

India's Preparedness Against Technological Adaptations of Terrorism

*Saanya Sidhra**

Emerging technologies are redefining terrorism, which is moving away from traditional manpower-intensive forms of violence to a new hybrid form that incorporates digital technology, cyber warfare and drones. This article focuses on exploring India's adaptability to the evolving dimensions of terrorism in relation to technological advancements in the field and international laws that govern the use of drones by terrorists. The main case studies are based on an analysis of the attack at the Air Force Station in Jammu in January 2021 involving drones, and the palpable increase in the smuggling of such drones through the Punjab border between 2020 and 2024.

Situating these developments within broader global trends of technology-driven terrorism, the article assesses India's institutional, regulatory and operational preparedness across counter-UAS frameworks, cyber governance structures, inter-agency coordination, and public-private security integration. Arguing against the grain of reactive, incident-driven responses towards an anticipatory, technology-driven architecture in counter-terrorism, the article concludes by emphasising that in the longer term, India's security resilience will depend on integrated

* Ms Saanya Sidhra is a former Research Intern at the Manohar Parrikar Institute for Defence Studies and Analyses (MP-IDSA), New Delhi, India.

policy reform, technological innovation and cohesive institutional coordination.

Keywords: *Technological Terrorism; Drones and Terrorism; Counter-terrorism preparedness; counter-UAS systems; cyber-terrorism; border-security; Unmanned Aerial Vehicles (UAVs); India's national security architecture*

EVOLUTION OF TECHNOLOGICAL TERRORISM: GLOBAL TO INDIAN CONTEXT

The combination of technology and terrorism has become a serious national security threat in recent years. States have been forced to review their preparedness frameworks due to terrorism's transition to technology-driven operations, including cyberattacks, drone-enabled strikes and encrypted communication. India faces challenges in fending off these modern threats because of its rapidly digitising economy and growing technological footprint. It is essential that cyberspace be secure and resilient. This has been acknowledged by the Ministry of Electronics and Information Technology (MeitY) in its National Cyber Security Policy of 2013, which recognises cyber threats as an increasingly important aspect of national security.¹ Terrorism becoming increasingly adept at technology raises complex operational and policy challenges.² Other emerging tools such as 3-D printed weapons, autonomous vehicles, CBRN-linked delivery systems, and AI-engineered toxins are recognised but not discussed in detail here, because they remain largely nascent in India or lack verified instances of use by terrorists.

The expanding technological toolkit at the disposal of terrorist organisations extends across a variety of different domains, as indicated in Table 1.

Table 1 Emerging Technological Tools Used in Contemporary Terrorism

Category	Examples of Use by Terrorist Groups	Relevance to the Indian Context
Cyber Operations	Hacking of government databases, ransomware campaigns, cyberattacks on critical infrastructure	AIIMS-Delhi ransomware attack (2022) highlighted critical infrastructure vulnerability

Online Radicalisation and Propaganda	Use of encrypted messaging platforms like Telegram and WhatsApp among other social media recruitment networks	ISIS-inspired modules in India using encrypted communication platforms
Unmanned Aerial Systems (UAVs)	Surveillance drones, weaponised drones, cross-border smuggling of drugs and arms	Jammu Air Force Station drone attack (2021) and repeated drone smuggling along the Punjab border
Artificial Intelligence and Deepfakes	Disinformation campaigns, AI-generated propaganda, automated bot networks	Enhanced risk of AI-driven influencing operations and digital radicalisation
Financial Technologies	Use of darknet marketplaces, cryptocurrency and anonymous digital wallets	Illicit procurement and use of virtual currencies for terror financing
Emerging Physical Technologies	CBRN delivery systems, 3D-printed weapons and autonomous vehicles	Currently limited use against India has been verified but still pose major future risks

Source: Compiled by the author using global terrorism and Indian security reports.

Among the technologies listed above, unmanned aerial systems (UAVs) are already operational, repeatedly observed crossing the border into India via drone infiltrations, and also at the time of the Jammu Air Force Station incident in 2021, thus making UAVs the primary focus of this article.

