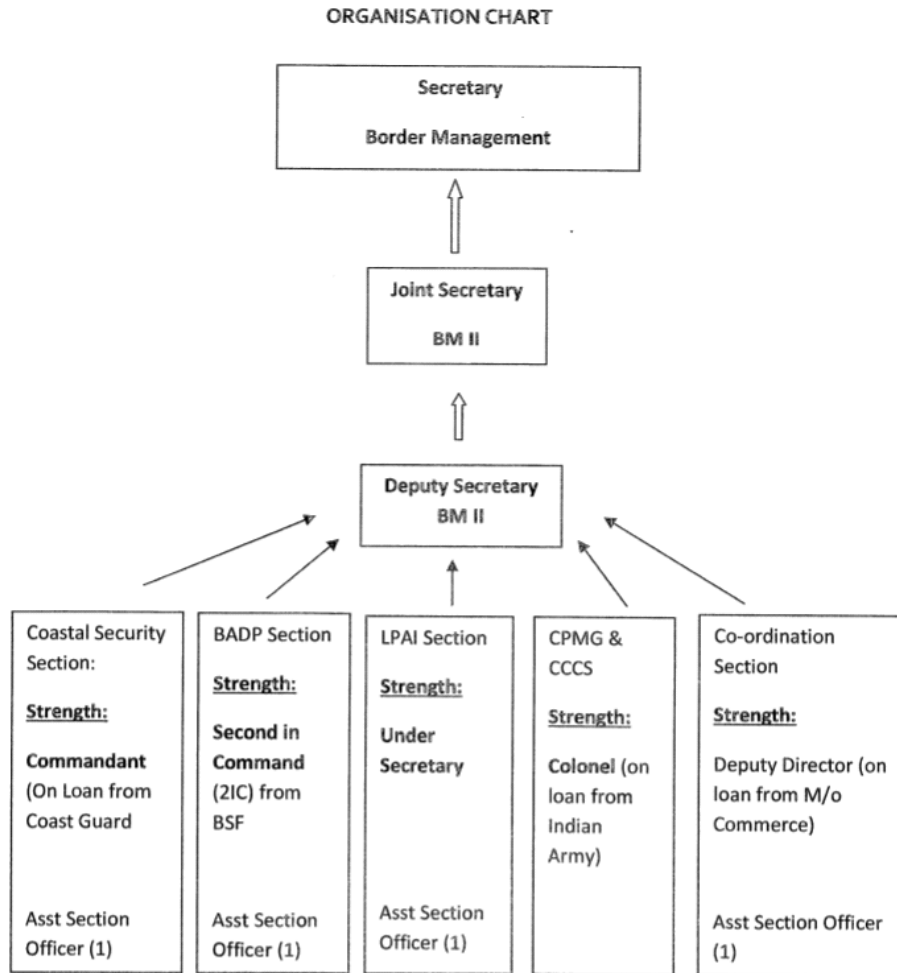
- Multi-tier arrangement
- Surveillance on high seas carried out along EEZ limits by Navy, Coast Guard
- Territorial waters: Coast guards - vessels, aerial surveillance
- Close coastal patrolling: by State Marine Police

Initiatives

- Coastal Security Scheme CSS
 - Strengthen surveillance thru AIS Automatic Identification System receivers, chain of overlapping coastal radars
- Coordination
 - Apex: **NCSMS National Committee for Strengthening Maritime and Coastal Security**
 - Headed by Cabinet Secy
 - Coordinates all matters related to maritime and coastal security
- **Joint Operation Centres**
 - Setup by Navy
 - Command and control hubs for coastal security
 - Manned 24x7
- Continuous Surveillance - Navy, ICG, Marine Police
- Modern technical measures
 - Chain of 74 AIS receivers
 - Chain of 46 coastal radars
 - 2nd phase ongoing
- **NC3I National Command Control Communication and Intelligence Network**
 - To enhance Maritime Domain Awareness
 - Over-arching coastal security network
 - Inputs analysed at **IMAC Information Mgmt and Analysis Centre @ Gurgaon**
 - Disseminates compiled Common Operating Picture for Coastal Security to all 51 nodes of Navy, Coast Guard
- Fishermen cooperation
 - ID cards issued - centralised database
 - Equipped w/ suitable equipments - vessel id, tracking
- Training to marine police by navy, CG
- Sagar Prahari Bal
 - Specialised force raised by Navy
 - To protect bases, adjacent vulnerable areas, vulnerable points
- Informal layer of surveillance comprising fishermen community
 - Formalised, activated in all coastal states
 - Aka Sagar Suraksha Dal
- Electronic surveillance
 - For gapless surveillance of entire coastline
 - Prevent intrusion of undetected vessels under coastal surveillance network project
 - Comprises Coastal Radar Chain, Automatic Identification System, VTMS Vessel Traffic Mgmt System
- Harbour defence and surveillance system
 - **IUHDSS Integrated Underwater Harbour Defence and Surveillance** at Mumbai, Vizag naval harbour
 - Designed by Israeli aerospace industry ELTA
 - Comprises Coastal Surveillance Radars, High Power Underwater Sensors, Diver Detection Sonars
 - Can detect, id, track, generate warnings for all surface, subsurface threats to harbour security

Way Forward

- Designate ICG as single auth responsible for coastal security
 - o Strengthen, train
 - o To be treated as border guarding force
 - o Include under MHA
 - o -> admin cohesion, revenue flow for ICG as indep entity
- Indian Navy to concentrate on developing blue water capabilities, defence of ctry during wartimes
- Training marine police - sea-faring, sea-policing, sea-navigation



Security forces + Mandate

20 June 2020 18:11

- Sashastra Seema Bal
 - under the aegis of the Ministry of Home Affairs
 - part of the Central Armed Police Forces (CAPF), along with six other
 - Others: Assam Rifles, BSF, CISF, CRPF, ITBP, NSG
 - Estd 1963 (aftermath 1962 Chinese aggression)
 - Deployed: Nepal, Bhutan borders
 - UK, UP, Bihar, WB, Sikkim, Assam, Arunachal
 - Declared Lead Intelligence Agency for these border areas
 - Coordinates w/ IB, RAW, MAC (Multi Agency Centre) of various agencies under Home Min
 - Responsibilities:
 - Security in border areas
 - Prevent trans-border crimes, unauth border entry/ exit
 - Civic action programme in area of responsibility

- [police](#) , [\(TJ\)](#)

- [AS](#)



Defence

23 June 2020 18:35

General

- Largest arms importer
- **SRI Self Reliance Index**
 - o 1992
 - o Developed by committee under APJ
 - o Target - 70% by 2005 (30% in 1992)
 - Pushed to 2027
 - Not achieved yet
- Paradox:
 - o We have created world class ICBM, inter planetary mission but severely lack in minor techs - assault rifles, bullet proof vests, snow boots
- CAG Report
 - o 10% indigenous in Dhruv helicopters (v/s 50% requirement)
 - o LCA indigenisation pegged at 70%; achieved only 30%
 - o Operational inefficiencies
 - o Delays
 - o Quality issues
- Vacancy - acc to MoD data
 - o 10k officers, 50k below officer rank - vacant
 - o Stress on serving men
- Women
 - o Now allowed in combat roles in all services
 - o Res for women in paramilitary and some state police forces (Bihar)
 - o --
 - o Art 14
 - o Presence in Army under military nursing scheme 1927, medical officer cadre 1943, women entry scheme
 - o 2015: Delhi HC - granted Permanent Commission for women; MoD, Navy for sexist bias, blocking women's progress
 - o Challenges
 - Physical reasons - practically not possible to put women in combat roles
 - Familial priorities - defined roles, compromising discipline
 - Patriarchal attitude of rural recruits in army - challenge leadership position held by women
 - Prejudices for women
 - o Benefits
 - Manpower
 - Tech
 - Urban warfare
 - Need for best people - irresp of gender
 - Women part of Indian freedom struggle - reflect struggling ethos
 - Rani Lakshmi Bai, Rani Gaidenliu, Kalpana in revolutionary activity in Chittagong
 - Advantage for military operation in internal security -
 - Better mgmt of AFSPA
 - Women empowerment - spill-over effect: literacy, health, employment in other sectors

- Tooth to Tail ratio T3R
 - o Ratio of combat soldier (tooth) to supply and support personnel (tail)
 - o Low in India (1:1.15) - must be reverse
 - o Reco of Shekatkar committee

Doctrines

- Sundarji Doctrine

- o Since 1984
- o 7 holding corps, 3 strike corps
- o Hold offensive till strike corps gave punitive response
- o Inadequate in 2001 - couldn't give military response - mobilisation of army slow
- o -> int'l pressure built against offensive
- o Defensive offense

- Cold Start Doctrine

- o After limitations of Sundarji doctrine were exposed
 - 2001 attack on Indian parliament
- o Offensive Defence
- o Doctrine to be put to use in case of a war w/ Pak
- o By Indian Armed Forces
- o Obj: launch a retaliatory conventional strike against Pak inflicting significant harm on Pak Army before any int'l community could intercede, but not in a way Pak would be provoked to make a nuclear attack
- o Incl limited, rapid, armoured thrusts w/ infantry, necessary air support
- o Deviation fm 1947's 'non-aggressive, non-provocative defence policy'
- o Official stance: denial of Cold Start Doctrine;
- o Pros:
 - Better capabilities to respond to terror incidents sponsored by Pak state actors
 - Prepares India on any responsive surgical strike w/o provoking nuclear escalation
 - Improves deterrence
 - Promotes self restraint on Pak
- o Cons:
 - Concern whether army can execute CSD - lack of ammunition
 - Justification to Pak for dyping Tactical Nuclear Weapons

- Joint Doctrine of the Indian Armed Forces JDIAF 2017

- o Surgical strikes will be formal part of India's retaliatory toolkit against terror provocations
- o Uses CMD Credible Minimum Deterrence instead of CD Credible Deterrence - 1st such doc
- o Shows separation of control of nuclear weapons b/w military, civilian authorities
- o Reveals preference for expeditionary, overseas operations
- o 'complete & effective inter-operability' w/ countries, big and small - logistics, intel collab b/w US, Japan, Australia, SE Asian

- Land Warfare Doctrine LWD 2018 [ref1](#)

- o In conjunction w/ JDIAF
- o 1st time discusses emerging tech in context of future warfare
- o Aims to institute deterrence thru punitive strikes at tactical level
- o Proactive strategy
- o Future force posture will be planned on assumption of worst-case scenario

- Acknowledgement of combined threat from China, Pak
- Departure fm single-front centric threat planning
- Clarity in identifying threat spectrum
- Use of IBGs Integrated Battle Groups to give effect to limited aims strategy
 - Structured on case-to-case basis
 - Composition depends on terrain
- Nuclear envi:
 - Continue to enhance capability to maintain 'tempo of operations'
 - -> conventional war-fighting by IBGs will continue even after nuclear threshold is crossed
 - Lack of clarity on what happens when threshold is breached - limited conventional obj/ full scale conventional operations
- So far: defensive at conventional level; defensive-offensive posture at tactical level
- Seeks to maintain escalation dominance
- Systemises surgical strikes to achieve deterrence by punishment
- At LAC
 - Need to be prepared for any escalation
 - Deliberate transgressions along LAC will be responded w/ resolute actions that cause minimal escalation in consonance w/ existing Agreements, Protocols
- Evaluation! (Pros, Cons)

Defence Planning Committee

- Estd 2018
- Chman: NSA National Security Adviser
- Permanent body
- To facilitate comprehensive & integrated planning for defence matters
- Mandate:
 - Prepare draft national security strategy
 - Strategic defence review, doctrines
 - Formulate international defence engagement strategy
 - Roadmap to build defence mfg eco-system
 - Strategy to boost defence exports
 - Prioritised capability dvpment plans for armed forces over diff time frames in consonance w/ overall priorities, strategies, likely resource flow
- Pros
 - Break silos, take integrated approach
 - Certainty in defence planning
 - Max outcome from scarce resource
 - Speed up defence acquisition w/ long term view
 - Evaluate foreign policy imperatives

Chief of Defence Staff

- Tenure not fixed; upper age limit 65 yo
- Suggested by Kargil Review Committee - 1999
- 4 star CDS, COSC chman - Naresh Chandra Committee 2011
- Single point military adviser to govt
- Coordinate working of 3 services
- Integration of land-air-sea operations thru eventual setting up of theatre commands
- Military advisor to PM led Nuclear Command Authority
- Direct command of tri-service organisations to handle space, cyberspace warfare

- Principal Military Adviser to the Defence Min; Permanent Chairman, Chiefs of Staff Committee (COSC)
- Member of Defence Acquisition Council, Defence Planning Committee
- Pros:
 - o Synergy among forces
 - o Slash wasteful expenditure

