

Issues in News - Indian Intelligence Architecture: An Overview

Intelligence agencies are crucial for the general well being of the nation. The agencies are only good as the surrounding architecture that sets them up. Thus it is crucial to know how well structured (or not) these setups are.

In this article, you can read about India's intelligence set up, intelligence architecture and agencies for the IAS exam. This is an important part of the syllabus.

Nature of Security Threats

The country is being faced with a multitude of threats which are mainly due to-

- The geographical location of the country shares borders with unfriendly neighbours like Pakistan and unstable nations like Afghanistan, exposing our nation to the terror groups across the borders.
- The terrorist infiltration through coastal areas is increasing as seen in Mumbai and Gujarat.
- Organised crime networks involving nationals of different countries like smuggling of drugs, human trafficking etc.
- Communal violence and secessionist movements in various states.
- The Government's increasing push for digitisation and the problems associated with it-
- Vulnerability of critical infrastructure like Banking. Ex: The recent ATM hacking which led to sensitive banking information being compromised.
- Lack of awareness of the public about the do's and don'ts over the internet sometimes even threatening the security of the individual.
- Attacks on sovereign infrastructure ranging from stealth of sensitive defense data to breach of aadhar database.
- Attacks on private infrastructure ranging from denial of service to the recent extortion like ransomware(WannaCry).

SECURITY THREATS

Kashmir Insurgency along with cross border terrorism.

Another significant threat is to major cities, the economic hubs of country

Naxalism

Vulnerable coastline



REGIONAL THREATS

Multiple secessionist movements in Northeast

Growing threat of Maoist, now infested in more than three states

TYPES OF THREATS

CYBER CRIMES



- **PHISHING**
Using fake email messages to get personal information from internet users
- **IDENTITY THEFT**
Misusing personal information
- **HACKING**
Shutting down or misusing websites or computer networks
- Spreading **hate and inciting terrorism**
- Distributing **child pornography**
- **GROOMING**
Making sexual advances to minors.
- **Denial of service**
- **ATM Theft**
- **Abuse of Social Media**

1 NAXALISM



2 ORGANISED CRIME



3 CYBER AND DATA THREATS



4 FINANCIAL THREATS



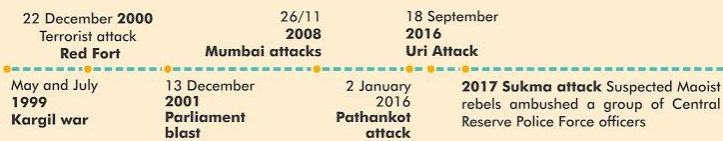
5 BORDER THREATS



6 RELIGIOUS THREATS



A TIMELINE of some major lapses in INTELLIGENCE GATHERING



Facets of Intelligence Gathering

- **Human Intelligence(HUMINT)**– Data gathered by the personnel of the investigating agency through direct involvement in the field of action.
- **Technological Intelligence(TECHINT)**- Tracking and monitoring suspicious activities and individuals through various means like satellite tracking, phone tapping etc.

With the coordination of technological intelligence and human intelligence we can get real time information which is required for action against terrorism threats or any other threats to the country.

Current Intelligence Infrastructure

The major intelligence agencies currently operating in the country include-

- **Intelligence Bureau(IB)** – The Intelligence Bureau specialised agency used to garner intelligence from within India and also execute counter-intelligence and counter-terrorism tasks.
- Counter-intelligence refers to information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations or persons or international terrorist activities, but not including personnel, physical, document or communications security programs.
- Counter-terrorism tasks include political or military activities designed to prevent or thwart terrorism thereby giving a wide remit to the agency.
- **Research and Analysis Wing (RAW)** – A specialised, independent agency dedicated to foreign intelligence gathering.
- **Computer Emergency Response Team (CERT-IN)**- Deals with the Collection, analysis and dissemination of information on cyber security incidents.
- **Directorate of Enforcement (DE)**- An economic intelligence agency responsible for enforcing economic laws and fighting economic crime in India.
- **Directorate of Revenue Intelligence (DRI)**- A major intelligence agency which enforces the prohibition of the smuggling of items including drugs, gold, diamonds, electronics, foreign currency, and counterfeit Indian currency.
- Intelligence units of different states with different mandates. For ex: Maharashtra intelligence unit is concerned with organised crime and smuggling activities while north eastern states also have to deal with secessionist movements.

Concerns about the existing intelligence network

- The changing nature of threats emanating from the Cyberspace and social media like ISIS using secure communications networks to further its propaganda and recruit people online which cannot be tackled through the traditional setup.
- Chronic shortage of specialised personnel coupled with the inefficient use of human resources. Take for instance the IB, a major portion of its human resources gets diverted

doing daily police work like verifications, something that the agency claims it does not do any better than the police forces.