State-sponsored cyber operations and digital radicalisation shape the broader digital threat environment, within which terrorist groups operate and often replicate techniques.

India needs to be prepared to tackle situations where cyber-enabled attacks, disinformation campaigns, or remote technological disruptions could supplement or even replace traditional terror tactics. This article therefore treats State-sponsored activity as a parallel trend that influences terrorist capabilities. India's readiness needs to be assessed not only through its current regulatory framework but also by its ability to quickly adapt to new technologies, coordinate across agencies, and form partnerships with the

private sector. Such agility will determine how effectively India stays ahead of evolving technology-enabled threat vectors.

Against this backdrop, the article examines the preparedness of India's national security system *vis-à-vis* the issue of technology-upgraded terrorism, especially the use of unmanned aerial systems (UAS), cyber-attacks, and digital media by terrorist groups and their proxy agents. Recent developments, including the drone attack on the Jammu Air Force station and the increasing trend of drone-based smuggling activities along the Punjab border, have been covered in detail.

A key aspect of this examination is the capacity to 'connect the dots'. Effective responses to terrorism require the integration of various intelligence, regulatory and technological capabilities from various stakeholders, including the Ministry of Home Affairs (MoHA), the Ministry of Defence (MoD), and security and research agencies. The issue is no longer about technology being available, but the extent to which technology is integrated and operationalised through a unified national counter-terrorism strategy.

Early in the 21st century, terrorism started to move away from traditional strategies like bombings and armed attacks, towards more dispersed, technologically enabled forms of disruption, violence and propaganda. This new era, often referred to as 'technology-driven terrorism', resulted from the proliferation of inexpensive UAS/drones, the globalisation of encrypted communications, growing cyberattacks targeting vital infrastructure and the ability of social media to mobilise and radicalise.³ Terrorist groups have already shown how technology can increase their capabilities and capacities. The Islamic State of Iraq and Syria (ISIS) used online propaganda networks, encrypted platforms like Telegram and social media to radicalise young people, plan attacks, and disseminate operational manuals.⁴ Research reveals that in order to recruit foreign fighters and spread instructions for lone-wolf attacks, ISIS established a sophisticated 'digital jihad' ecosystem using Twitter, YouTube and specialised online forums.⁵ This change is further demonstrated by terrorist organisations' misuse of drones. To target military positions, the ISIS in Iraq and Syria, drop grenades and carry out reconnaissance with repurposed, commercially available drones. Originally intended for civilian use, these drones evolved into inexpensive precision weapons for asymmetric warfare, demonstrating how non-State actors can weaponise readily available technologies,⁶ leading to the increasing hybridisation of terrorism.⁷

As these techniques proliferate, they are no longer restricted to conflict areas in Eastern Europe or West Asia. Their spread throughout South Asia shows how quickly extremist actors modify instruments created elsewhere to

fit local circumstances. In India, cross-border groups like Lashkar-e-Taiba (LeT), Jaish-e-Mohammed (JeM) and pro-Khalistan extremist networks have already adapted global tactics of using drones for weapon drops, exploiting encrypted applications for recruitment and coordination, and amplifying propaganda through social media ecosystems aimed at specific Indian fault lines, among other techniques.⁸

These worldwide patterns are now proliferating in India, in regionally specific ways, compelling the government to improve its counter-UAS systems, in light of the 2021 drone attack on the Air Force Station in Jammu and other cross-border UAS incidents.⁹ Drone routes across Punjab and Jammu have been customised for low-altitude, short-duration flights that bypass Indian radar signals; dropped payloads range from small arms to IED components, fake currency and narcotics—a fitting example of how groups have adapted the use of drones to India's border terrain and local networks.¹⁰ Also, the terrorist handlers based in Pakistan have started using end-to-end encrypted communication platforms and VPNs (Virtual Private Networks) to coordinate with the ground workers in India, thereby reflecting a regionally adapted model of digital terrorism.¹¹ The drone attack in 2021 proved to be a significant case of technological terrorism, revealing concerns about India's real-time detection, interdiction and response mechanisms against low-altitude, small-payload unmanned systems. This incident showed that low-cost, commercially available drones that can avoid detection, GPS-jammed areas, and conventional air defence systems, are still a threat to even the most secure military installations. Crucially, it exposed the lack of an agency-wide counter-UAS protocol, the restricted use of Radio Frequency (RF) sensors and anti-drone jammers, and the requirement for standard operating procedures (SOPs) for perimeter security.¹²