Integrated Theatre Command

- Reco of [Shekatkar Committee](#), Kargil Committee
- Joint command - army, air force, navy
- Resources of all forces commanded by a senior military commander
- Pros:
 - o Not answerable to individual services - free to train, equip, exercise command to make cohesive fighting force
 - o Logistic resources under commander's control - less time in mobilisation
- Cons:
 - o No occasion during actual war when 3 services haven't operated w/ considerable cooperation
 - o Faraway lands war, medium to high intensity wars - distant possibility
 - o Increased communication network - interaction b/w 3 orgs easy despite spatial distance
 - o Likely limited domain knowledge of integrated force commander wrt other 2 services
- Problems w/ current struct:
 - o None of the present 17 commands co-located; non-contiguous areas of operational responsibility
 - o 2 tri-service commands - 3 services' officers head by rotation
 - Strategic Forces Command SFC
 - ANC Andaman & Nicobar Command
 - o SFC: looks after delivery, operational control of nuclear assets
 - Integrated functional command rather than theatre command since no geographic responsibility
 - o Dd for other integrated functional commands - cyber, aerospace, special operations commands
- Other issues
 - o Lack of coordination
 - o COSC not very effective
 - o Requirement for battle preparedness
 - o Need for unified expert advice from military
 - o Civilian bureaucracy acting as interface
- Argument against
 - o India geographically not large enough, resources from one theatre can be easily moved to another theatre (Navy)
 - o Division of already scarce resources infeasible (Air Force)

Modernisation of defence

- Modernisation
 - o Modernising, upgrading existing equipment
 - o Buying, manufacturing new equipment
 - o Modernising military procedures, doctrines, etc
 - o Structure of higher defence - reln of military leadership among one another, w/ civilian govt

- Status
 - o Air Force fighter squadron at 60% of mandatory requirement
 - o Naval Submarine fleet dwindled to 40% of minimum requirement
 - o India is world's largest defence importer, with 60% of requirements met from outside. This sector has potential to boost manufacturing and create jobs
 - o Growing offensive capabilities of China is putting more pressure
- Budget allocation- at less than 2% of GDP. Salaries, pension takes up most of it.
- Procurement Issues-
 1. Corruption, Large unused funds and Multi-layer decision making process
 2. [New Defense Procurement Policy 2016](#)
 1. Eliminating repetitive procedures
 2. New category of Indigenous Designed Developed and Manufactured (IDDM) as most preferred category for procurement
 3. Buy, Buy and Make, and Make. Buy is further categorised as Buy IDDM, Buy Indian, Buy Global. Buy and Make is ToT
 4. Most components have been taken out from the list of defense products requiring Industrial License
 3. Defense Acquisition Council approved the long pending policy for blacklisting firms involved in corruption in arms purchases
 4. PSC on Defense supported MoD proposal of Non Lapsable Capital Fund Account
- **Strategic Partnership Model**
 - o DPP didn't list down criteria for selecting private Indian defense companies under SP model
 - o Proposal to grant all contracts of a particular military platform to a particular private firm
 - o Reasons for delay in finalization of SP model
 - Price is determined on a cost plus model however acquisition wing of ministry wants price discovery through competition
 - SP model may also face legal challenges from losing companies
 - May lead to monopolization
 - o SP model aims to create expertise in four key areas- fighter aircraft, helicopters, submarines and armored vehicles and main battle tanks
- Chief of Staff Committee in 2012 proposed creation of three new inter service divisions-
 - o Space Division
 - o Cyber space division
 - o Special Operation division

Indigenisation of Defence Tech

[more](#)

- Need
 - Reducing Fiscal Deficit
 - 2nd largest arms importer; after Saudi Arabia
 - 5th largest defence budget - 60% procured fm foreign markets
 - Can export
 - Security imperative
 - Tech expertise intact
 - Encourages spin-off tech
 - Employment generation
 - Creation of 100-120k highly skilled jobs in India

- Strategic capability
- Nationalism, patriotism
- Problem to upkeep, repair, overhaul and maintenance of the imported equipment due to low availability of spares and assemblies
- MRLS (Manufacturers Recommended List of Spares) leads to mismatch in demand and supply of defense equipment

- Issues

- Limited defence expenditure

- ~2% of GDP - mostly spent in salaries, pensions
 - Decreasing share
 - Only 25% on capital expenditure
 - Pak - 3.5%
- Parliament Standing Committee - we need min 2.5%
- Budget constraint -> halving the size of upcoming Mountain Corps on China border
- Defence Procurement Policy, 2016
- Strategic Partnership Model
 - Atre Committee
- Defence Innovation Fund
- Tech Transfer
 - Russia: Brahmos, 5th Gen Fighter Aircraft
 - US: DTTI - critical devices for aircraft carriers, drones; proposed F16 mfg
 - UK: Hawk Trainer Aircrafts
 - France: Scorpene
- Creation of Non Lapsable Capital Account Fund

- Cancellation/modification of tenders

- Over-ambitious - no company can do it

- Hierarchical, multi-layered

- Red-tape, corruption
 - Barak, Augusta Wetlands - corruption
- Financial powers of Defence Min to clear funds increased
 - Also for Defence Secy
- Defence Acquisition Council - **more!**
- **Need Defence Procurement Organisation**

- Cooperation w/ Private

- Raksha Udyog Ratna - couldn't succeed - trade union opposition, reservation fm firms over partner id method
- FDI to 100%, 49% under automatic
- Defence Procurement Policy, 2016
- Strategic Partnership Model
- Defence Innovation Fund
- Dhirendra Singh Committee Recos
 - MoD must plan expansion to private players in advance
 - Single window clearance for exports
 - Fiscal support - tax rebates
 - HRD:
 - ◆ University program for military engg
 - ◆ Industry MoD linked internship
- Need for Sovereign Fund (like USA)

- Raise FDI
 - Need \$100bn, currently <\$5mn
 - B'cos 49% doesn't allow to wrest control
- DRDO
 - Need to disaggregate - like in Israel
- Unused Funds
- Draft Defense Production Policy 2018
 1. Objectives-
 1. self-reliance in 13 identified areas by 2025 such as manufacturing of aircrafts, missile systems, small arms, land combat vehicles, etc.
 2. Increase domestic arms sales and export
 3. Make India as a global leader in Cyberspace and AI technology.
 2. Ease of Doing Business-
 1. Liberalization of licensing process, rationalization of taxation to support domestic startups and MSMEs
 2. Competency mapping of private defense industry
 3. Streamlining Make-II process of DPP 2016
 4. Increasing FDI Cap- allowing upto 74% in niche technology sector
 3. Intellectual Property cell creation
 4. Defense Industrial Corridors- in TN and UP
 5. Defense Export Organization to be setup jointly with industry
 6. Boosting Ordnance Factory Board and PSUs performance
- Promotion of Private Sector in Defense-
 1. Make II procedure under DPP 2016
 2. SPM
 3. Make in India
 4. 49% automatic FDI, and more through approval route on case by case basis
 5. Level playing field by removing anomalies on excise duty/ custom duty between private sector and public sector
 6. Rafale deal,
- [Self Reliance Index](#)

Military Agreements

--

Nuclear

24 June 2020 09:17

Nuclear Policy

AS

- Nuclear Doctrine
 - a. Building and maintaining a credible minimum deterrent;
 - b. A "No First Use (NFU)" posture; nuclear weapons to be used only "in retaliation against a nuclear attack on Indian territory or on Indian forces anywhere";
 - c. Nuclear retaliation to a first strike will be "assured", "massive" and designed to inflict "unacceptable damage".
 - d. Nuclear retaliatory attacks to be authorized only by civilian political leadership through the Nuclear Command Authority.
 - Nuclear Command Authority
 - Political council - headed by PM
 - Exec council - headed by NSA
 - e. Non-use of nuclear weapons against non-nuclear weapon states.
 - f. India to retain option of retaliating with nuclear weapon in the event of a major attack against it with biological or chemical weapon
- No First Use Policy-
 - Economic- need not spend on huge stockpile of Nuke and their maintenance
 - Diplomatic- international acceptance eg, NSG waiver
 - Wartime- onus of escalation on adversary but assured response acts as deterrent
 - Reduces probability of Nuclear war as India would not initiate it
 - Negatives-
 - NFU allows possibility of large scale destruction in first strike
 - Elaborate and costly ballistic missile defence
 - Doesn't hold in case of biological, chemical attacks
- Challenges to its relevance in current times-
 - Pak is going ahead with its tactical nuclear weapon program
 - Globally, very few countries adhere to NFU
 - Need of ambiguity for deterrence
- For NFU and CMD, to function effectively we require-
 - Sufficient and survivable nuclear force to inflict unacceptable damage on second strike
 - Operational preparedness at all times
 - Intelligence and early warning capabilities
 - Robust Command and Control System
- Revision of NFU - 2019
 - India's future commitment to posture of NFU 'depends on circumstances'
 - Points in favour
 - Priority to national security

- Can help underpin deterrence
- India can avoid the 'first casualty' if war were to break out
- India is the world's only country wedged b/w 2 nuclear-armed allies
- Points against
 - Might affect India-Pak reln
 - Might lead to instability in an already volatile envi
 - Announcements made w/o proper deliberation/consultation
 - Leaves India's nuclear doctrine more ambiguous
 - Moving away fm responsible nuclear
 - Self-proclaimed restraint -> basis for claims to belong in nuclear mainstream
 - Membership in Missile Technology Control Regime MTCR, Wassenaar Arrangement, Australia Group
 - Ongoing attempt to join NSG
- Related: K Subrahmanyam Board - dealt w/ India's nuclear posture, emphasised NFU

Disarmament-

1. 1988 Rajiv Gandhi proposed Action Plan to the Third Special Session on Disarmament
 - a. Binding commitment by all nations
 - b. All countries including all NWS must be part of this process
 - c. Tangible and verifiable processes at each stage
 - d. Accompanied by changes in global institutional framework to sustain a nuclear weapon free peaceful world
2. **NPT - 1970**
 - [lambi kahani](#)
 - 189 members
 - Non signatories: India, Pak, Israel, S Sudan
 - N Korea non-party after initially signing for it
3. **CTBT**
 - India not signed along with Pak and N Korea
 - US and China have signed but not ratified
 - Indian concerns
 - Discriminates against the non P-5 countries,
 - Is partial against countries like India that have recently acquired the tech,
 - Does not cover Electronic and Digital Tests,
 - Insignificance of role given the continue N Korea tests,
 - Does not provide a Time frame for complete Disarmament
 - Benefits of Joining
 - May help in acceding to NSG, Wassenaar, Nuclear deals, Provides Info from International Monitoring system (IMF) that will help to keep tabs on nations like Pak and it role in Global Peace and non proliferataion esp to terrorists
 - Conclusion - India voices its support for Disarmament, was one of the first countries to call for it in 1954, but is wary of doing it in a way that prejudices against other countries. Nonetheless, India has voiced its support for the proposed Fissile Material Cut Off Treaty that is expected to me fair in nature

4. **Fissile Material Cutoff Treaty FMCT -**

- proposed international treaty to prohibit further production of fissile material for nuclear weapons.
- Disagreement-
 - Regarding the definition of the term fissile material
 - Scope of the treaty (what materials, facilities and countries will be covered under the treaty)
 - Verification process: Many countries, particularly the non-weapon NPT countries, feel that without verification the treaty is really pointless

5. Treaty on the Prohibition of Nuclear Weapons 2017-

- first legally binding international agreement to comprehensively prohibit nuclear weapons, with the goal towards total elimination
- Prohibits parties from developing, stockpiling, using, threatening to use, acquiring, transferring, and stationing nuclear weapons and also assisting above processes.
- Adequate assistance to individuals affected by the use or test of nuclear weapon
- Over 120 countries in UN voted to adopt this treaty. India and other NWS did not participate in the negotiations
- India maintained that Geneva based Conference on Disarmament is the single multilateral disarmament negotiation forum
- International verification was essential to global elimination but current process didn't include that

6. NSG Nuclear Suppliers Group

- multinational body concerned with reducing nuclear proliferation by controlling the export and re-transfer of materials that may be applicable to nuclear weapon development and by improving safeguards and protection on existing materials.
- set up in 1974 as a *reaction to India's nuclear tests* to stop what it called the misuse of nuclear material meant for peaceful purposes.
- Currently, it has 48 members.
- Benefits of Joining
 - Trade
 - Free to buy nuclear fuel
 - India fulfils 40% of fuel by imports
 - Although, NSG has already granted a one time waiver, but is still needed because
 - Countries like Namibia reluctant to sell on account of non proliferation
 - ◆ Pelindaba treaty - ANWFZT African Nuclear Weapon Free Zone Treaty
 - Tech
 - NSG waiver led to exemptions in trade
 - But tech transfer is still difficult
 - Export nuclear tech
 - Military
 - Pak says as civil nuclear plants have enough Uranium, the homemade ones can now be used for the military set ups & will fuel arms race
 - But, Argument flawed as it is Pak which is becoming the obstacle in the ratification of Fissile Material Cut Off Treaty (FMCT)
 - ◆ To extend non proliferation aims
 - ◆ Since, NPT, NSG does not cover India, Pak, Israel
 - ◆ But, Pak opposing it

