ARTICLES

The Technological Transformation of India's Northeast Insurgency

Author: Neha Sethi • **Published:** July 17, 2026 • **Source:** Centre for New Age Warfare Studies



EXECUTIVE BRIEF & KEY FINDINGS

Insurgency in Northeast India is no longer shaped only by terrain, local networks and access to conventional weapons. Satellite internet, encrypted communications and commercially available drones are giving insurgent groups new ways to coordinate, evade surveillance, gather intelligence and strike from a distance. As these technologies reduce the operational advantages traditionally held by the state, they are reshaping the character of asymmetric conflict and forcing India to rethink how counterinsurgency is conducted in one of its most strategically sensitive regions.

One of the hotspots of insurgent movements in India has been the North East Region (NER). Although defining insurgency is easier said than done, a commonly accepted characterisation describes it as an organised armed resistance against a constituted authority or the state, undertaken with the objective of challenging, weakening, or overthrowing the existing political order.

While the terms terrorism and insurgency are often used interchangeably, important distinctions exist between the two. Insurgencies typically depend upon mass mobilisation and the support of local elements to achieve their political objectives. Terrorism, although a form of political violence, does not necessarily require popular support to sustain its operations. Additionally, the term terrorism carries a distinctly pejorative connotation. In contrast, concepts such as

guerrilla warfare and insurgency are often perceived as more legitimate due to their historical association with national liberation movements and resistance struggles.

Since gaining independence in 1947, the Republic of India has faced the persistent challenge of insurgency across several regions. North East India has witnessed insurgency, which was primarily driven by ethnic separatist aspirations among several indigenous communities. Notable examples include the Naga insurgency, which began in 1956, the Mizo insurgency of 1966, and the insurgencies and separatist movements that have emerged in Punjab, Jammu and Kashmir, and other parts of NRE.

However, there has been a fresh set of challenges to counter the insurgency in the NER, and one of the prominent topics of discussion remains technological advancement. Cross-border sanctuaries have played a strategic role in enhancing insurgent resilience by reducing the effectiveness of counterinsurgency operations by giving them access to new sets of technologies, allowing groups to recruit, and maintain supply networks. Technological advancement doesn't occur in isolation; it often generates spillover effects across multiple sectors.

The integration of Satellite Internet, Encrypted Communications, and drones in insurgents' operations

Technological advancements in telecommunications facilitated the growth of the Internet, which in turn created the conditions for the emergence and rapid growth of social media platforms. As a result, the technological capabilities of insurgent groups in Northeast India are evolving beyond conventional weapons and communication systems. Increasing access to commercial technologies such as satellite internet and unmanned aerial systems (UAS) has enhanced the operational flexibility of insurgent organisations, enabling them to overcome many of the geographical and infrastructural constraints that historically limited their activities. These developments represent a significant shift in insurgency, requiring corresponding adaptations in counter-insurgency strategy.

India's internet penetration reached 55.3% of the population at the beginning of the year, significantly expanding digital connectivity and access to information. However, this increased connectivity has also facilitated the rapid dissemination of misinformation, proactive messages, and incitement of violence. Such content is capable of undermining public order and national security. In conflict-prone regions, including areas affected by insurgency, such a digital ecosystem can further complicate the security environment. Online platforms may be used to circulate coordinated messaging, used for recruitment or to amplify psychological influence operations, thereby posing additional challenges for law enforcement agencies operating in sensitive areas.

Simultaneously, the widespread adoption of end-to-end encrypted (E2EE) messaging platforms, such as WhatsApp, has reduced the effectiveness of conventional lawful interception and cyber surveillance mechanisms. While encryption plays a critical role in protecting user privacy, it also limits visibility into communications that are relevant for security monitoring in insurgency-affected regions. For example, the rise of internet-based calling services has complicated security operations, largely due to end-to-end encryption that limits lawful interception. In 2018, officials reportedly examined the possibility of restricting WhatsApp calling in insurgency-affected areas over concerns that militants were using it to communicate with handlers across the border. In 2024, a Naga organisation alleged unlawful surveillance and infiltration of private WhatsApp groups by security personnel in an open letter to the Assam Rifles. These instances highlight the growing tension between the operational requirements of state security agencies in insurgency-affected regions

Satellite internet, which provides broadband connectivity through satellites operating in either Geostationary Orbit (GSO) or Non-geostationary Orbit (NGSO), has primarily been promoted as a means of extending digital connectivity to remote and underserved regions. In India, the technology supports the objectives of Digital India by providing internet

access in mountainous terrain and other locations where terrestrial telecommunications infrastructure is either absent or economically unviable. However, the same characteristics that make satellite internet beneficial for civilian connectivity also create strategic advantages for insurgent groups.