The increase in cross-border drone smuggling incidents along the Punjab border between 2020 and 2024 highlight a different but equally serious aspect of technological terrorism: the systematic use of UAVs for weapons, explosives, drugs and communication payloads. This is in contrast to the Jammu attack, which showed the kinetic potential of drones. By taking advantage of the loopholes in India's border surveillance networks, night vision coverage and counter-UAS coordination between the Border Security Force (BSF), state police and intelligence agencies, Pakistan-based groups have institutionalised drone-based supply chains that evade conventional detection grids, thereby increasing the frequency of such interceptions.¹³

Together, the drone attack in Jammu and the surge in border smuggling in Punjab show how India is facing a range of technological terrorism,

from one-time kinetic attacks to long-term infiltration networks. In light of this, the article evaluates how well India's present institutional structures, technological capabilities and policies address these threats. The article identifies operational gaps, new vulnerabilities, and the structural changes needed to create a robust, future-ready counter-terrorism architecture, by assessing preparedness across detection systems, inter-agency coordination, border management and the larger cyber-digital domain.

INDIA'S EMERGING THREAT LANDSCAPE

There is the growing threat scenario in India, of new actors leveraging the fast-paced new technologies on the exponentially expanding surveillance capacity of the internet. This is also evident in the increasing use of hybrid forms of cyber-cum-UAV (drone) attacks, and end-crypto platforms by the ISIS.¹⁴ This also includes the ransomware attack on AIIMS-Delhi in 2022 that caused national health emergencies.¹⁵

Extremist ecosystems are also evolving virtually in the form of encrypted communication channels, algorithmic propaganda spreading tools, and online radicalisation in a decentralised manner, as evident in NIA-constated ISIS-inspired modules in Telangana and Kerala, that did not require any organisational set-up. Moreover, the quick proliferation of generative artificial intelligence (AI) tools would only add to these risks, as they can disseminate disinformation, create propaganda, use deep fake to manipulate influence operations, and would fall under the category of 'white-collar' terrorism.¹⁶ This is accompanied by a lack of accountability in terror financing in the form of virtual currencies, darknet markets, and anonymous money wallets that facilitate fund exchange as well as purchase operations, despite strict Anti-Money Laundering (AML)/ Know Your Customer (KYC) norms in Decentralised Finance (DeFi) platforms, Privacy Coins, peer-to-peer transactions and international virtual currency exchanges.¹⁷ This sets the stage for a virtual, multi-dimensional threat environment in spite of well-established counter-terror paradigms.

Recent incidents are a testimony to the dynamic nature of technology-facilitated terrorism in India. In one such incident, a car bombing in the Red Fort in November 2025, carried out by a module of educated professionals, was facilitated by the use of advanced digital tradecraft, including the use of end-to-end encrypted communication tools such as 'Threema', dead drop email, and advanced explosive technology.¹⁸ These incidents are a testimony to the evolution of 'white-collar terrorism', wherein a group of technically

skilled professionals use their expertise in digital technology to avoid being detected by the anti-terrorist response matrix.