- Political
 - To deny Pak the membership as China is doing today
 - The waiver to India can be subsequently reversed by future amendments
- Information
 - Gets timely information on nuclear matters.
 - Contributes by way of information.
 - Is part of a very transparent process.
- Psychological
 - Precursor to UNSC
 - Turning full circle- NSG created to act against India and India itself desires to be its member shows its fulfilled utility
- Negatives of joining NSG
 - India will have to curtail nuclear weapon program since, India is a non nuclear weapon state as per the NPT
 - Or India will have to sign the NPT & acknowledge that we are not a nuclear weapon state
 - Allow Pak to join the NSG too to appease China
 - Be a 2nd class member in NSG, one with lesser powers likely
- India's arguments:
 - France in similar situation; was not a signatory of NPT when it was made a member of NSG
 - Plus, exemplary record of India
 - Affirmed by close cooperation with IAEA
 - India formed 6 nation 5 continent summit to put international pressure for disarmament
 - India has a voluntary moratorium on nuclear testing
 - Not joined CTBT
 - No first use policy
 - China only other ctry following an NFU doctrine

7. MTCR Missile Control Technology Regime

- Missile export restrictions for those with range > 300km and payload of 0.5 tonne
- 34 countries
 - 4 countries like Israel comply voluntarily
- India formally applied , but was denied a membership by Italian intervention
- Benefit
 - Access to better tech
 - India could get access to Javelin missiles, Predator UAC as credibility of India would increase
 - Can export missiles
 - Space
 - Earlier cryogenic engines restricted from Russia
 - Boost to GSLV
 - Stepping stone to NSG, UNSC
 - Leverage against China, Pak
 - China not a member of MTCR
 - India can use the mechanism to shove China into accepting India's inclusion before accepting China's entry into MTCR, since decision based on consensus
 - Similarly for restricting Pak entry
- Utility of MTCR
 - Limited
 - In spite of it, proliferation has happened to Pak, N

Korea via China

- Something better than nothing
 - Lately, American pressure has prevented China from proliferating again
 - MTCR forced Russia into not sharing GSLV tech with India

8. Hague Code of Conduct HCoC

- Against Ballistic Missile Proliferation
 - Primarily nuclear weapon delivery system; can carry any type of warheads
- India joined in 2016
- Voluntary, legally non-binding
- Supplements MTCR
- 137 members
 - China, Pak, Israel not members
- Restrained in prodn, dvpment, testing, deployment of missiles
- Benefits
 - Can pave way for MTCR - obstructed by Italy
 - Non-proliferation record - aid joining NSG, UNSC
 - Doesn't hamper existing Indian program
 - Imp part of Indo-US nuke deal
- Negatives
 - Will have to provide pre launch info on missiles, SLVs
 - Need to submit annual policy on launches
 - China, Pak not party

9. Wassenaar Arrangement

- To control conventional weapons and dual use technology
- India granted membership
- No China, Pak
- Benefits
 - It would provide us the critical dual use technology which has important ramifications in sectors like Space, Nuclear, Metallurgy, Microbiology, etc
 - Is critical to our entry to NSG
 - Recognition that India possesses critical technologies
 - It may allow India to restrict China and Pak which could provide us with bargaining power
 - Provides us the ability to exports
 - Provides us with advanced information
 - Eg Brazil provided critical radar technologies to Pak and we were caught unaware

- **Australia Group**

- Multilateral export control regime MECR
- For biological, chemical weapons
- Informal group of cties to help members identify exports that need to be controlled; not legally binding
- Response to Iran's 1984 use of chemical weapons
- India member; total 43

Nuclear Safety

- Nuclear Safety Summit in New York
 - India too a part
 - This one 4th
 - 1st in 2010
 - Though plagued by Russian absence
- International measures taken
 - Airports and sea ports have radioactive scanners
 - More security to fissile products
 - Coordination from IAEA, UNO, Interpol
 - Highly Enriched Uranium (HEU) enough to make 100 bombs have been moved to safeguarded sites
 - 13 countries HEU free
 - Nuclear Security Fund
 - India has contributed 1 million \$
 - Dedicated organisations like (have existed from before)
 - Global Initiative to Combat Nuclear Terrorism
 - Global Partnership against spread of WMD
- Vulnerability of India
 - According to a Washington based report
 - India's installations even less secure than Pak and China
 - Mostly because of corruption
 - India doesn't take the report seriously
 - India has also not signed the Nuclear Security Implementation Initiative (same with China, Russia and Pak)
 - Included peer reviews
 - National commitment
 - Steps India has taken
 - Database of all radioactive sources
 - Real time tracking of radioactive sources when they are transported
 - Permanent team of technical and security experts simulating exercises
 - In the process of equipping all major airports and seaports with radioactive detectors
 - No research reactor will use HEU
- Dirty Bomb: Mixing radioactive materials with conventional bombs just for radioactive leakage
- Reprocessing spent fuel
 - Separating plutonium out of the spent fuel
 - Can then be used to power reactors/ bombs
 - India actively pursuing this
 - Pro
 - Less reliance on imports

More

- CLINDA Act, 2010 Civil Liability for Nuclear Damage Act
 - Nuclear Liability law
 - Insurance pooling
 - Liability of operator in case of nuclear damage cause by nuclear incident or involving nuclear material coming from/ originating in that nuclear installation

- Not liable in exceptional natural disaster, acts of hostility/ civil war, terrorism
 - Liability of govt when liability exceeds amount of liability of an operator/ occurring in nuclear installation owned by it
 - Issues
 - Section 17(b) says that liability for nuclear accident can be channeled from operator to supplier, if accident due to supplier fault
 - Not clear in reality
 - India changing interpretation. Why?
 - ◆ India party to CSC Convention on Supplementary Compensation
 - ◆ Exec changing interpretation of CLINDA in support of nuclear suppliers
 - Section 46 says operators can sue the supplier under ordinary Tort Law
 - Sue amount only fraction of cost of nuclear plant
 - Why do we need onus on supplier
 - Fukushima - flaw in reactor design
 - \$200bn costs for radioactive cleaning - swept by taxpayer money -
 - Similar liability law in Japan - designer GE could escape
 - New nuclear plant proposed in Mithi Virdi - untested design
- Proposal for mega reactors
 - Location
 - Jaitapur- Maharashtra
 - Mithi Virdi - Gujarat
 - Kovadda - Andhra
 - Around 10k MW each
 - Total target of 63k MW by 2032
 - Though, has been revised now to about 27k MW
 - Challenges
 - New designs
 - Costs likely to escalate because of untested technologies
 - Same happened in US and France where costs escalated by nearly 50%
 - Safety factor
 - Enormous scale
 - Pro
 - Economies of scale
 - Con
 - Land acquisition problem
 - ◆ 13 villages near Jaitapur passed a resolution against the nuclear plant
 - Costs of construction
 - More risk involved
 - Delays
 - Narora took 20 years to be built
 - Uncertain future of Fast breeder reactor
 - Also leads to issue of Cost overruns
 - Political
 - Nuclear Liability Law
 - Nuclear deals incomplete

Heavy Water Reactor	Light Water Reactor
<ul style="list-style-type: none">❑ Fuel: natural Uranium❑ Coolant: deuterium oxide❑ By products: plutonium tritium (more amount)❑ Need frequent re-fuelling❑ Less heat generates	<ul style="list-style-type: none">▪ Fuel: enriched Uranium 235▪ Coolant: distilled water▪ By-products: plutonium, tritium▪ More energy per Uranium unit
Light water	Heavy water
<ul style="list-style-type: none">❑ Absorb more neutrons than needed❑ Enrichment of uranium fuel becomes necessary	<ul style="list-style-type: none">▪ Free neutron collide with hydrogen in the water - and slow down them▪ If water heated - expand - less dense - less collision - less slowing down▪ Thus, Heavy water heated with pressure in PHWR

SHREYA SHREE AIR 71 - CSE 2021

Indigenisation of Defence

Wednesday, June 24, 2020 12:45 PM

Clipped from: <https://www.drishtiias.com/to-the-points/paper3/indigenisation-of-defence>

[Prev](#) [Next](#)

- 14 Jun 2019
- 14 min read

What is Indigenisation of Defence?

- Indigenisation is the capability of **developing** and **producing** any defence equipment within the country for the dual purpose of achieving **self reliance** and reducing the **burden of imports**.
- Self-reliance in defence manufacturing is one of the key objectives of **Department of Defence Production**.
- **Defence Research Development Organisation (DRDO)**, **Defence Public Sector Undertakings (DPSUs)**, **Ordnance Factory Board (OFB)** and private organisations are playing a critical role in indigenisation of defence industries.

Background

- Overdependence on the Soviet Union, brought about a change in India's approach to **defence industrialisation** from **licence based production** to production based on **indigenous design**.
- From the mid-1980s, the government pumped resources into **R&D** to enable the DRDO to undertake high profile projects.
- A significant beginning in defence indigenisation was made in 1983, when the government sanctioned the **Integrated Guided Missile Development Programme (IGMDP)** to develop five missile systems:
 - **Prithvi** (surface-to-surface)
 - **Akash** (surface-to-air)
 - **Trishul** (the naval version of Prithvi)
 - **Nag** (anti-tank)
 - **Agni** Ballistic missiles with different ranges, i.e. Agni (1,2,3,4,5)
- In 1990 **Self Reliance Review Committee (SRRV)** under A.P.J. Abdul Kalam, had formulated a **10-year self-reliance plan** under which, the **self-reliance index (SRI)**, (defined as the percentage share of indigenous content in total procurement expenditure), was to be increased from 30% in 1992-1993 to 70 % by 2005.
 - This target has not been achieved till today.
- The indigenous efforts were not adequate to meet the requirements of the armed forces, this resulted in the shift of focus towards **co-development** and **co-production** in partnership with foreign companies.
- A beginning was made in 1998, when India and Russia signed an **inter-governmental agreement** to jointly produce **Brahmos supersonic cruise missile**.
- Apart from Russia, India has also partnered with other countries such as **Israel and France** for a number of projects.

Why Indigenisation?

- **Reducing Fiscal Deficit:** India is the second **largest arms importer** in the world (after Saudi Arabia).
 - Higher import dependency leads to increase in the fiscal deficit.
 - Despite having the **fifth largest defence budget** in the world, India procures 60% of its weapon systems from foreign markets.
 - India can export its indigeneous defence technology and equipment to the neighbouring nations.
- **Security Imperative:** Indigenisation in defence is critical to **national security** also. It keeps intact the technological expertise and encourages spin-off technologies and innovation that often stem from it.
 - Indigenisation is needed in order to avert the threats associated with the frequent **ceasefire violations** like that of the Uri, Pathankot and Pulwama attacks.
 - India being surrounded by **porous borders and hostile neighbours** needs to be self sufficient and self reliant in defence production.
- **Employment generation:** defence manufacturing will lead to the generation of satellites industries that in turn will pave the way for generation of employment opportunities.
 - As per government estimates, a reduction in **20-25%** in defence related imports could directly create an additional 100,000 to 120,000 **highly skilled jobs** in India.
- **Strategic Capability:** self sufficient and self reliant defence industry will place India among the **top global powers**.
- **Nationalism and Patriotism** can increase with indigenious production of defence equipment, that in turn will not only boost the **trust and confidence** of the Indian forces but will also strengthen a sense of **integrity and sovereignty** in them.

Government Initiatives

- **Defence Procurement Policy:** based on the recommendations of the **Dhirendra Singh committee**, Defence Procurement Procedure 2016 (replaced DPP 2013) added an additional category "**Buy (Indian-IDDm)**" i.e Indigenously Designed, Developed and Manufactured, as the most preferred way of defence goods acquisition.
 - DPP allowed the **Defence Acquisition Council** to take a "**fast-track**" route to acquire weapons, something which was limited to only the armed forces till now.
- **E-Biz Portal:** process of applying for Industrial License (IL) and Industrial Entrepreneur Memorandum (IEM) has been made completely online on ebiz portal.
- **Restriction of annual capacity** in the industrial license for defence sector has been removed.
- **Outsourcing and Vendor Development Guidelines:** for DPSUs (defence public sector undertaking) and OFB (ordnance factory board) to promote the participation of private sector, particularly SMEs (small manufacturing enterprises) for defence manufacturing.
 - The guidelines mandate that each DPSU and OFB to have a **short-term** and **long-term outsourcing** and **vendor development plan** to gradually increase the outsourcing from private sector including SMEs.

- The guidelines also include vendor development for **import substitution**.
- **Uniform custom duty:** In order to establish a **level-playing field** between Indian **private sector and the public sector**, all Indian industries (public and private) are subjected to the same kind of **excise and custom duty levies**.
- **The FDI policy:** composite foreign investment upto **49%** is allowed through Government route (FIPB) and beyond 49% with the approval of the Cabinet Committee on Security (CCS) on case-to-case basis.

- Restrictions such as **single largest Indian shareholder** to hold at least **51% equity** and complete restriction on **Foreign Institutional Investor (FII)** have been removed to facilitate investment in the sector.
- Preference to **'Buy (Indian)', 'Buy & Make (Indian)' & 'Make'** categories of acquisition over **'Buy (Global)'** category, thereby giving preference to Indian industry in procurement.

