5. NATGRID – Internal Security

Authorities started using the National Intelligence Grid (NATGRID) to trace and track suspects and criminals, though several practical challenges remain on the ground

Background and Rationale - The 2008 Mumbai terror attacks (26/11) exposed deep structural weaknesses in India's intelligence ecosystem. A critical failure lay not in absence of data, but in the inability to connect fragmented datasets across agencies. Information related to operatives such as David Coleman Headley existed across immigration, travel, financial, and communication records, yet remained siloed. The post-26/11 reform agenda thus focused on data integration, real-time access, and inter-agency coordination, rather than only manpower expansion. In this context, National Intelligence Grid (NATGRID) was conceived as the technological backbone of counter-terror intelligence.

NATGRID- Concept, Design, and Evolution

NATGRID is a centralised intelligence database housed under the Ministry of Home Affairs (MHA). It aggregates over 24 categories of data, including

1. Immigration and visa records
2. Banking and financial transaction data
3. Telecom and call detail records
4. Travel, rail, and airline data
5. Identity and authentication databases

Conceived in 2008, formally announced in 2009, and operationalised in 2012 through an executive order, not a parliamentary statute. Its original mandate was post-facto intelligence analysis—to help agencies reconstruct networks after suspicious activity was detected.

Recent Developments and Expansion of Scope - NATGRID now reportedly processes around 45,000 queries per month, indicating routine rather than exceptional use. Access has been expanded beyond central agencies to state police officers up to the rank of Superintendent of Police, significantly widening the user base.

Integration with the National Population Register (NPR)—covering approximately 1.19 billion residentsmarks a qualitative shift from targeted intelligence to population-scale data mapping

Technological upgrades include the analytical engine "Gandiva", which enables

1. Entity resolution—linking fragmented records across databases to a single individual
2. Pattern recognition across time, geography, and associations

Cross-referencing of

1. Facial recognition systems
2. KYC and financial databases

This allows predictive and inferential profiling, not merely retrospective investigation.

Key Concerns and Risks

Algorithmic Bias and False Positives - Algorithms trained on biased datasets may replicate or amplify social prejudices related to caste, religion, region, or occupation. Individuals may be flagged as "suspicious" due to associational or demographic patterns, not evidence of wrongdoing. Such false positives disproportionately affect already marginalised communities.

Weak Oversight and Accountability Deficit - With tens of thousands of queries monthly, audit trails and logging mechanisms risk becoming ineffective. There is no independent oversight authority to review

1. Purpose limitation
2. Proportionality of access
3. Abuse or misuse of data

Internal executive control substitutes for judicial or parliamentary scrutiny.

Mission Creep- From Counter-Terrorism to Routine Policing

NATGRID was designed for constitutional-level threats like terrorism. Its expanded access and routine querying risk normalising its use for everyday law enforcement, without statutory safeguards. This blurs the line between exceptional security powers and ordinary policing, undermining rule-of-law principles.

Constitutional and Legal Ambiguity - Intelligence databases like NATGRID operate without a dedicated statutory framework. Courts have not conclusively adjudicated their legality. The Puttaswamy (2017) judgment established

1. Right to privacy as a fundamental right
2. Tests of legality, necessity, proportionality, and procedural safeguards

However, these standards remain under-applied in intelligence governance.

Risk of Digital Authoritarianism - Intelligence failures often stem from institutional weaknesses, poor coordination, and lack of accountability, not data scarcity. Without independent oversight, NATGRID risks becoming a tool of pre-emptive suspicion and surveillance, rather than targeted threat prevention. Concentration of data and discretion in the executive raises concerns of surveillance overreach.

Conclusion

NATGRID was conceptualised as a corrective to the intelligence failures exposed by 26/11, with the legitimate aim of preventing future terror attacks. Over time, however, it has evolved into a mass surveillance architecture, enabled by scale, technology, and widening access. Expansion without clear statutory backing, judicial oversight, or parliamentary accountability risks normalising constant monitoring of citizens.

Effective counter-terrorism requires not only advanced technology, but also

1. Legal clarity
2. Institutional checks and balances
3. Transparency and accountability mechanisms

Without these, NATGRID may undermine the very democratic freedoms it seeks to protect.

Source- https-//www.thehindu.com/opinion/lead/natgrid-the-search-engine-of-digital-authoritarianism/article70483515.ece