EMERGENCE OF DRONES IN INDIA'S BORDER SECURITY ARCHITECTURE

Drones, also known as UAVs, are aircraft that are controlled remotely or by autonomous systems and have become essential tools in modern border management. For monitoring large and challenging terrain, their small size, operational flexibility, ability to launch from confined spaces, and capacity for persistent surveillance and precision strikes offer significant advantages.¹⁹ The Indian Army, the BSF and the Indo-Tibetan Border Police (ITBP) oversee border security in India. All the three agencies have progressively integrated drones into their operational frameworks.²⁰ Border management mostly uses smaller drones, although the Indian Army has a varied drone fleet that includes tactical UAVs and medium-altitude long-endurance platforms. In a similar vein, the BSF and ITBP use lightweight UAVs for real-time surveillance, to identify terrorist infiltration, illegal immigration and cross-border smuggling of weapons, drugs, counterfeit currency and other contraband. Drones are more and more useful, but operational, legal and security issues hamper their effective integration.²¹ Their increasing use in civilian applications, including land surveys, infrastructure monitoring and agricultural services, has led to a rapid expansion of the Indian drone market, which comprises manufacturers, training institutions, service providers, digital regulatory platforms and a unified governance structure.

This rapid growth in the Indian ecosystem for drones has been enabled by various regulatory and skill-building initiatives that support pilot training, drone certification, and integration with various aspects of governance and infrastructure monitoring using UAV technology. Various government initiatives such as the SVAMITVA (Survey of Villages Abadi & Mapping with Improved Technology in Village Areas) programme have used drones to survey more than 3.2 lakh villages, thereby highlighting the scale at which this technology is being used in Indian governance.²²

CASE STUDIES: DRONES AS THE NEW VECTOR OF CROSS-BORDER TERRORISM

A significant change in the security environment between India and Pakistan occurred between 2020 and 2024, as terrorist organisations began using drones more frequently for cross-border operations. Drones provided

militants with a secret, unmanned and untraceable method to move weapons, drugs and surveillance payloads across the international border (IB) and Line of Control (LoC), in contrast to conventional infiltration routes.²³ Drones allowed adversaries to 'strike without crossing the fence', enabling low-cost but high-reward operations, as security agencies have repeatedly noted.²⁴ This evolution is the core of India's current threat landscape: non-State actors are now repurposing technological tools at a never-before-seen pace, which were previously only available to militaries. The cumulative trend in J&K and Punjab shows that India is dealing with a growing technological theatre of terrorism that goes against established doctrines and preparedness frameworks, rather than being just isolated drone incidents.

However, the increasing drone activity along the western border must also be seen in the larger context of Pakistan's changing strategy of proxy war against India. Over the last decade or so, the security apparatus of Pakistan and the terrorist organisations that operate in tandem, have increasingly begun to use UAVs to carry out anti-India operations. Lashkar-e-Taiba (LeT), Jaish-e-Mohammed (JeM) and the pro-Khalistan organisations have used drones to carry out cross-border movement of arms, explosives, narcotics, as well as communication equipment. This strategy has helped the terrorist organisations to sustain their operations in India while minimising the risks of infiltration for militants. Unlike conventional infiltration, where militants would cross the border to carry out operations in the adversary's territory, the use of drones has helped the Pakistani security apparatus to direct their proxy organisations in India, remotely. Thus, the use of drones as a tool of asymmetric warfare against the Indian security apparatus has increasingly gained favour.

On the other hand, India has simultaneously been developing a structured national drone ecosystem with training institutions, pilot certification and digital governance. Currently, India has over 38,500 registered drones and close to 40,000 DGCA (Directorate General of Civil Aviation) remote pilots²⁵

JAMMU AIR FORCE STATION ATTACK: THE FIRST CONFIRMED DRONE TERROR STRIKE IN INDIA

In the early hours of 27 June 2021, two small UAVs, believed to have been built using commercial off-the-shelf components, broke into Air Force Station Jammu, and dropped homemade explosives inside the high-security technical area. Investigators subsequently concluded that the attack was planned from

across the border, with militants using remote piloting techniques to fly the drones across the LoC without compromising a single foot soldier.²⁶

The event exposed a significant technological advancement in terror tactics. Due to their small size, inability to be detected by traditional radar systems, and their ability to deliver payloads precisely, the drones were able to get past perimeter defences that would normally prevent human infiltration.²⁷