Present Scenario

- **INS Vikrant**, also known as Indigenous Aircraft Carrier 1 (IAC-1), is the first aircraft carrier to be built in India for the Navy.
 - It is expected to commence **sea trials in 2020**.
- **Tejas aircraft:** DRDO is not able to develop its indigenous Kaveri engine due to restricted access to high-end defence technology by countries such as USA, JAPAN etc.
- **Project75:** Indian Navy in 2017, initiated submarine programme called Project-75 (India), the **"mother of all underwater defence deals"** with France, Germany, Russia, Sweden, Spain and Japan to build six advanced stealth submarines.
 - Project 75 Submarines **INS Kalvari, INS Khanderi, INS Vela, S53, S54 and S55** are constructed by Mazagon Dock Limited and designed by French company DCNS in Mumbai.
- **Long-range artillery gun "Dhanush":** first indigenous long-range artillery gun also called the **"desi Bofors"**.
 - It has a strike range of 38 kilometres and **81% of its components** are indigenously sourced.
- **Arihant: first indigenous nuclear submarine** was developed in association with BARC and DRDO.
 - But due to insufficient fuel inventor it cannot go for long deployment and is in a need for further improvement.
- **AGNI V** has given India the status of ICBM (Intercontinental ballistic missile) holder country in 2013, though the project on integrated guided missile development was started in 1983.
 - Apart from **AGNI V**, Dhanush, Nirbhaya, Prithvi, Akash missiles have also contributed to indigenisation of defence.
- **The Pinaka Multi Barrel Rocket Launcher:** was developed by armament Research

Development Establishment (Pune).

- Pinaka is a precision system with **near zero-error probability**.
- **Supersonic Cruise Missile BRAHMOS**: is a Joint Venture between India and the Russian federation.
 - The Indian contribution is 50.5% and the Russian contribution is 49.5%
- **Arjun Tank** is a third generation main battle tank developed by DRDO.
 - DRDO is working on using composites to reduce the weight.

Facts and Findings

- According to the Stockholm International Peace Research Institute (SIPRI), **India was the world's second largest importer** of major arms in 2014-18 and accounted for 9.5% of the global total.
- According to the Stockholm International Peace Research Institute (SIPRI), India's military expenditure rose by 3.1%.
- In a **2011 report** to the Parliament, the Comptroller and Auditor General of India (C&AG) highlighted the 90% import dependency of Hindustan Aeronautics Ltd (HAL) for 'raw materials and bought out items' for the production of indigenous .
- India has been spending around **2.4% of its GDP** on defence.
- The **Self-Reliance Index (SRI)** which may be defined as the ratio of indigenous content of defence procurements to the total expenditure on defence procurements in a financial year is at an abysmal 0.3.

Challenges

- **Lack of an institutional capacity and capability** to take different policies aimed at indigenisation of defence to its logical conclusion.
- **Dispute Settlement body**: There is an urgent need for a **permanent arbitration committee** which can settle disputes expeditiously.
 - In the USA, the procurement agency DARPA has a permanent arbitration committee which resolves such issues amicably and their decision is final.
- **Infrastructural deficit** increases India's logistics costs thus reducing the country's cost competitiveness and efficiency.
- **Land acquisition issues** restrict entry of new players in the defence manufacturing and production.
- **Policy dilemma** offset requirements under the [DPP](#) are not helping it achieve its goal. (Offsets are a portion of a contracted price with a foreign supplier that must be re-invested in the Indian defence sector, or against which the government can purchase technology.

Way Forward

To ensure indigenisation of defence the government no doubt is heading in the right direction by laying emphasis on **"Make in India"**. It is the implementation that needs to be fine tuned. Some of the steps that can be taken in this direction are:

- **Permanent Arbitration Cell** can be set up to deal with all objections and disputes.

- **Private Sector boost** is necessary as it can infuse efficient and effective technology and human capital required for modernisation of indigenous defence industry.
 - The private sector must be allotted big ticket contracts in order to strengthen their confidence and reduce the **trust deficit between private and government sector**.
 - Ensure a **level playing field** for the private industry, DRDO, DPSUs and OFB.
- **Export capability:** If the aim is to achieve export capability, then the weapon system must first be in service with our armed forces.
- **Software Industry** and technologies like **Artificial intelligence and cyber security** should be used to develop and manufacture the “chip” indigenously.
- **Providing Financial and Administrative autonomy** to DRDO in order to enhance its confidence and authority.
- **Training and Tenure:** The staff at the **Department of Defence Production** need to be trained and given longer tenures to ensure continuity.
- **Investee Company** should be structured to be **self-sufficient in areas of product design and development**. The investee/joint venture company along with manufacturing facility should have maintenance and life cycle support facility of the product being manufactured.
- **In-house design capability should be improved** amongst the three services, the Navy has progressed well on the path of indigenisation primarily because of the in-house design capability, the Naval Design Bureau.
 - Hence, they do not have to depend on the DRDO for the design & development of the complete ship, but outsource the sub-systems for them to develop.
- **Robust supply chain** is critical for a defence manufacturer looking to optimize costs.
 - Indian SMEs are playing a key role in the global supply chain of OEMs (Original Equipment Manufacturer).

New Defence Acquisition Procedure 2020 NDAP

- Architectural continuity with DPP 2016
- Important
 - System of classification of capital procurements to promote indigenous design & development (D&D)
 - Multi-stage procurement cycle
 - Bespoke procedures for certain types of procurement
 - Standardisation of tender & contract documents
 - Offset
- 5 new chapters deal with 5 aspects hitherto lacking proper guidelines/ dealt in an ad-hoc manner
 - Procedure for acquisition of systems designed by DRDO/ DPSU/ OFB
 - Acquisition of Systems Products, ICT Systems
 - Leasing
 - Other capital procurement procedure -- formalise armed procurement of revenue oriented 'stores' items by armed forces using capital budget
 - Post contract management

Salient Features

- Policy framework
 - Forcible indigenisation - disallowed imports of certain items, notified by MoD
 - Emphasis on use of AI, indigenously developed military materials, special alloys, indigenous software, aero-engines, silicon wagers
 - Issue: associated instructions not well integrated with procurement procedure

- Tweaked the planning system, that forms the basis of capital procurements
 - Issue: absence of overarching organisation dedicated to defense planning/ national security strategy documents/ composite plans covering armed forces + Coast guard + BRO +++ lack of financial pragmatism
- 5 Procurement categories

Categories, descending order of priority	Special categories	Eligible vendors	Indigenous content IC
Buy (Indian - Indian designed, Developed & Manufactured) = Buy IDDM	- Make - Make I, II, III - Innovation	Indian	Indigenous Design >= 50%
Buy (Indian)	Strategic Partnership Model	Indian	In case of indigenous design >= 50% Otherwise >= 60%
Buy and Make (Indian) (buy portion may be nil)	Leasing - Lease (Indian) - Lease (Global)	Indian	- >=50% of the 'Make ' portion; - Transfer of critical tech from foreign vendors, acc to specified range, depth, scope
Buy (Global - Manufacture in India)		Foreign and Indian	>= 50%
Buy (Global)		Foreign and Indian	- Foreign Vendor - Nil - Indian Vendor >= 30%

- Make I, II, III
 - Make I - govt funded
 - Make II - industry funded
 - Indian vendors, w/o govt funding; incl single individual or suo-moto proposal from a firm
 - Make III - not designed/ developed indigenously; can be mfged in India as import substitution in collab or Transfer of Tech from foreigners OEMs Original Equipment Manufacturers
- Incentives for MSMEs
 - Make I & II subcategories w/ project cost upto ₹100 crore/ year earmarked for MSMEs
 - Start-ups also eligible ID'ed by DPIIT in Make II
 - Min 50% IC Indigenous Content -- will be acquired through Buy IDDM category
 - Min 60% IC for Make-III
- Innovation
 - Involving individual innovators, technocrats, professionals, academics, smaller enterprises, start-ups and MSMEs
 - Routes
 - iDEX - Innovations for Defence Excellence Scheme; under DIO Defence Innovation Organisation
 - TDF Technology Development Fund Scheme
 - Indigenous Development by Services through Internal Organisations
- Leasing
 - Lease (Indian), Lease (Global)

- To save on initial capital cost
- Lessors could be Indian or foreign companies
- Useful where
 - Procurement not feasible due to time constraint
 - Asset/ capability required only for a specific period; would remain underutilised if procured
 - Limit quantity requirement; administrative/ maintenance cost likely to be high
 - Rent is better than one-time acquisition cost
- Strategic Partnership Model
 - Facilitate Indian private companies to become system integrators
 - Allowing them to tie up w/ approved foreign vendors to supply essential equipment to armed forces
 - Pvt sector expected to develop an ecosystem consisting of developmental partners, specialised supplies from MSMEs
- Offset guidelines
 - Focus on technology, investment, export of major platforms (previously on components)
 - Avenues revised to allow Indian industry to receive technologies for which foreign vendors eligible to receive direct credit
 - Higher tech reserved for govt entities
- Other special procedures
 - Acquisition of systems designed and developed by DRDO/ DPSU/ OFB
 - Fast Track Procedure FTP
 - Revitalising Defense Industrial Ecosystem through Strategic Partnerships
 - Acquisition of Systems Products and ICT Systems
 - Other Capital Procurement Procedure
 - Procedure for Defence Ship Building
- Misc
 - Standard Contract Document - edited
 - Post contract management
- FDI in Defence Manufacturing
 - May 2020 - increased from 49% to 74% under automatic route
 - Incorporated in DAP 2020
 - Eligible for Buy (Indian), Buy and Make (Indian), Buy (Global - Mfg in India), Make III
 - To protect interest of Indian industry while encouraging the OEMs to mfg in India certain categories of arms

Expected benefits

- EoDB - time bound, revised offset guidelines, rationalisation of trials and testing procedures
- Develop India into Global Manufacturing Hub - FDI
- Promote Make in India, Atmanirbhar Bharat initiatives
 - Reservation for Indian vendors in various categories
 - Ban on import of certain items
 - Indigenisation of imported spares
 - Overall enhancement in IC
- Cost cutting through leasing

Challenges

- Leasing may open a back door for import; need to curb that as major efforts towards

controlling direct imports would be hindered

Way forward (Need for Complementary Reforms)

- Early promulgation of National Security Strategy
 - Lack NSS/ defence white paper
- Resource commitment
 - 15-30% shortfall in fund requirements by MoD since DPP 2016 implementation
- Accountability in procurement
- Dedicated acquisition Cadre
 - DAP 2020 for the first time provides institutionalised personnel training, both in India and abroad
 - No of functionaries involved in procurement + professional training still inadequate
- Fewer procurement categories
 - Must merge categories with similar intents for simplicity
 - Buy (Indian) and Buy (IDDM) can be merged into one, w/ graded incentive for indigenous design and higher indigenous content
 - Buy and Make (Indian) + SPM - can be combined
- QR Cell within HQ IDS
 - QR - Qualitative Requirement
 - IDS - Integrated Defence Staff
 - QR Cell must be under overall supervision of CDS to drive in accountability
 - DAP 2020 tries to streamline formulation of QR by emphasising on Comparative Analysis of Specifications
 - CAG pointed out inappropriate QR formulations have impeded faster, cheaper procurement
- Medium and Long Term Defence Indigenisation Plan
 - Need robust, institutionalised indigenisation plan
 - List of items banned for import must be supplemented by a long term and medium term defence production plans as corollary of 10 and 5 year procurement plans

Related initiatives

- DPEPP Draft Defence Production and Export Promotion Policy 2020
- iDEX Innovations for Defence Excellence
- Mission Raksha Gyan Shakti - for increasing patents in DPSUs, OFB

Space

24 June 2020 09:17

Space

Outer Space Treaty 1967

- Sputnik launched in 1957 by USSR and cold war conditions led to space race

Weaponization of Space-

placing weapons in outer space or on heavenly bodies as well as creating weapons that will travel from Earth to attack or destroy targets in space. Weaponization of space is distinctly different from militarization of Space (using Space tech in military operations eg, GPS).

China pursuing ambitious space weaponization programs that poses serious threats to military giants like the US. Chinese efforts of space weaponization are in sharp contrast to its efforts to push for Prevention of an Arms Race in Outer Space (PAROS) treaty. It has even submitted a draft treaty to the UN along with Russia. A PAROS treaty would complement and reaffirm the importance of the 1967 Outer Space Treaty, which aims to preserve space for peaceful uses by prohibiting the use of space weapons, the development of space-weapon technology, and technology related to "missile defense." The treaty would prevent any nation from gaining a military advantage in outer space.

China's Space Weaponization Efforts include-

- Advancements in ICBM
- 2007 successful testing of ASAT (Anti-Satellite) missile
- Development of co orbital anti satellite system. Soft kill methods such as jammers.

