NATGRID

Mains: *GS-III – Internal Security*

Why in News?

NATGRID, originally conceived after the 26/11 attacks to prevent intelligence failures, has now evolved into a mass surveillance tool that risks undermining privacy, accountability, and democratic oversight.

What is NATGRID, and how has it evolved over time?

- **National Intelligence Grid (NATGRID)** – It is a ***public-private counter-terrorism initiative*** of the central government.
- It is a secure, integrated intelligence-sharing platform between Intelligence Agencies and E-Governance organizations of India.
- It deals with integrating databases from different governments, quasi-government, as well as private organisations of Indian e-governance.
- **Goal –** To strengthen India's internal security by enabling counter-terrorism, criminal investigations, and national security coordination through real-time intelligence sharing.
- **Nodal Ministry –** Under the Ministry of Home Affairs.
- **Legal Basis –** Section 5(2) of the ***Indian Telegraph Act, 1885***, which allows interception during "public emergency" or "public safety" concerns.
- **Premise –** It is a ***middleware platform*** that would allow 11 central agencies to query databases across 21 categories (not an agency itself, but a tool for agencies to query data legally).
- These databases come from providers covering identity & assets, travel & movement, financial records, and telecom data.
- **Origins in 26/11 attacks –** NATGRID was proposed to aggregate fragmented intelligence data (travel records, financial transactions, telecom data) to prevent lapses like those seen during the Mumbai terror attacks.
- It was cleared in 2012 by executive order, not through Parliament, raising constitutional concerns.
- **Function –** It provides a 360-degree view of suspects/events by integrating fragmented data.
- It enables early warning systems and faster identification/prosecution of terror suspects.
- It gives agencies real-time access to key records (immigration, banking, telecom, travel, etc.) to strengthen law enforcement and intelligence work.
- **Significance –** Among the institutional expansions after 26/11, the ***technological***

crown jewel was the National Intelligence Grid (NATGRID).

What happened in NATGRID's 2025 expansion?

- **Expansion of scope –** The first report (after national conference of Directors General of Police in Raipur, Nov, 2025), States were asked to "scale up" NATGRID usage.
- Initially limited to 11 central agencies, now the access has ***expanded to state police units***, including officers at the Superintendent of Police level.
- **Integration with NPR** (National Population Register) – NPR contains details of 1.19 billion residents, mapping households and identities, it is politically sensitive due to NRC debates.
- By linking NPR with NATGRID shifts the paradigm from tracking discrete events as intelligence inputs to the mapping every Indian citizen, raising fears of citizenship filtering and profiling..
- **Advanced analytics** – The deployment of "***Gandiva***", an analytical engine capable of entity resolution, facial recognition, and large-scale inference.
- This moves NATGRID beyond a "search bar" into predictive surveillance, where algorithms infer intentions.
- **Recruitment drive –** New posts were announced - Director-II and Assistant Directors (Project Management, Transit Accommodation, Relationship Management, Capacity Building).
- All positions filled on deputation only, signaling a closed, internal expansion.
- **Operational surge –** NATGRID activity spiked to around 45,000 monthly data requests, showing its growing role in real-time intelligence.
- **Database integration** – It has been integrated with the Passport Seva Programme & Bureau of Immigration, while efforts are underway to connect it with the Crime and Criminal Tracking Network System (CCTNS), enabling nationwide access to police FIRs.

What are the critical concerns about NATGRID?

- **Bias in algorithms** – Algorithms don't just reveal truth; they replicate distortions in the data they process.
- If policing is already skewed by caste, religion or geography, analytics will harden those inequities and wrap them in an aura of objectivity.
- **Impact varies by social position** – For the affluent, a false positive is an administrative nuisance.
- For marginalized groups, already under suspicion, a misidentification can lead to serious ordeals or even fatal consequences.
- **Tyranny of scale –** Modern analytics is dangerous not for omniscience but for ubiquity; queries are classified by sensitivity, and officials claim every access is logged and justified.
- Tens of thousands of queries logged each month, without independent oversight risks turning safeguards into clerical rituals.
- **Life & death claim –** Supporters often argue that NATGRID is essential for national survival, is a matter of life and death. Yet, its drift from counter-terrorism into everyday policing raises doubts.

- **Intelligence failures –** It often arise not from data shortages, but from institutional weakness, perverse incentives, inadequate training, and lack of accountability (e.g., 26/11 - local police hadn't trained with firearms for over a year).
- **Privacy rights –** Our constitutional courts have grown inactive, leaving the broad privacy protections from the ***K.S. Puttaswamy (Retd.) & Anr. vs. Union of India & Ors, 2017*** judgment unused, even as the surveillance state continues to expand.
- **Legality of intelligence programmes –** It lacks any clear statutory foundation or meaningful oversight has not been squarely adjudicated, despite multiple pending cases.
- **Broad "National Security" Clause –** Section 5(2) of the Telegraph Act allows interception during "public emergency" or "public safety," but these terms are vague and open to misuse.
- **Public temper & political rhetoric** – Political discourse and cultural moulding, including mainstream cinema that treats questioning the security establishment as heresy.
- It creates silence on accountability, even after tragedies like the New Delhi bombing (Nov 10, 2025, 15 lives lost) and raises many uncomfortable question.
- **Data protection & security risks** – It integrates sensitive datasets (telecom, immigration, banking, police FIRs, etc.), but citizens don't know which private datasets are included, becomes a high-value target for hacking or insider leaks.
- **Exemption from RTI** – NATGRID is outside the scope of the Right to Information Act, reducing transparency.

What lies ahead?

- **Conditions for true prevention –** It requires professional investigation insulated from political whims, transparency about intelligence lapses, and oversight vested within the parliamentary and the judiciary.
- **Without these safeguards –** NATGRID is an architecture of suspicion, built in the name of safety and normalised through fear, but functioning in the service of digital authoritarianism.

References

1. The Hindu | 'Natgrid', the search engine of digital authoritarianism
2. Geostrata | NATGRID
3. Medianama | NATGRID