The attack highlighted a paradigm shift proving that non-State actors could remotely target high-value military installations. It exposed the limitations of traditional perimeter security and air defence systems. This changes the threat landscape, because small, low-cost drones can deliver precise payloads under cover of darkness, transforming civilian-grade technology into tactical weapons. Large-scale infiltrations and mass-casualty bombings are no longer the only risks. Security agencies were compelled to re-assess their airbase security procedures, after several drones were allegedly spotted over nearby military zones in the days after the strike. Apart from the incident at Air Force Station, Jammu, various other incidents involving drones have been reported from other areas of J&K. Security forces near Kathua, Samba and the Jammu region have intercepted drones carrying small arms, explosives and narcotics. Various incidents of drones have also been reported near the LoC, indicating the increasing use of UAVs for surveillance and logistical activities.

Thus, our counter-UAS architecture must be urgently upgraded, radar and RF-based drone detection systems must be deployed, standardised layered air defence measures must be put in place around vital installations, and inter-agency protocols must be able to react quickly to asymmetric aerial threats.²⁸ India needs to be ready for a hybrid threat environment where cyber tools, drones and remote operations are key components of terror tactics, in addition to traditional terror mechanisms. The Jammu case study provides a blueprint and a wake-up call apart from being a retrospective account of a single incident.

THE PUNJAB BORDER: A PARALLEL SURGE IN DRONE SMUGGLING (2020–2024)

The attack in Jammu was a symbolic escalation, but at the same time, there was a persistent increase in drone activity along the Punjab border, which demonstrated how thoroughly terrorist organisations had incorporated UAVs into their supply chains. Such drone sightings and arms drops suggest that UAV-assisted infiltration is now a regional strategy in India's north-

western border region. Along the 553-km India–Pakistan border, the BSF observed an exponential rise in drone sightings and recoveries since 2020. -The security forces had reportedly intercepted almost 200 drones and seized significant amounts of heroin by 2023 alone.²⁹

The scale of this trend is visible in the sharp increase in drone-related smuggling incidents and interceptions along the Punjab sector of the India–Pakistan border in recent years, as shown in Table 2.

Table 2 Rising Drone-Related Smuggling and Interceptions Along the India–Pakistan Border (Punjab Sector)

Year	Drone-Related Smuggling Incidents	Drones Intercepted / Recovered	Narcotics / Arms Seizures (Indicative)
2020	Initial cases reported	Limited recoveries	Early narcotics drops detected
2021	Three documented drone-drug smuggling cases	Several drones seized	Drugs and small arms recovered
2022	Rising interceptions across Punjab border districts	Dozens of drones intercepted	Heroin and ammunition consignments seized
2023	Significant spike in drone sightings	200 drones intercepted by BSF	287 kg heroin seized
2024	179 drone-driven smuggling cases reported	Continued interceptions across border districts	Multiple consignments of drugs and weapons

Source: Compiled from BSF operational reports and media reporting, including *The Hindu* and *Hindustan Times*.

The trend also demonstrates the transformation of drone-assisted smuggling activities from being isolated occurrences into an institutionalised cross-border logistics network by terrorist and organised criminal organisations.

According to investigations, many of the recovered UAVs were Chinese-made quadcopters with high-capacity batteries, GPS modules, and specially designed compartments for payload drops, which frequently amounted to 5–10 kgs of drugs per sortie. The BSF found drones with night-vision cameras in several instances, suggesting an increasing number of attempts to avoid Indian ground patrols. In order to arrange landing zones, pick-up times and retrieval locations, handlers in Pakistan frequently used cross-

border WhatsApp and VoIP communication with local Indian accomplices, according to Punjab Police and NIA case files.³⁰ Furthermore, repeated interceptions in Amritsar, Tarn Taran and Ferozepur between 2022 and 2024, point to an institutionalised drone-based supply chain run by Pakistan-based organisations, with networks connected to Khalistani networks and LeT, implicated in multiple seizures.³¹