India's response

- Agni V- ICBM
- PSLV, GSLV
- GSAT-7 for the Indian Navy

Impact of space weaponization

- Space debris
- Arms race in outer space

Need for a Space Law-

- Currently space activities are guided by Satellite Communication Policy, 2000 (which enacted a framework to provide licenses to private sector players to operate communication satellites over India) and Remote Sensing Data Policy, 2011
- International principles are evolved under UNCOPUOS (UN Committee on Peaceful Uses of Outer Space)
- There has been a growing interest of private sector in space activities with startups like TeamIndus, Astrome Technologies, planning their own space-based products and services.
- The involvement becomes crucial as current throughput of ISRO is not sufficient to meet market demand

Salient features of the Draft Law-

- Provisions apply to all sectors
- Nontransferable license for commercial space activity
- Register of all space objects will be maintained by govt
- Regulate procedures for conduct and operation of space activity through a regulatory body
- Fine for violations
- Criticism-

- Erroneous definition of space activity- even data companies handling satellite imagery or universities operating ground facilities for their microsatellites may also need a license.
- Non Specification of Regulator- Making Dept Of Space a regulator would involve conflict of interest.
- One blanket law for all space activities
- Non differentiation of liabilities-
- Non clarity on space pollution

SHREYA SHREE
AIR 71 - CSE 2021

Weapons etc

23 June 2020 18:32

[UAV](#)

[drones](#)

[Chemical weapons](#)

SHREYA SHREE
AIR 71 - CSE 2021

Left Wing Extremism Division | Ministry of Home Affairs | Gol

Saturday, June 20, 2020 7:36 PM

Clipped from: https://www.mha.gov.in/division_of_mha/left-wing-extremism-division

About the Division

This Division was created w.e.f. October 19, 2006 in the Ministry, to effectively address the Left Wing Extremist insurgency in a holistic manner. The LWE Division implements security related schemes aimed at capacity building in the LWE affected States. The Division also monitors the LWE situation and counter-measures being taken by the affected States. The LWE Division coordinates the implementation of various development schemes of the Ministries/Departments of Govt. of India in LWE affected States. The States of Chhattisgarh, Jharkhand, Odisha, Bihar, West Bengal, Andhra Pradesh, Telangana, Maharashtra, Madhya Pradesh, Uttar Pradesh and Kerala are considered LWE affected, although in varying degrees.

Role and Functions of the Division

- Capacity building of States to combat LWE through schemes of Ministry of Home Affairs like Security Related Expenditure (SRE) scheme, Special Infrastructure Scheme, Special Central Assistance etc.
- Deployment of Central Armed Police Forces(CAPFs) in LWE affected States.
- Providing funds to the CAPFs for strengthening of infrastructure/Helicopters/civic action etc.
- Reviewing the security situation in the LWE affected States and issuing advisories to the State Governments concerned.
- Providing assistance to State Governments for initiatives to combat LWE in the form of funds for items of emergent nature.
- Coordinating implementation of LWE related Schemes of other Central Ministries for LWE affected Districts.

Organisational Chart

Swipe to view

SR-NoTitleDownload/Link

- 1 Organisational Chart. [Download \(66.33 KB\)](#)



Background

- A number of Left Wing Extremist outfits have been operating in certain remote and poorly connected pockets of the country for a few decades now. In a significant development in 2004, the People's War

(PW), then operating in Andhra Pradesh, and the Maoist Communist Centre of India (MCCI), then operating in Bihar and adjoining areas, merged to form the CPI (Maoist) Party. The CPI (Maoist) Party, is the major Left Wing Extremist outfit responsible for a majority of incidents of violence and killing of civilians and security forces and has been included in the Schedule of Terrorist Organizations along with all its formations and front organizations under the Unlawful Activities (Prevention) Act, 1967. The CPI (Maoist) philosophy of armed insurgency to overthrow the Government is unacceptable under the Indian Constitution and the founding principles of the Indian State. The Government has given a call to the Left Wing Extremists to abjure violence and come for talks. This plea has been rejected by them, since they believe in violence as the means to capture State power. This has resulted in a spiraling cycle of violence in some parts of India. The poor and the marginalized sections like the tribal are bearing the brunt of this violence. Many well-meaning liberal intellectuals fall prey to the Maoist propaganda without understanding the true nature of Maoist insurgency doctrine which glorifies violence and believes in adopting the military line to capture power. Between 2004 to 2019 (up to 31.12.2019) 8197 people have been killed by the LWE in different parts of India. The majority of the civilians killed are tribal's, often branded as 'Police informers' before being brutally tortured and killed. In fact, the tribal and the economically underprivileged sections, whose cause the Maoists claim to espouse, have been the biggest victims of the So-called 'protracted peoples war' of the CPI (Maoist) against the Indian state.

The dynamics of Maoist insurgency:

- Some sections of the society, especially the younger generation, have romantic illusions about the Maoists, arising out of an incomplete understanding of their ideology. The central theme of Maoist ideology is violence. The Maoist insurgency doctrine glorifies violence as the primary means to overwhelm the existing socio-economic and political structures. The Peoples Liberation Guerilla Army (PLGA), the armed wing of CPI (Maoist), has been created with this purpose in mind. In the first stage of the insurgency, the PLGA resorts to guerrilla warfare, which primarily aims at creating a vacuum at the grass-roots level of the existing governance structures. This is achieved by killing lower-level government officials, police-personnel of the local police stations, the workers of mainstream political parties and the people's representatives of the Panchayati Raj system. After creating a political and governance vacuum, they coerce the local population to join the movement. A strident propaganda is also carried out against the purported and real inadequacies of the existing state structure.
- In areas under Maoist domination, the absence of governance becomes a self- fulfilling prophecy since the delivery systems are extinguished through killings and intimidation. This is the first step in the strategy of the Maoists to seek to control the countryside. In the meanwhile, many Front Organisations are created to facilitate mass-mobilisation in semi-urban and urban areas through ostensibly democratic means. Most of the Front Organisations are led by well-

educated intellectuals with a firm belief in the Maoist insurgency doctrine. These ideologues function as masks to cover the violent nature of the CPI (Maoist) ideology. They also form the propaganda/disinformation machinery of the party.

- They stridently take up issues like 'displacement of tribals', 'corporate exploitation', 'human rights violations' by security forces etc. and often make fantastic claims in this regard which get reported even by the mainstream media. The Front Organisations also skilfully use state structures and legal processes to further the Maoist agenda and weaken the enforcement regime. The important functions of these Organisations include recruitment of 'professional revolutionaries', raising funds for the insurgency, creating urban shelters for underground cadres, providing legal assistance to arrested cadres and mass- mobilisation by agitating over issues of relevance/ convenience. The Front Organisations aim to provide short-term democratic subterfuge to cover-up the totalitarian and oppressive nature of the Maoist ideology. The CPI (Maoist) also have a strategic game-plan to create a 'United Front' with all like-minded insurgent/terrorist outfits in India. It needs to be remembered that many of these outfits are supported by external forces inimical to India and the CPI (Maoist) consider such alliances as strategic assets.
- In a nutshell, the CPI (Maoist), the main LWE outfit in India, aims to overthrow the existing democratic state structure with violence as their primary weapon, and mass mobilization and strategic united fronts as complementary components and plans to usher in So-called 'New Democratic Revolution' in India.

THE GOVERNMENT OF INDIA'S APPROACH

- The Government's approach is to deal with Left Wing Extremism in a holistic manner, in the areas of security, development, ensuring rights and entitlements of local communities, improvement in governance and public perception management. In dealing with this decades-old problem, it has been felt appropriate, after various high-level deliberations and interactions with the State Governments concerned, that an integrated approach aimed at the relatively more affected areas would deliver results. With this in view, a detailed analysis of the spread and trends in respect of Left Wing Extremist violence has been made and 90 districts in eleven States have been taken up for special attention with regard to planning, implementation and monitoring various interventions. However, 'Police' and 'Public Order' being State subjects, action on maintenance of law and order, lies primarily in the domain of the State Governments. The Central Government closely monitors the situation and supplements and coordinates their efforts in several ways. These include providing the Central Armed Police Forces (CAPFs); sanction of India Reserve (IR) battalions, setting up of Counter Insurgency and Anti Terrorism (CIAT) schools; modernisation and upgradation of the State Police and their Intelligence apparatus; reimbursement of security related expenditure under the Security-related Expenditure (SRE) Scheme; providing helicopters for anti-LWE operations, assistance in training of State Police through the Ministry of Defence, the Central Police

Organisations and the Bureau of Police Research and Development; sharing of Intelligence; facilitating inter-State coordination; assistance in community policing and civic action programmes etc. The underlying philosophy is to enhance the capacity of the State Governments to tackle the Maoist menace in a concerted manner.

MONITORING MECHANISMS

- The Union Home Minister, the Home Secretary & the Special Secretary/Additional Secretary and a Review Group chaired by the Cabinet Secretary review the LWE situation on a regular basis. The Progress of the various schemes is regularly monitored by MHA through meeting and Video Conferencing with the Central Ministries/Departments concerned and State Governments.

Recent Reviews

- The Union Home Minister has visited Chhattisgarh and Jharkhand in the month of May 2018 and reviewed the LWE situation.
- The Union Home Minister has convened meetings of Chief Ministers of LWE affected States on February 09, 2015, May 08, 2017 and August 26, 2019.
- The Minister of States (Home) have visited LWE affected States and reviewed the LWE situation.
- Review Group meeting conducted by the Cabinet Secretary on 15/12/2016, 03/08/2017 and on 23/7/2018.
- Meetings are being conducted regularly by Union Home Secretary with Secretaries of Central Ministries and Chief Secretaries, DsGP of the LWE affected States and DsG of CAPFs.
- Union Home Secretary also visited the LWE affected States to review the LWE situation.
- The Union Home Secretary has visited Chhattisgarh in the month of October, 2019 and reviewed the LWE situation.

IMPORTANT INITIATIVES FOR LWE AFFECTED STATES

- In order to holistically address the LWE problem in an effective manner, Government has formulated National Policy and Action Plan adopting multi-pronged strategy in the areas of security, development, ensuring rights & entitlement of local communities etc.
- **Security Related Expenditure (SRE) Scheme:** This Scheme has been extended by the Government on 27.09.2017 as a subscheme of the Umbrella Scheme Modernization of Police Forces for a period of 03 years till 2020. Under the Security Related Expenditure (SRE) Scheme, the central Govt. reimburses to the State Governments of 11 LWE affected States Security Related Expenditure of 90 districts relating to training and operational needs of security forces, ex-gratia payment to the family of civilians/security forces killed/injured in LWE violence, compensation to Left Wing Extremist cadres who surrendered in accordance with the surrender and rehabilitation policy of the concerned State Government, community policing, Security related infrastructure for village defence committees and publicity materials. There is a substantial increase in annual outlay and new items such as compensation for Security force personnel

incapacitated during anti LWE operations and compensation for the property damage have been included in this scheme. The SRE Scheme aim at strengthening of the capacity of the LWE affected States to fight the LWE problem. Rs. 212 crore have been released in the current financial year as on 31.12.2019.

- **Special Central Assistance (SCA) for 30 most LWE affected districts:** This Scheme has been approved by the Government on 27.09.2017 as a sub-scheme of the Umbrella Scheme, 'Modernization of Police Forces' for a period of 3 years i.e. from 2017-18 to 2019-20. The main objective of the Scheme is to fill the critical gaps in Public infrastructure and Services, which are of emergent nature. Rs. 1775 crore have been released to the States during last 3 years. Rs. 600 crore have been released in the current financial year as on 31.12.2019.
- **Special Infrastructure Scheme, along with Construction of Fortified Police Stations in the LWE affected States:** On regular demand of the LWE affected States, the Central Government has approved this Scheme as a sub-scheme of the Umbrella Scheme, 'Modernization of Police Forces' for a period of 3 years i.e. from 2017-18 to 2019-20. The total outlay of the scheme is Rs. 1006.00 crore i.e. Rs. 604 crore as Central Share (60%) and Rs.402 crore as State share (40%). Rs. 56.5 crore have been released in the current financial year as on 31.12.2019.
- **Scheme of Fortified Police stations:** The Ministry had sanctioned 400 police stations in 10 LWE affected States. Of these 399 of PSs have been completed.
- **Assistance to Central Agencies for LWE management Scheme:** This Scheme has been approved by the Government on 27.09.2017 as a sub scheme of the Umbrella Scheme Modernization of Police Forces for a period of 03 years i.e. from 2017-18 to 2019-20. Under the Scheme, assistance is provided to Central Agencies (CAPFs/IAF etc) for strengthening of infrastructure and hiring charges for Helicopters.
- **Civic Action Programme (CAP):** This Scheme has been approved by the Government on 27.09.2017 as a sub scheme of the Umbrella Scheme Modernization of Police Forces for a period of 03 years i.e. from 2017-18 to 2019-20. CAP in LWE affected areas is being implemented since 2010-11 to bridge the gaps between Security Forces and local people through personal interaction and bring the human face of SFs before the local population. The Scheme has been very successful in achieving its goal. Under the Scheme, funds are released to the CAPFs, deployed in LWE affected areas, for conducting various civic activities for the welfare of the local people. 17.16 crore have been released to CAPFs in the current financial year as on 31.12.2019.
- **Media Plan:** This Scheme has been approved by the Government on 27.09.2017 as a sub scheme of the Umbrella Scheme Modernization of Police Forces for a period of 03 years i.e. from 2017-18 to 2019-20. The Maoists have been misguiding and luring the innocent tribals/ local population in LWE affected areas by their So-called poor-friendly revolution through petty incentives or by following their coercive strategy. Their false propaganda is targeted against the

security forces and the democratic setup. Therefore, the Government is implementing this Scheme in LWE affected areas. Under the scheme activities like Tribal Youth Exchange programmes organised by NYKS, radio jingles, documentaries, pamphlets etc. are being conducted. 7.41 crore have been released in the current financial year as on 31.12.2019.

