The Intelligence Illusion: How AI is Exposing Strategic Vulnerabilities in the Developing World

By
Tahir Mahmood Azad

For decades, intelligence agencies in developing countries, especially in South Asia, have been portrayed as all-knowing, all-seeing, and deeply involved in every part of politics and security. Pakistan's Inter-Services Intelligence (ISI) and India's Research and Analysis Wing (RAW) are often mythologized as all-powerful institutions capable of shaping domestic politics and manipulating regional events. However, this description disguises a basic reality: the traditional human intelligence (HUMINT)–centered model that sustained these agencies is being fundamentally disrupted by artificial intelligence (AI), big-data surveillance, and automated analysis. The actual picture today is not the strength of these institutions but the growing mismatch between their legacy intelligence cultures and the demands of the AI era.

AI has improved intelligence operations in developing nations, but it has also created a new intelligence gap due to disjointed technological implementation, political exploitation of surveillance, reliance on foreign suppliers, and insufficient integration between HUMINT and AI-driven systems. Pakistan and India have large human resources and developing technological ecosystems, but institutional fragmentation and political agendas prevent the development of integrated, modern intelligence frameworks.

The problems that South Asian intelligence services are having are part of a larger global transformation. AI is now a segment of intelligence operation in the US, China, Israel, and some European countries. This includes automated translation, pattern-of-life analysis, algorithmic triage of intercepted data, commercial satellite imagery analytics, and cyber-enabled anomaly detection. China's surveillance state uses AI-powered facial recognition, behavior prediction, and nationwide data fusion to show what a fully integrated intelligence model looks like. The U.S. is pushing for automated signals intelligence (SIGINT) processing and predictive analysis in all its intelligence agencies in the Office of the Director of National Intelligence (ODNI). As shown in studies of its military AI systems, Israel uses AI in real-time targeting and ISR fusion.

Developing countries are just as vulnerable to cyber-attacks, terrorism, and false information, but they do not have the institutional frameworks that let AI grow. This global gap is what makes the changes in intelligence in Pakistan and India so important for strategy. Pakistan and India have both spent resources on AI-enabled surveillance systems like ID databases, CCTV networks, predictive policing tools, interception systems, and cyber technologies that come from other countries. The NADRA database and Safe City projects in Pakistan give a lot of biometric and real-time data. India has made the Central Monitoring System (CMS) and the National Intelligence Grid (NATGRID) to connect databases between state agencies. The ministry, military, police, and intelligence systems are separate. Legacy bureaucracies promote compartmentalization over integration. AI needs centralized databases, clean data, agency cooperation, and agreed analysis criteria. These requirements are missing; hence, AI systems exhibit limited and inconsistent intelligence. Agencies are collecting more data than ever but lack the framework to analyze it.

Pakistan and India still value HUMINT for intelligence. It is crucial for counterterrorism, political spying, and regional operations. HUMINT alone can't compete with hybrid enemies who use AI-driven processing. Strategically, China's integrated military and civilian AI

ecosystem is advantageous. Developing states are stuck between two sources of intelligence: First is a legacy HUMINT system with deep networks and second is an AI ecosystem that is fragmented and not fully developed, so it cannot support strategic analysis. In cross-border threat assessments, cyber invasions, and emerging non-traditional security issues like information warfare, this mismatch causes delays, blind spots, and analytical distortions.

In both Pakistan and India, AI-enabled surveillance has been used more for political purposes than for improving strategic intelligence. Amnesty International reported that India's use of Pegasus spyware targeted journalists, activists, and political opponents. Pakistan has been criticized for using automated social media monitoring and political profiling, which often focuses on threats from within the country rather than threats from other countries. When surveillance tools are used to control political competition within a party, two things happen. First, institutional resources prioritize domestic control over strategic analysis. Second, technology investments strengthen policing instead of updating intelligence. This challenges national security by making it harder for the intelligence system to predict cyberattacks, regional crises, and threats from outside the country.

South Asia has a lot of foreign AI and cyber infrastructure. Pakistan employs Chinese surveillance equipment (Hikvision, Huawei), while India uses Israeli, US, and European and American forensics platforms. This increases structural risks, including data exfiltration and espionage due to entrenched vulnerabilities, strategic reliance on foreign updates, and weakened sovereignty over vital intelligence activities.

Two traditional rivals, nuclear-weapon states, are weakened by this reliance. AI-powered surveillance systems increase digital access points for assault. Big national data repositories attract attackers. Pakistan has had multiple government system hacks, and India has had large breaches that compromised critical infrastructure and government information. Failures in the past were largely caused by human error, but in the AI era, bias in algorithms, data manipulation, hostile and automated cyberattacks, and misclassification can lead to erroneous operational decisions. These dangers make the strategy unstable.

Increasing intelligence gaps between Pakistan and India jeopardize national and regional security. More likely to misjudge opponents: In fast-moving crises, agencies may miss signals, misjudge threats, or misread trends without AI–HUMINT fusion. Cross-border escalation risks rise; poor intelligence integration in nuclearized environments may aggravate misperceptions during crises like the 2019 Pulwama–Balakot incident or the May 2025 standoff. Cyber attacks expose national secrets. Easy-to-get digital network intelligence can have fatal repercussions. China-asymmetric strategic competition: China is decades ahead in intelligence upgrading, and Pakistan and India may fall further. Domestic AI reduces institutional capacity: political survival trumps strategic intelligence.

In summary, countries that do not update their intelligence risk being caught off guard, making mistakes, and becoming more vulnerable. The myths of shadows, secrecy, and huge people networks that fueled emerging country intelligence organizations are gone. AI has highlighted bureaucratic opacity's long-hidden structural flaws: dysfunctional systems, politicized surveillance, reliance on foreign technology, and a lack of HUMINT-AI integration. Thus, Pakistan and India's new intelligence divide is not about data or resources. It is about institutions' failure to transition from analogue intelligence to AI-connected ecosystems. State and non-state adversaries that accelerate this transformation will benefit.

In nuclearized, crisis-prone South Asia, small misunderstandings could lead to massive wars. Pakistan and India need more than AI tools to stay competitive strategically. They need data architectures that work together, technical specialists, protocols to prevent politicians from abusing their authority, and strategic AI–HUMINT fusion.

Dr. Tahir Mahmood Azad is currently a research scholar at the Department of Politics & International Relations, the University of Reading, UK