This pattern indicates that drones now underpin an organised cross-border smuggling ecosystem. They are no longer merely a platform for kinetic terror attacks. This reflects increasing technological sophistication among adversarial networks, and the increasing threat to India from intermittent attacks to a continuous, low-cost, high-volume infiltration model that can support organised crime and terrorism. However, rather than continuing the Jammu attack pattern, this increase in drone-enabled smuggling represents a distinct technological threat stream. The analysis must make a clear distinction between (a) the hardware-centric threat, where drones facilitate kinetic attacks or logistical supply chains, and (b) the cyber-digital threat, which includes cyber intrusions, online radicalisation, encrypted communications, and AI-enabled influence operations, in order to prevent forcing an artificial link between unrelated domains. Even though they both develop concurrently, they do not form a single convergent trajectory unless they are combined with other technologies like autonomous systems, 3D-printed weapons, or AI-enhanced targeting. This conceptual division highlights the fact that India is dealing with a variety of technological threat ecosystems. When taken as a whole, these developments demonstrate that the Punjab region has turned into a testing ground for persistent drone-enabled infiltration. The pattern in Punjab reveals an equally hazardous operational trend, in contrast to the Jammu strike, which showed the kinetic potential of drones: the development of UAV-based supply networks intended to take advantage of weaknesses in India's radar coverage, inter-agency coordination and night surveillance.

INDIA'S INSTITUTIONAL AND POLICY RESPONSE

The Jammu Air Force Station drone attack and overall escalation in drone-aided smuggling activities along the Punjab border have contributed substantially to improved counter-drone and technology-based security frameworks in India. Since 2021, the Government of India has enhanced its overall counter-UAS readiness framework through steps entailing regulatory, operational, as well as institutional efforts. The Drone Rules, 2021, and

subsequent amendments by the Ministry of Civil Aviation (MoCA) and the Bureau of Civil Aviation Security have brought about tougher regulations around protected airspace, digital tracking arrangements, registration and geo-fencing, as well as regulated approval mechanisms for drone operations around defence sectors. These activities have also seen the development and implementation of Unmanned Aircraft System Traffic Management regimes as well as site-specific aviation circulars, which help integrate monitoring efforts around drone activities, thereby improving overall security situational awareness through increased monitoring efforts following a security event like that in Jammu.³² These are complemented by digital governance platforms and skill development initiatives to support pilot certification, training infrastructure, and the integration of drones into civilian and security applications within India.³³

From an operational perspective, the applications/implementation of counter-UAS systems have been integrated with, and made a part of, the overall security and border control apparatus in India. The defence forces, BSF, and central security establishment entities have begun the process of integrating counter-drone surveillance, intercept missions, and radio frequency scans with air base and border protection strategies and objectives. The National Security Guard, defence forces, and the respective technical teams now conduct regular security exercises and vulnerability scans as far as the use of drones in illicit activities is concerned, and the NIA, state police, intelligence organisations and BSF, conduct investigations and probe drone-smuggling activities.³⁴

Simultaneously, India's preparedness to address technology-related, cyber-mediated facets of terrorism has also improved through institutional arrangements for supporting the safeguarding of critical information infrastructure. The Indian Computer Emergency Response Team (CERT-In) is involved in issuing real-time advisories, notifications, vulnerability analyses, and coordination warnings for public and strategic actors.³⁵ Besides this, CERT-In is the primary national incident response centre for responding to major computer security incidents involving government as well as private sector computer networks. However, the effectiveness of the response mechanism is hampered due to the delay in reporting the breach, lack of information sharing, and the level of preparedness of the ministries as well as the state-level organisations. The National Critical Information Infrastructure Protection Centre (NCICI PC) issues sectoral advice and undertakes security coordination in sectors such as energy, finance, telecommunications, transport and healthcare.³⁶ The significance of NCICI

PC's role lies in the fact that these sectors form the backbone of India's national infrastructure. However, the coordination between NCICI PC, the sectoral regulators, and the private infrastructure operators, is not always balanced. These institutional responses are reinforced through national-level policy documents, including the Information Technology Act, 2000, the National Information Security Policy, or National Information Security Policy Guidelines (NISPG). The overall combined effect of these is towards attribution, response and preparedness in situations where cyber operations, encrypting communications, or cyber/digital platforms, are involved in terror activities.³⁷ There have been a number of cyber incidents that prove the vulnerability of critical infrastructure despite these frameworks. The ransomware attack at AIIMS, Delhi is one such example.