- **Road Requirement Plan-I (RRP-I) for LWE affected areas:** This Scheme is being implemented by Ministry of Road Transport & Highways for improving road connectivity in 34 LWE affected districts of 8 States i.e. Andhra Pradesh, Bihar, Chhattisgarh, Jharkhand, Madhya Pradesh, Maharashtra, Odisha and Uttar Pradesh. This scheme envisaged construction of 5,422 km roads lengths in LWE affected States, of which 4,868 km roads have been completed by 30.11.2019.
- **Road Connectivity Project for LWE affected areas (RRP-II):** The Government approved this scheme on 28.12.2016 for further improving road connectivity in 44 districts of 9 LWE affected States. This Scheme envisages 5412 km roads and 126 bridges at an estimated cost of Rs. 11,725 Crores. Ministry of Rural Development is the nodal Ministry for this project. The roads included under the scheme have been identified by the Ministry of Home Affairs in consultation with the State Governments and the security agencies. 1373 km roads have been constructed so far till 31.12.2019.
- **LWE Mobile Tower Project:** To improve mobile connectivity in the LWE areas, the Government on 20.08.2014 approved installation of mobile towers in LWE affected States and 2335 mobile towers have been installed in Phase-I. Phase-II of the project has been approved by the Government of India, under which 4072 mobile towers, involving an expenditure of Rs. 7330 crore, will be installed in LWE affected States.
- **Aspirational District:** The Ministry of Home Affairs has been tasked with the monitoring of Aspirational districts programme in 35 LWE affected districts.

Conclusion


- It is the belief of the Government of India that through a holistic approach focussing on development and security-related interventions, the LWE problem can be successfully tackled. However, it is clear that the Left Wing Extremists do not want root causes like underdevelopment to be addressed in a meaningful manner since they resort to targeting school buildings, roads, railways, bridges, health infrastructure, communication facilities etc in a major way. They wish to keep the population in their areas of influence marginalized to perpetuate their outdated ideology. Consequently, the process of development has been set back by decades in many parts of the country under Left Wing Extremists influence. This needs to be recognised by the civil society and the media to build pressure on the Left Wing Extremists to eschew violence, join the mainstream and recognise the fact that the socio-economic and political dynamics and aspirations of 21st Century India are far removed from the Maoist world-view. Further, an ideology based on violence and annihilation is doomed to fail in a democracy which offers legitimate

forums of grievance redressal.

Annexures:

Swipe to view

SR-NoTitleDownload/Link

- 1 Frequently Asked Questions (FAQs) [Download \(72.9 KB\)](#) 

P.S.: All references to Maoism in this portal is in the context of CPI(Maoist) and other LWE organizations included in the schedule of Terrorist organizations under the Unlawful Activities (Prevention) Act, 1967.

SHREYA SHREE
AIR 71 - CSE 2021

Building the resilience of India's internal security apparatus | ORF

19 May 2020 14:19

Clipped from : <https://www.orfonline.org/research/building-the-resilience-of-indias-internal-security-apparatus-45753/>

26 November 2018 marked a decade since 10 Pakistan-based terrorists killed over 160 people in India's financial capital of Mumbai. The city remained under siege for days, and security forces disjointedly struggled to improvise a response. The Mumbai tragedy was not the last terrorist attack India faced; there would be many others since. After every attack, the government makes lukewarm attempts to fit episodic responses into coherent frameworks for security-system reforms. Yet, any long-term strategic planning, which is key, remains absent. The state of India's internal security is often qualitatively linked to the incumbent government and the ability of its policymakers to appreciate security challenges. This paper argues that India needs a comprehensive and coordinated approach amidst growing and evolving threats to its security.

This paper is part of ORF's series, 'National Security'.

Find other research in the series [here](#):

Introduction

Even as dominant public discourse largely focuses on the external dimensions of India's national-security challenge, equally important is the internal dimension. Internal security, a subset of national security, is concerned with threats and challenges emanating from within a country and has the potential to threaten public order and national security. India's internal security challenges have varied sources, such as across-the-border enmity permeating as insurgency in Kashmir, some ethnic groups opting for secessionist movements in the Northeast, sections of people resorting to violent solutions to perceived or real grievances, direct acts of terrorism aided and abetted by Pakistan, illegal migration, and organised crime.

According to the Indian Constitution, "Public Order" and "Police" figure as entries 1 and 2 respectively in the State List in the Seventh Schedule, giving states exclusive power to legislate with respect to police system and exercise full administrative control over the police. The union or central government can exercise similar powers only in the Union Territories. Under entry 2A of the Union List, the central government can deploy any armed force of the union in any state in aid of civil power. However, powers under this entry are invoked only in a serious emergency, when a state civil administration requests the assistance of central armed forces to maintain public order.

Many policing functions—such as traffic control, enforcement of civic laws, investigation of "ordinary" crimes, and routine law-and-order problems—can be effectively supervised by state-police forces. However, the police are the first responders in almost all internal-security crises and have to deal regularly with organised crimes, cyber crimes, terrorism, insurgency and large-scale political violence. The nexus between terrorists on the one hand and organised-crime syndicates (such as smugglers and drug traffickers) on the other has added a new dimension to the internal-security situation. The legal and jurisdictional lines between terrorism and organised criminal activities are often blurred, especially given the difficulty in defining these concepts.

At present, there is no national agency to deal with organised criminal syndicates (of which there are many operating in various states) and advise states on coordinated preventive action. Since 'police' is a state subject, the powers of the central government to make an intervention is limited, except when the entire state administration is taken over by the central government. The Constitution does not provide for central intervention in serious situations that pose a potential threat to the security of the nation. Thus, despite terrorist activity being one of the major national-security threats for India, the internal-security mechanism seems unprepared to deal with such situations, due to political reasons and limited operational capacity of police and intelligence organisations. Intelligence, physical security, coordination amongst agencies, investigation and crisis management

are considered the most important components of counterterrorism activity. If the intelligence apparatus fails to provide early warning about an act of terrorism, the physical-security machinery should be able to prevent the terrorists. In the event that both intelligence and physical-security mechanisms fail, the crisis-management processes should be effective enough to cope with the consequences.^[1] Not much data is available in the open domain about the lapses. However, a careful analysis of some previous instances of terrorism indicates that intelligence, physical-security and crisis-management apparatus in India have not performed commendably. After each major terrorist attack, the citizens question how such incidents keep happening despite years of experience in countering terrorism and insurgency in various parts of the country. The answer is that India's institutional capabilities to fight terrorism have stagnated or have developed only marginally. Even the Modi government, which has highlighted the need for a robust security policy, has dithered on key security-sector reforms. Many crucial projects relating to internal security remain pending.

India's National Security Architecture

There are two styles of counterterrorist activities: a criminal justice counterterrorism, which deals with acts of terrorism within a law-enforcement framework; and a militaristic counterterrorism, which views terror as a threat to national security and, thus, to be countered with armed force. India uses a combination of both styles: intelligence, military, and police organisations together contribute to counterterrorism (CT) efforts.

Given India's large population and its heterogeneous character, the Indian Constitution has distributed certain powers between the central government and the state governments. While maintenance of law and order is a state subject, the federal nature of Indian polity complicates the structures needed for counterterrorism. Thus, India's performance in policing terrorism has been mixed.

Despite constitutional provisions, the central government has raised seven Central Paramilitary Forces (CPMFs), which are regularly deployed for law-and-order duties along with the police forces of respective states. These seven CPMFs are the Central Reserve Police Force (CRPF), Border Security Force (BSF), Assam Rifles, Central Industrial Security Force (CISF), Indo-Tibetan Border Police (ITBP), Seema Surksha Bal (SSB) and the National Security Guard (NSG). The personnel of all seven CPMFs total around one million.

The CRPF, the most important of the CPMFs, performs a wide range of duties, including management of law and order, counterinsurgency and counterterrorism, all over India. Though the BSF, the ITBP and the SSB are primarily meant for border security, they play a crucial role in counterinsurgency and counterterrorism operations in three critical conflict zones: the Northeast, Maoist-affected areas and Kashmir.

The Intelligence Bureau (IB), India's main intelligence agency, functions under the Ministry of Home Affairs and is responsible for internal security and intelligence. The IB is considered the nodal counterterror agency and works closely with the state police and the central paramilitary forces on counterterrorism intelligence. However, it cannot fully execute this function because it has no legal authority to investigate an offence, arrest anyone or prosecute them in court. The Research & Analysis Wing (RAW), India's premier external intelligence agency, operates under the cabinet secretariat and, thus, reports to the prime minister. Rivalries between the IB and the RAW often hamper overall intelligence effectiveness.^[2] Other intelligence agencies, such as the Central Economic Intelligence Bureau and the Directorate General of Military Intelligence, also perform counterterror functions as part of their organisational mandate.

After the 1999 Kargil incursion, the central government conducted a comprehensive review and reform of India's intelligence apparatus in particular, and national security system in general. Based on the recommendations of a Special Task Force, the government set up a revamped national-security mechanism. The main features of the new mechanism included the creation of a National Security Council (NSC), chaired by the prime minister and consisting of a few cabinet members to discuss national-security issues; a Strategic Policy Group (SPG), headed by the cabinet secretary^[3] and comprising the professional heads of the ministries concerned with national security and the heads of intelligence agencies and armed forces, to work out policy options and submit them to the NSC for consideration; a National Security Advisory Board (NSAB) consisting of non-governmental experts to provide policy inputs to the National Security Council Secretariat (NSCS), which was set up to aid the work of the NSAB, the SPG and NSC; and the National Security Advisor (NSA) to oversee the functioning of the new mechanism and to advise the prime minister on national-security issues.

Recently, the central government has effected a change in the SPG. It will now be headed by the NSA instead of the cabinet secretary. Its 18 members include the three service (army, navy, air force) and two intelligence chiefs (IB and RAW); defence, home, finance, revenue, and space secretaries; the governor of the Reserve Bank of India; and vice chairperson of the NITI Aayog. The Joint Intelligence Committee (JIC), a part of the NSCS, collates national-level intelligence inputs from all intelligence agencies and presents its independent analysis to the Cabinet Committee on Security (CCS). The Defence Intelligence Agency (DIA), as a nodal point to coordinate the activities of army, navy and air-force intelligence, complements the work of the RAW.^[4]

Unfinished Reforms

Since the 26/11 Mumbai attacks, India's counterterrorism architecture has been revamped, with the creation of the National Investigation Agency (NIA) to improve investigation capabilities.

Deployment of the National Security Guard (NSG) has also been decentralised, with four NSG hubs in different parts of India. The NSG is now a fully functioning terror-fighting agency. The amended Unlawful Activities Prevention Act (UAPA) has given new powers to the security agencies, including the ability to hold terror suspects for six months without charges.

Given the complexities involved in India's national-security architecture, it is crucial to improve coordination between various federal and state-security agencies. Following the Mumbai attacks, the first step in this direction was the strengthening of the Multi-Agency Centre (MAC), an intelligence-sharing "fusion centre" created within the IB in 2002 in the aftermath of the 1999 Kargil incursion. The national MAC coordinates across approximately two dozen representatives from the intelligence agencies in the home, finance and defence ministries.

Much of the intelligence sharing between the centre and states happens through the state offices of the IB and the Subsidiary Multi-Agency Centres (SMAC) as well as through the connectivity between the SMAC and the state-police special branches. Currently, 429 SMAC nodes and 251 district-police offices are connected to the MAC/SMAC Network.^[5] However, personnel shortages have hindered their efficacy, and in practice, they function as little more than state-level IB offices. That much of the intelligence inputs into the MAC come from only a handful of states reflects the fundamental weakness of many of India's state-police services. Moreover, under constitutional provisions, intelligence sharing depends on the goodwill of the states: if a state is unwilling to cooperate with the central government, it cannot be forced to do so. Each agency guards its own turf, and coordination mostly depends on the interpersonal relationships between the officials of the agencies.^[6]

Due to this ad-hoc process, and because of India's federal structure, the current national-security architecture (and counterterrorism structure in particular) is faulty, as there is no single authority from which these agencies receive unified directions. Countering terrorism in India is fraught with numerous difficulties. The legal structure, a legacy of the colonial past, has been struggling to cope with the demands placed upon it. India's Ministry of Home Affairs (MHA) oversees national police, domestic intelligence and paramilitary forces. The major legislation to deal with terrorism in India is the UAPA. Some Indian states, such as Maharashtra and Karnataka, have their own laws, which are used to prosecute suspected terrorists. The Terrorist and Disruptive Activities (Prevention) Act (TADA), the first anti-terrorism law to define and counter terrorist activities, was allowed to lapse in 1995.^[7] When there were several allegations of misuse in the application of the new anti-terror law, the Prevention of Terrorism Act (POTA), it was decided to repeal the act in 2004. This was followed by an amendment to the already existing UAPA.