Unlike conventional internet services that depend on mobile towers or fibre optic infrastructure, satellite internet operates independently of terrestrial networks and is therefore less vulnerable to local infrastructure disruptions or internet shutdowns. This enables insurgent groups operating from remote forested and border regions to maintain uninterrupted communication, coordinate dispersed units, access online intelligence, and disseminate propaganda despite restrictions imposed on conventional communication networks. The seizure of a Starlink terminal from members of the banned Meitei insurgent organisation, the Revolutionary People's Front (RPF), in Manipur highlights that the satellite internet is being employed by non-state actors like insurgents to overcome security surveillance with the assistance of neighbouring countries.

Starlink, the satellite internet service operated by SpaceX, offers significant connectivity benefits but also raises strategic concerns for India. As a foreign-operated network, it may constrain the government's ability to regulate service availability during security contingencies. These concerns are not unique to Starlink but apply broadly to foreign satellite communication providers.

Alongside advances in communication technologies, insurgent organisations are increasingly incorporating unmanned aerial vehicles (UAVs), commonly known as drones, into their operational strategies. Originally designed for civilian applications such as aerial photography, surveying, and logistics, drones have become inexpensive, commercially accessible platforms that can be adapted for reconnaissance, surveillance, intelligence gathering, logistics, and in some cases, the delivery of improvised explosive devices. Their affordability and ease of acquisition have lowered the technological barriers for non-state armed groups seeking to enhance their operational capabilities.

Reports from Northeast India indicate that several insurgents' organisation have acquired surveillance drones, quadcopters, hexacopters, drone jammers, and related accessories through transnational procurement networks. Similarly, Manipur police have confirmed the use of weaponised drones by Kuki militant groups to deploy explosive devices, while security agencies have expressed concern over the acquisition of drone components by extremist organisations representing both the Meitei and Kuki-Zo communities. These developments indicate that drone technology is no longer confined to state militaries but has become an increasingly accessible force multiplier for insurgent organisations.

What new challenges arise for security forces?

Technology is reshaping the operational capabilities of insurgent groups, enabling them to move beyond conventional guerrilla tactics toward more sophisticated forms of asymmetric warfare. The integration of satellite and drone technologies significantly complicates the operational environment for security forces. Persistent satellite connectivity enables insurgent groups to communicate securely from remote locations, reducing the effectiveness of traditional surveillance methods and communication disruption strategies. Simultaneously, drones expand insurgents' intelligence, surveillance, and reconnaissance (ISR) capabilities by allowing them to monitor troop movements, identify security installations, transport supplies, and conduct attacks without exposing personnel to direct engagement.

Security agencies have warned that insurgent groups are seeking to deploy drones against critical infrastructure, including oil refineries, dams, military installations, and Indian Air Force bases such as Tezpur and Chabua, reflecting a shift from direct confrontation to standoff attacks on strategic assets. The porous international borders shared with Myanmar, Bangladesh, Bhutan, and, historically, China have facilitated the development of these external support systems. Cross border sanctuaries and external assistance enhanced insurgent resilience, highlighting the importance

of regional geopolitical dynamics alongside internal political factors in shaping the conflict. The persistence of external support as reflected in reports from 2017 demonstrates continued Chinese assistance to Naga insurgents through the supply of arms and other forms of support.

Together, these developments suggest that technology is not merely augmenting insurgent tactics but fundamentally changing how such groups organise, sustain operations, and project their capabilities. As a result, traditional counterinsurgency methods focused on controlling territory and blocking ground communication are becoming less effective.

Conclusion

The persistence of insurgency in North East India cannot be explained solely through domestic, political and ethnic grievances. It must also be understood within a broader regional and transnational context. The rapid advancement of emerging technologies has transformed the nature of insurgency by enabling non-state actors to exploit commercially available communication systems, unmanned aerial vehicles (UAVs), satellite internet, and other dual-use technologies. As Artificial Intelligence, quantum technologies, biotechnology, and space-based capabilities continue to evolve, governments will face increasingly complex challenges in preventing their misuse while maintaining an effective technological edge.

However, technology alone does not determine the success of insurgencies. Their resilience is equally rooted in socio-political grievances, local support networks, and in some cases, external assistance. Therefore, an effective counterinsurgency strategy must extend beyond technological superiority and military operations. It should include disrupting insurgents' access to advanced technologies through strengthened border surveillance, intelligence sharing, and regulatory frameworks, while simultaneously addressing the underlying political, economic, and social conditions that sustain insurgent movements. A balanced approach that integrates technological preparedness with inclusive governance is likely to offer the most sustainable response to the evolving character of modern insurgency.

The views expressed are those of the authors and do not represent the views of CNAWS.

Image Source: ChatGPT