Taken together, these developments have certainly boosted the institutionalisation of counter-drone governance in India. In this context, it is noteworthy that India's newly developed counter-terrorism strategy framework, PRAHAAR, offers a significant doctrinal guideline.³⁸ The strategy focuses on an intelligence-driven approach to prevention, improved coordination between different agencies, and a whole-of-government approach to counter-terrorism. By focusing on the aggregation of national capacities and information-sharing between different agencies, it aims to institutionalise a more integrated and proactive approach to counter-terrorism. Placing India's technology-based counter-terror preparedness within this framework would ensure the alignment of the country's responses with its developing national security strategy. The ongoing mismatch between the rate of technological diffusion and the rate of regulatory response is a major obstacle to India's readiness. This is particularly true in the cyber domain, where policy development may take place at a slower pace than the evolving threat environment. While the National Cyber Security Policy (2013) and the Cyber Crisis Management Plan (2019) provide institutional roles and response mechanisms, their effective implementation is inconsistent across ministries, states and private sector organisations. Despite being intended to liberalise India's UAV ecosystem, the Drone Rules (2021) were only implemented following the first confirmed drone terror attack at the Jammu Air Force Station in June 2021, which was widely reported as the country's first UAV-enabled strike on a military facility.³⁹ The Rules created regulatory blind spots with regard to drone tracking, component importation, operational altitude limitations, and counter-UAS deployment, despite streamlining permissions and introducing digital sky mechanisms. Acknowledging these shortcomings, the government has now taken steps to replace the 2021 Rules with a specific

legislative framework, the Civil Drone (Promotion and Regulation) Bill, 2025, indicating a move towards more stringent regulations, mandatory certification and registration, and criminal penalties for unapproved drone operations. This legislative update highlights how long India has operated under reactive rather than proactive policymaking, but it also presents a chance to close prior regulatory gaps.⁴⁰ The Bill introduces criminal penalties for unauthorised drone use, including cross-border operations, and strengthens compliance requirements by requiring mandatory registration, remote identification, pilot authorisation, and operator certification. These provisions fill in a number of gaps left by the 2021 Rules, including the lack of statutory support for counter-UAS protocols and the lack of enforceable deterrence mechanisms. The action, however, also demonstrates India's ongoing propensity for reactive policymaking: significant reforms are only implemented in response to recurring operational incidents, an increase in drone-smuggling cases, and ongoing security alerts from border authorities. The Bill offers a chance to unify oversight, but its success will depend on the development of technical capacity to support remote-ID, geo-fencing, and real-time airspace monitoring systems, prompt rule-making, and inter-agency coordination for enforcement.

The increasing overlap between cyber operations and terrorism has made India's preparedness more complex. Terrorist groups increasingly use encrypted communication tools, online propaganda networks, and digital financial networks to coordinate their activities and radicalise individuals. This necessitates the integration of cybersecurity agencies, intelligence agencies, and law enforcement agencies to counter these challenges within India's counter-terrorism framework.

POLICY GAPS AND CHALLENGES

While significant progress has been made since the release of the National Cyber Security Policy (NCSP 2013) and Drone Rules (2021), India's preparedness remains uneven due to implementation gaps, fragmented institutional responsibilities, and limited inter-agency coordination. The NCSP 2013, which strongly emphasises 'creating a secure cyber ecosystem', strengthening public-private partnerships, and safeguarding critical information infrastructure (CII), serves as the foundation for India's cyber preparedness framework. However, many of its fundamental mandates, such as integrated information-sharing mechanisms, sector-specific cyber audits, and mandatory breach disclosure, remain only partially implemented across

ministries and crucial sectors, leading to disparities in preparedness.⁴¹ The Cyber Crisis Management Plan (CCMP)-2019, which outlines response procedures for major cyber disruptions, replaced India's CCMP (2014) in the face of rapidly changing technological threats.⁴² The updated CCMP-2019 was distributed to all central ministries, departments, states/UTs, and related organisations.