India's experiments with TADA, POTA and UAPA have failed to deliver the desired results. There have been allegations that these anti-terror laws are designed to shield or harass a particular community. The Second Administrative Reforms Commission (ARC) of India, in its report in 2008, said, "A comprehensive and effective legal framework to deal with all aspects of terrorism needs to be enacted. The law should have adequate safeguards to prevent its misuse."^[8]

No intelligence organisation can remain static in the face of growing technological complexity, geopolitical uncertainty, the changing nature of terrorism, and increasing media intrusion. The US vastly improved its intelligence collection, coordination and assessment system immediately after the 9/11 terror attacks. India, however, did not overhaul its intelligence apparatus after 26/11.

The sweeping internal-security reforms initiated after the Mumbai attacks were followed by the announcement of central government's intention to create a National Counter Terrorism Centre (NCTC) and a national computerised information-sharing network, known as the NATGRID. But the

greatest failure of the post-Mumbai reforms was the NCTC, which was supposed to be established within a year of its announcement in December 2012. The central government's efforts to set up the NCTC—whose aim included preventing, containing and responding to terrorist attacks—were trapped in the political quagmire of centre–state relations. Thus, the intended launch of the NCTC had to be put on hold. The non-Congress ruling states of Gujarat, Tamil Nadu, Odisha, Karnataka, Bihar, Tripura and West Bengal were opposed to the proposal; their main contention was that the NCTC would violate the principle of federalism. Under the Indian Constitution, “public order” and “police” are state subjects and, thus, the sole preserve of a state government.

The NCTC was conceived as the centrepiece of internal-security reforms. It was modelled on the American institution of the same name, which functions as a centre for joint operational planning and joint intelligence. India's NCTC was meant to subsume the MAC and its operatives would have arrest powers throughout India. Many state governments vehemently opposed it, citing two reasons. First, the NCTC's power to arrest any suspect and to carry out operations without prior approval from and knowledge of the respective states. Second, its “power to seek information, including documents, reports, transcripts, and cyber information from any agency” to carry out its functions. Civil-liberty activists, too, saw the move as an unconstitutional expansion of government control. In the face of such opposition from several quarters, the scope of the NCTC were steadily narrowed down: first, the operational wing was eliminated; then, the NCTC as a whole was placed under the control of the IB.

In wanting to copy the US model, the MHA had overlooked a significant detail: The US NCTC is part of its Directorate of National Intelligence (DNI), which is manned by officials from the Pentagon, FBI, CIA and other agencies who can access its databases. The centre analyses and collates terrorism-related information to support counterterrorism operations of intelligence agencies. However, it is not authorised to conduct intelligence operations on its own and has no powers to investigate or arrest.^[9]

The IB's control over the NCTC became a major source of controversy. It is a general principle in all liberal democratic countries that an intelligence agency should not possess police powers of arrest. The opposition parties expressed fear that if the NCTC was made part of the IB, the powers given to it under the UAPA could be misused. Presently, the IB is largely insulated from any parliamentary oversight, and its lack of parliamentary accountability will be further perpetuated by the NCTC.^[10]

The politicisation of India's intelligence agencies has allowed the ruling parties to use them to monitor the activities of opposition leaders. For instance, Bihar Chief Minister Nitish Kumar had opposed the proposed structure of the NCTC on the ground that it was to be “created within the Intelligence Bureau, which is a secret intelligence organisation without any accountability to Parliament or the court.”^[11] There have been several allegations that the previous UPA government used the NIA for political purposes, to probe right-wing terror cases such as the 2006 Malegaon blasts and the 2007 Samjhauta Express bombings. However, amidst all allegations and counter-allegations, more than 10 years after the Malegaon blast in 2008, the NIA court framed charges against the accused under the UAPA and various other sections of the IPC for their alleged involvement in the blasts. The NIA court has already rejected the pleas of the accused who challenged the invoking of UAPA.^[12]

Additionally, the turf war between the intelligence agencies operating under different government ministries contributed to the difficulty in establishing NCTC. In making the NCTC a part of the IB, instead of allowing it to be an independent institution, the MHA made people more distrustful of it. According to B. Raman, a former senior official of the RAW, “There were inadequate consultations even at the centre as one could see from the opposition expressed by an increasing number of ex-RAW officers to the move to make the NCTC a part of the IB.”^[13] Finally, there have also been several accusations that security agencies show bias against minority communities, particularly during counterterror operations.

In 2014, the BJP's election manifesto had criticised the UPA regime for its inability to create NCTC. According to the document, “The government has been unable to evolve political consensus in the country for the establishment of a Centralized body such as the National Counter Terrorism Centre (NCTC) to collectively combat terror.”^[14] But the change of regime at the centre could not revive NCTC's fortunes. As the Minister of State for Home Hansraj Ahir said in November 2016 to the Rajya Sabha, the “[o]perationalisation of NCTC has been kept in abeyance as some states raised concerns regarding its structure, functions and mandate. A final decision on operationalisation of NCTC is yet to be taken.”^[15]

Other internal security reforms have received mixed responses. The NATGRID was originally envisioned as a unified database that would compile a wide variety of currently available intelligence inputs. It has acquired some of the world's most advanced data-mining software that can be used to track and potentially predict terrorist attacks. The system has faced internal resistance, however, particularly from the IB, which feels that NATGRID encroaches on its turf.^[16] Ten years after 26/11, NATGRID has not come out of its embryonic stage. In fact, it remained without a head for two years between May 2014 and July 2016. It was likely to be partially functional around the 10th anniversary of 26/11, but full functionality cannot be achieved before March 2019.^[17] Some of the features of NATGRID will be replicated by the Crime and Criminal Tracking Networks & System (CCTNS), which is meant to seamlessly link India's 15,000-plus police stations to allow for better information sharing. The NCRB chief recently announced that 14,749 out of the 15,655 police stations in the country have been connected with the CCTNS.^[18]

However, some challenges remain. The CCTNS received no financial allocation for two consecutive budgets for 2014-15 and 2015-16, hampering the progress of the project.^[19] While CCTNS was designed to be used in conjunction with the e-prisons system, the integration has not been successful, inconveniencing the police as they "upload the data on the CCTNS and later print out a hard copy to take to the court."^[20] The National Investigation Agency (NIA) has also faced backlash from the states, which resist giving up their jurisdiction over policing. Nonetheless, the central government continues its efforts to make it the leading national agency.

Police Incapacity

Until the 2001 terror attack on the Indian Parliament, intelligence was rarely used to inform investigative strategy in mainstream policing function, although there was an intelligence architecture supporting higher policing function, and some sections of the police service utilised intelligence, often to support covert-policing strategies. Knowledge of intelligence-gathering techniques was passed down from generation to generation within police's special branches/units as a form of oral history. The craft of the trade that such units used were often hidden behind the opaque screen of "need to know." While there could be perfectly sensible reasons for limiting access to such knowledge, the outcome has been a limited ability of police officers outside those discrete units to identify "best practices" to improve their professional practice for countering the growing challenges of organised crime, terrorism, insurgency and political violence. Additionally, terror attacks have the effect of bringing the failings of police-intelligence work into public view.

The Mumbai attacks of 2008 and Pathankot airbase attack of 2016 exposed key vulnerabilities in India's policing system, primarily that it was woefully inadequate in combating suicidal assaults. Ajai Sahni, executive director of the Institute of Conflict Management, is accurate in locating the problem in "the glacial pace of an early 20th century structure of governance trying to cope with an exponentially accelerating 21st century problem,"^[21] saying that Indians "can't have first-rate counter-terrorism in a third-grade policing system."^[22]

The criminal justice system cannot function without a healthy police and investigative agency. However, India's criminal justice system faces huge challenges, with a poorly trained and understaffed police force and insufficient modern equipment at their disposal. There is considerable variation in the size and competence of India's various state-police forces. India's low police-to-population ratio of about 180 per 100,000 is much lower than what the United Nations recommends for peacetime policing. In Western countries, the police-to-population ratio ranges from 250 to 500 per 100,000. According to India's Bureau of Police Research & Development, 24 percent of posts in the police forces nationwide are vacant. Uttar Pradesh has the largest number of vacancies, with only 181,000 police personnel against the sanctioned strength of 363,000.^[23] Moreover, because of India's notorious VIP culture, only a dismal number of police personnel are available for the security of the common citizen. Calculating against the population, only one police officer is available for the security of 729 Indian people, leaving the police personnel overburdened.^[24] Given the acute shortage in their ranks, police personnel are required to work long hours, without a break, and rarely get to take their weekly off, leaving them stressed and frustrated. This has a huge bearing on their professional responsibilities, including counterterrorism duties.

The police in India are trained to deal with law-and-order problems. When faced with terrorism and insurgency, they find it difficult to respond effectively. To successfully prevent terrorism, the public must be willing to share with the police any vital information or suspicious activity in their locality. However, even after 70 years of the country's independence, the image of the Indian police has not

improved and they are often viewed with suspicion. There are several reasons for this.

First, political authorities still have a stronghold over the police. Political interference in the functioning of the police, which has become a norm, leads to the abuse of authority. For instance, whenever a new government is elected, the first thing it usually does is to replace the Director General of Police of the state. Thus, people do not trust the police and perceive them as partisan and politicised. Nothing confirms this perception more than the frequent demand for probes by the Central Bureau of Investigation into crimes that can be effectively handled by the Criminal Investigation Department of the state police.

Unfortunately, many police officers deliberately allow their professional autonomy to be dominated by political pressures in an attempt to please the political masters. Police officers cannot be insulated from political pressures if many of them are willing participants. The most undesirable fallout of political interference in police functioning is the decline in its ability to respond effectively to difficult and violent situations. Instances of failure of police leadership far outnumber the achievements. For instance, Haryana Police's handling of the incidents at Panchukula in the aftermath of the conviction of the self-styled Godman Ram Rahim Singh displays police ineptitude and lack of professionalism. It was a re-enactment of their poor performance in responding to the previous Jat agitations.

Many state governments have a vested interest in perpetuating the presence of central forces in their state, as it allows them to shift the financial burden of responsibility for dealing with critical law-and-order situations to the central government. Ved Marwah, a former governor of Manipur, Mizoram and Jharkhand, says that when a state government is reluctant or fails to deal with violent conflicts and anti-national movements, "instead of strengthening the state police machinery, it rushes to the Centre to hand over its responsibility at the first sign of any serious trouble. It is not surprising that in these states some sections of the police have actually joined hands with the subversive forces against the central forces."^[25] Only when the operational capabilities of the state police are improved at the local level can counterterrorism efforts succeed.

Corruption in the police forces further aggravates the challenge of fighting terrorism, as there is a close relationship between crime, corruption and terrorism in India. For instance, criminal gangs such as 'D Company' have widespread smuggling networks that include corrupt police and customs officers. Moreover, politicians often manipulate the police for nefarious purposes or turn a blind eye when officers remain inactive in the face of communal disorders.

While terrorists invariably have political objectives, criminal syndicates do not. Once established, a criminal network of drug traffickers and smugglers will continue to flourish and systematically corrupt the administrative machinery at various levels. As early as 1993, the Vohra Committee made startling revelations about the penetration of organised crime in India. In the past quarter-century, it has gripped almost every aspect of national life. However, only few states—Maharashtra, Delhi and Karnataka^[26]—have specific laws to combat organised crime. Punjab had begun the process of enacting a similar law, the Punjab Control of Organised Crime Act (PCOCA), which now seems to have fizzled out.^[27] On 15 November, the Madras High Court, while calling for details of political parties that had appointed "persons with muscle power/criminal background" as office bearers, also asked the government to explore the possibility of a special law to deal with organised crime.^[28]

In 2006, the Supreme Court of India, in a landmark judgment, ordered the central and state governments to implement some crucial police reforms, the most important one calling for a separation of the investigation and law-and-order functions of the police. Moreover, the order to establish the State Security Commission is primarily to ensure that the state government does not exercise unnecessary influence or pressure on the police. However, all state governments have displayed absolute indifference to the court order.^[29] The police are not insulated from partisan politics, because the state governments do not allow the police to develop into an efficient and effective service. All governments want the police to behave as 'the armed wing of their ruling party' since much of the power of the executive (in a post-colonial system such as India) is derived from the control of police.