- Intelligence Agencies with different mandates, often overlapping each others', sometimes leading to duplication of efforts and non cooperation between agencies. For Ex: The mandates of RAW and IB with respect to organised crimes like smuggling.
- Intelligence collection is ad-hoc in the absence of clear-cut requirements from the consumers of intelligence.
- Poor cadre management and inability to recruit qualified language specialists and technical skills .
- Lack of intellectual capacity and investment in the education system exacerbate recruitment shortfalls in intelligence agencies. Engaging private players for specialist tasks is therefore necessary.
- Agencies suffer from chronic shortage of military expertise.
- Lack of a comprehensive national level database of suspected individuals. Initiatives like NATGRID are yet to take off due to differences over data sharing between the centre and states.
- Failure to act swiftly over the gathered intelligence by the enforcement agencies due to doubts over credibility of the data , a fact which came to light post the Pathankot air base attacks.
- The country's inability in ending various armed conflicts, be it Naga insurgency or other northern movements or Kashmir militancy exposing the faultlines in our intelligence establishment. Neighbouring countries such as Pakistan and China too have a role in fomenting these movements.
- Inability of the police forces to prevent communal violence and growing fundamentalism in many instances like the muzaffarnagar violence, which is mainly due failure of the traditional intelligence networks.
- Lack of parliamentary statute failing to enforce accountability in intelligence agencies.
- The National Cyber Security Policy which aimed at creating a skilled workforce of 5,00,000 professionals to tackle the growing cyber attacks fails to suggest ways to create such a talent pool.
- Lack of political attention and effective guidance has prevented reform and optimal functioning of the intelligence system.
- The absence of the Chief Of Defense staff has hampered the coordination between the military and other intelligence agencies.

Proposed agencies to help improve the Intelligence Infrastructure

- **NATGRID** will utilize data analytics to process the huge volumes of data generated from the 21 data sources so as to analyse events, match patterns and track suspects. It will help in zeroing in on a suspect by converging and processing all kinds of personal details including medical and financial information, iris, fingerprints and transactions of an individual.

- The National Counter Terrorism Centre (**NCTC**) to draw up and coordinate counter-terrorism plans, integrate intelligence gathering and coordinate with all existing investigating and intelligence agencies.
- The National Cyber Coordination Centre (**NCCC**), which will screen online threats and coordinate with the intelligence agencies to handle issues related to national security.
- The Central Monitoring System (**CMS**) to stop the leakage of information from the service providers' end .The CMS, if implemented, will be connected with the Telephone Call Interception System (TCIS) which will help monitor voice calls, SMS and MMS, fax communications on landlines, CDMA, video calls, GSM and 3G networks.
- The Government has announced in budget 2017 to create a specialised agency **CERT-fin** to counter threats to the financial sector.

Financing the Security Infrastructure

- The Ministry of Home Affairs (MHA) in 2009-10 following the Mumbai terror attacks of November 2008, has been witnessing a steady increase in its allocations over the years in order to-
 - Enhance intelligence gathering.
 - Capacity building of security and law enforcement organisations through strength augmentation.
 - Improved training.
 - Modern weaponry.
 - Technical upgradation.
- In the last three years too, allocations have increased from Rs. 61,401.78 crore in 2014-15 to 73,406.37 crore in 2016-17.
- The enhanced budgetary allocations for the MHA since 2009 reflect the efforts of the successive Union governments to comprehensively overhaul the internal security set up of the country .
- One of the serious internal security threats that the country has been grappling with for more than a decade is left wing extremism (LWE). Although the primary responsibility of fighting LWE lies with the concerned states, the Union government assists them-
 - By providing funds for capacity building through various security related expenditure (SRE) schemes.
- Through increased budgetary allocations under the 'Police' head to prioritise threats and challenges and deal with them in a concerted and sustained manner.
- In lieu of the Government's commitment for Smart Policing, under police modernisation, Rs. 800 crore has been allocated for modernisation of the state police forces.
- The sum includes grants by the Union government to states to strengthen police infrastructure in terms of training, weaponry, mobility and communication, and the establishment of secure police stations.
- It also includes the establishment and upkeep of the crime and criminal network tracking system (CCTNS).

- The Intelligence Bureau (IB), which in recent years has been augmenting its strength, has also received an allocation of Rs. 1,577 crore, an increase of 11 per cent from the previous year.

Possible Solutions

- The Intelligence agencies need to anticipate threats in advance to prevent and mitigate possible security breaches.
- The states must rise above politics in matters of national security to implement crucial initiatives like NATGRID and NCTC.
- A comprehensive law bringing intelligence agencies under parliamentary scrutiny will help in delineating functions of different agencies and enforce accountability to the legislature rather than the present ad-hocism.
- The Central Government should take active steps to ensure inter agency, interstate and centre –state cooperation to plug the information gaps.
- While the revenue outlays have been increasing, the capital outlays have seen troughs and crests in the last four years. Hence, expenditure on expanding manpower has to be balanced by commensurate expenditure on infrastructure like training schools , forensic laboratories, procuring additional vehicles etc.
- The National Cyber Security Policy has to be strengthened to address the skill gap and develop cutting edge/bleeding edge technologies in the upcoming fields of big data and data analytics to detect early patterns of crime and effectively prevent it.

Conclusion

No security network would be strong enough to tackle security threats unless the centre and states focus on intelligence gathering and sharing. A coordinated plan of intelligence gathering involving all stakeholders and dissemination should come into place immediately without any delay so that we can tackle the present challenges effectively.