Additionally, the states are reluctant to provide resources to the police forces. In 2017, the central government approved INR 25,060-crore for an internal-security scheme to strengthen the law-and-order apparatus and modernise state-police forces. The umbrella scheme, "Modernisation of Police Forces," is scheduled to be implemented between 2017 and 2020. The central government's share is INR 18,636 crore and that of each state is INR 6,424 crore. It has special provisions for women's security, mobility of police forces, logistical support, hiring of helicopters, upgradation of police

wireless, satellite communications, crime and CCTNS and e-prisons, for assisting the states to upgrade their police infrastructure to help them tackle emerging challenges.^[30] However, after the recommendations of the 14th Finance Commission, which increased the share of states in central taxes from 32 percent to 42 percent, the central government de-linked eight centrally sponsored schemes from its support in 2015, which included the Modernisation of Police Forces. The official explanation was that with a higher devolution of financial resources to the state government, they should shoulder the additional burden. The central funding for the scheme was thus stopped, but the non-plan funding for the same continued. While the arrangement may be theoretically sound, it could not work practically, since most of the state governments were not interested in investing in the police forces. Thus, the modernisation scheme became a casualty.^[31] Finally, the MHA realised the perils and reverted to the old arrangement of releasing annual funds for modernisation. The Union Home Minister Rajnath Singh stated, “The government had already increased the outlay to states as per the 14th Finance Commission recommendations, from 32 per cent to 42 per cent. It was earlier felt that police reforms would also be funded by states. But today, we have decided to approve the umbrella scheme over and above that.”^[32]

With police reforms taking a backseat, the command-and-control system of the police is also in a state of utter breakdown. The way the police handled the Mumbai terror attacks demonstrates that they are not trained in the task of confronting modern-day terrorism. The attack manifestly revealed the catastrophic weaknesses in India’s police and intelligence apparatus. The poor job was not only due to lack of nerve on the part of the top police leaders but also due to poor command-and-control. The Mumbai Police Commissioner “did not take charge of the situation and allowed all and sundry to jump into the fray and create a chaotic situation.”^[33] In a recent interview, former union home minister, P. Chidambaram disclosed that as both the union home secretary and director of IB were about to retire, he spared them from suspension and instead continued with their knowledge of the situation.^[34]

The failure of intelligence agencies to anticipate major terror attacks and “to apprehend most of those responsible over the years, speaks not just to weak, under-motivated, and under-equipped police forces but also to dubious intelligence capabilities.”^[35] There is a great deal of difference between the failure to collect intelligence and the failure to act on it. Understandably, the outrage is more when such failure to act leads to terrorist disasters, as it happened in 26/11. Sharing of intelligence among various agencies was also a problem, as revealed by Chidambaram. He has lamented that “the complete lack of sharing of intelligence between various organisations was a big problem. The army, navy and other agencies were not sharing their inputs with each other.”^[36] Despite the intelligence warnings delivered to the Mumbai police, one of the reasons it could not act in a professional manner was due to the political environment at the time, which tended to visualise and dismiss terrorism as a North Indian or border-provinces’ problem.^[37]

India’s former prime minister, Manmohan Singh, had underlined the importance of state police and intelligence agencies in the fight against terrorism when he said, in September 2006, “Unless the beat constable is brought into the vortex of our counter-terrorist strategy, our capacity to pre-empt future attacks would be severely limited.”^[38] Prime Minister Narendra Modi, at the Guwahati Conference of the Directors General of Police in November 2014, discussed the concept of SMART Police: a police force that is sensitive, mobile, alert, reliable and tech-savvy.^[39] However, there has hardly been any developments in that direction, since not much has been done to either insulate the police from external influences or improve the orientation and operational capacity of police officers. India’s policing apparatus – the ‘first responders’ in case of any serious internal security threat – remains ill-equipped and substantially unprepared.

Conclusion and Recommendations

In the US, in the aftermath of 9/11, the government appointed a high-powered commission to look into the attacks. In India, no such commission was appointed by the Government of India after 26/11. The BJP’s 2014 election manifesto had emphasised the need to improve India’s internal-security system. In particular, to “[r]eform the National Security Council to make it the hub of all sector-related assessments. It will be accountable for real-time intelligence dissemination ... Completely revamp the intelligence gathering system...”^[40] However, no concrete measures have been taken to improve the capacity-building of police and intelligence agencies. It remains to be seen how, and if, the recent change in the organisational structure of the SPG in the NSC will improve the national-security mechanism.

Despite the 'strong' government at the centre, no attempt has been made to codify India's security doctrine. There does not seem to be any strategic vision for Jammu and Kashmir. As recently underlined by N.N. Vohra, former governor of Jammu and Kashmir, during first K.P.S. Gill memorial lecture organised by the Punjab police, "[The] situation in Kashmir is worsening since 2012. We are managing the war in the state on a day-to-day basis, but nowhere near to stop it."^[41] India's response to daunting internal-security challenges such as terrorism and insurgency has largely been characterised by improvisation and a lack of long-term planning, which has led to meta-institutional innovations and over-centralisation, as well as the state governments abdicating their constitutional responsibilities. Unless India improves the quality and functioning of its entire internal-security apparatus, the country will remain acutely vulnerable to threats.

This paper makes the following recommendations:

- To deal with internal-security threats, the first responders, i.e. the police, need to have modern equipment and training. The scarcity of trained and well-equipped police personnel often results in neglect of professional responsibilities, avoidable "short-cuts" and security lapses.
- Basic training in the police forces must be improved. Successive national commissions have highlighted the need for proper training, which have largely been ignored. At present, low morale is prevalent among the staff and faculty of most police colleges and academies in the country. Trainees are not deriving inspiration. There is a need to post experienced and competent faculty members in these academies, like what is being done in the training institutions of the defense forces. Training institutions in most states also lack basic facilities like a library, classrooms, and equipment. This situation must be corrected.
- Refresher courses must be introduced and implemented at all ranks. Today, police constables constitute 80 percent of the police organisation. After their basic training, they barely receive any in-service training program. This is unfortunate given that the constabulary is at the grassroots and their performance impacts the response to a terror attack or any other serious internal security crisis. The curriculum at police academies should also be constantly updated. The open-source sociopolitical aspects of basic training can be outsourced to experts in the field.
- Local policing is best done by the state police. However, dealing with phenomena such as terrorism, insurgency, organised crime and cyber crime needs coordinated responses.
- There is an acute shortage of cyber specialists in state police and central paramilitary forces, who can continue to work in their area of specialisation after their limited tenures. Even when some officers develop a degree of specialisation in the cyber domain, their next appointment often takes precedence over retaining domain expertise. This must be addressed and resolved.
- The recruitment system in the state and central police organisations leaves much to be desired. Human resource experts are not part of the recruitment committees and there are complaints of corruption and irregularities in the recruitment process. There is an acute need to standardise the norms of recruitment and institutionalise a fair and transparent system of recruitment. An accelerated recruitment drive to fill all sanctioned posts in the police force should be the highest priority within a time-bound framework. The state police forces should be expanded to the 220 police per 100,000 population.
- There is an urgent need for improved counterterrorism coordination between national-level and state-level security agencies. Intelligence flows generated through the state-police apparatus must be coordinated in real time with national databases.
- The government must consider setting up a separate Ministry of Internal Security (MoIS).
- The NCTC must be established and should function directly under the MoIS.

Endnotes

^[1] Theodor H. Winkler, Anja H. Ebnöther, Mats B. Hansson (eds.), *Combating Terrorism and Its Implications for the Security Sector* (Stockholm: Swedish National Defence College, 2005), 158; *A Case for Intelligence Reforms in India*, IDSA Task Force Report (New Delhi: Institute for Defence Studies and Analyses, 2012), 22.

^[2] Prem Mahadevan, *The Politics of Counterterrorism in India: Strategic Intelligence and National Security* (New York: IB Tauris, 2012).

^[3] National Security Council Secretariat (NSCS) has issued a notification recently, according to which

the NSA will now replace the cabinet secretary, who was earlier Chairperson of SPG, a mechanism first notified in 1999.

- [4] B.A. Sahukar, "Intelligence and Defence Cooperation in India," in *Intelligence Cooperation Practices in the 21st Century: Towards a Culture of Sharing*, M. Tuzuner (ed.), (Netherlands: IOS Press, 2010), 31–41.
- [5] Ministry of Home Affairs, [Annual Report 2017–18](#).
- [6] For a review of India's security reforms after the Mumbai attacks, see Sarah J. Watson and C. Christine Fair, "India's Stalled Internal Security Reforms," *India Review* 12, no. 4 (2013): 280–99.
- [7] "[The Terrorist and Disruptive Activities \(Prevention\) Act, 1987](#)", *South Asia Terrorism Portal*.
- [8] "[Dealing With Terrorism: Legal Framework](#)", Government of India, Second Administrative Reforms Commission, Eighth Report: Combating Terrorism, Protecting by Righteousness.
- [9] P.R. Chari, "National Counter Terrorism Centre for India: Understanding the Debate," IPCS Issue Brief No. 181, March 2012.
- [10] Josy Joseph, "Locating NCTC within Intelligence Bureau or not: The debate continues," *Times of India*, 17 July 2012.
- [11] "[NCTC flouts 'sacrosanct' tenet: Nitish](#)", *Telegraph*, 6 May 2012.
- [12] T.N. Raghunatha, "[NIA court frames charges against Purohit, Sadhvi Pragya, others](#)", *Daily Pioneer*, 31 October 2018.
- [13] B. Raman, "[The NCTC Controversy](#)", *Outlook*, 5 March 2012.
- [14] "[Dark Decade in Governance: BJP's Charge Sheet on Congress-led UPA](#)".
- [15] "[NCTC kept in abeyance: govt](#)", *Kashmir Times*, 16 November 2016.
- [16] Sandeep Unnithan, "Anti-terror grid in deep freeze," *India Today*, 25 November 2015.
- [17] Kamaljit Kaur Sandhu, "[10 years post Mumbai 26/11 terror attack, National Intelligence Grid yet to take off](#)" *India Today*, 16 March 2018.
- [18] Press Trust of India, "[CCTNS will help in containing crime and criminality: Ahir](#)".
- [19] Mohd Ujaley, "[Budget 2016 and anti-terror project funding: Will CCTNS catch Arun Jaitley's eye?](#)", *Financial Express*, February 27, 2016.
- [20] "[Digital India: 10 Years And 2,000 Crore Later, Central Government's Online Crime Tracking System Has Little to Show](#)" *Huffington Post*.
- [21] Ajay Sahni, "First responder most neglected part of counter terrorism system," *Hindustan Times*, November 22, 2008, New Delhi, p. 17.
- [22] Ajay Sahni, "[Cops can't wait for special forces](#)", *Times of India*, November 28, 2018.
- [23] PTI, "50 pc of police posts vacant in UP; national average at 24 pc," *India Today*, 2 April 2017.
- [24] "Shortage of police personnel alarming," *Deccan Herald*, 17 February 2017.
- [25] Ved Marwah, "India's Internal Security Challenges," *Strategic Analysis* 27, no. 4 (October–December 2003)
- [26] The Special Investigation Team (SIT) probing the murder of journalist Gauri Lankesh has invoked the Karnataka Control of Organised Crimes Act (KCOCA), which deals with unlawful activities committed by an individual, either as a member of an organised-crime syndicate or on behalf of a syndicate.
- [27] Ravinder Vasudeva, "[Captain Amarinder-led Punjab govt puts PCOCA plans on the back burner](#)", *Hindustan Times*, 11 May 2018.
- [28] "[Name parties with 'criminal' office-bearers: HC](#)", *The Hindu*, 15 November 2018.
- [29] Zee TV, "SC anguished over states' indifference to police reforms," 21 July 2009, http://zeenews.india.com/news/nation/sc-anguished-over-states-indifference-to-police-reforms_549020.html.
- [30] Press Information Bureau, "[Cabinet approves umbrella scheme of Modernisation of Police Forces](#)" 27 September 2017.
- [31] Prakash Singh, "Reforms money can't buy," *Indian Express*, 29 September 2017.
- [32] "For revamp & upgrade: Rs 25,000-crore package for police reforms," *Indian Express*, September 28, 2017.
- [33] Ved Marwah, "The Role of India's Police in Combating Terrorism," in *Combating Terrorism*, Maroof Raza (ed.), (New Delhi: Viking, 2009), 83.
- [34] Harindr Baweja, "India doesn't have capability to pick out Hafiz Saeed," Interview with P. Chidambaram, former Union home minister, *Hindustan Times*, November 22, 2018, New Delhi, p. 17.
- [35] David Malone and Rohan Mukherjee, "Polity, Security, and Foreign Policy in Contemporary India," in *South Asia's Weak States: Understanding the Regional Insecurity Predicament*, T.V. Paul

(ed.), (California: Stanford University Press, 2010), 160.

^[36] Interview with P. Chidambaram, *Hindustan Times*.

^[37] Prem Mahadevan, "Urban Counterterrorist Sieges: The 2008 Mumbai Attack and Police (In) capacity," *Central European Journal of International and Security Studies* 10, no. 2 (2016): 33–56.

^[38] *Yojana*, New Delhi, February 2007, 10.

^[39] "[PM's address at the All India Conference of Directors General/Inspectors General of Police](#)", 30 November 2014.

^[40] [Election Manifesto 2014](#), Bharatiya Janata Party.

^[41] "[Left-wing extremists, radicals' biggest threats, says former Jammu and Kashmir governor NN Vohra](#)", *Indian Express*, 2 November 2018.

SHREYA SHREE
AIR 71 - CSE 2021