However, there has been little institutional adoption of the 2019 plan: it has not been systematically internalised through frequent multi-agency drills, standardised SOPs, or updated resource requirements, nor has it kept up with new challenges like AI-driven attacks, deep fake-enabled disinformation, and ransomware, targeting vital services.⁴³ This exposes structural limitations in India's cyber crisis-readiness framework, as coordination between CERT-In, NCICI PC, sectoral regulators, and state agencies frequently takes place reactively during crises, rather than through established, well-exercised mechanisms.

Real-Time Tracking Challenges

The lack of a dependable real-time tracking system for both civil and security-operated UAVs is a significant obstacle to the use of drones for border management. Drones performing surveillance and other border-related tasks encounter challenges with identification and airspace integration in the absence of such systems. It is challenging for air defence operators to discern between friendly and hostile platforms in real-time when border-guarding forces operate their drones alongside rogue or unidentified civilian UAVs in the absence of authorised real-time tracking. This lack of on-board identification capabilities, particularly in sensitive border areas, complicates the timely neutralisation of hostile drones and creates operational ambiguities.

Similarly, the cases of Jammu Air Force Station and smuggling through drones in Punjab demonstrate that there is no strong and real-time identification and tracking system in place for UAVs that are functioning in strategic border regions and military skies. In Jammu, the hostile UAV's operating altitude overlapped with those of friendly UAVs and without proper Remote ID and live-tracking capabilities, it was impossible to clearly distinguish between friendly, hostile, and 'unknown' UAVs.⁴⁴ Alongside this, in Punjab's border regions, BSF seizures also took place in regions where 'unknown' UAVs cannot successfully or conclusively be identified in real-time, owing to unproved and hence unapproved tracking system combinations of Ground Control Station, GPS, satellite communications, and Sim Card-based connectivity in accordance with DGCA norms.

Although facilities such as Ground Control Systems, GPS, via satellite communication, as well as SIM-based cellular communication, are capable of facilitating real-time tracking, the DGCA is yet to completely test, approve and certify these facilities.

Absence of Unmanned Traffic Management (UTM)

The current Air Traffic Services (ATS) system is designed to operate with manned aircraft and is not well adapted to handling large numbers of drones at low altitudes. A functional UTM system will allow authorities to track authorised UAVs in real-time and more easily detect unauthorised and hostile drones. A deployed functional UTM system, integrated with real-time tracking on permitted drones, would allow for the continuous monitoring of compliant UAVs and greatly enhance the capability of air defence operators to identify, segregate, and neutralise rogue or hostile drones when necessary.

The smuggling ring in Punjab had drone flights going back and forth, which could neither be constantly monitored and distinguished from the permitted flights of UAVs since there was no interactive UTM system established to track legitimate and indicate those flying without notification or notification and compliance.⁴⁵ Similarly, the Jammu case again showed that security personnel did not have a unified common operational picture between authorised and unauthorised UAV operations in and around the facility.

Although policy structures for the management of UTM exist, none are operational. Operationalisation of a national UTM system architecture, especially one that integrates with military detection systems, would greatly enhance awareness and facilitate quicker detection of unauthorised drone operations. There is, therefore, a paramount need for a military-specific UTM architecture, which should incorporate collaborative detection, for real-time tracking of benign drones, alongside non-collaborative detection methods such as low-altitude radars and electro-optics to detect slow, low-altitude, uncooperative UAVs.

Integration of Drones with Air Defence (AD) Networks

One of the important operational issues related to drone-assisted border management is the meagre inclusion of small UAVs into the air defence (AD) systems in India. Being developed by Bharat Electronics Limited (BEL), along with the Integrated Air Command and Control System (IACCS) of the Indian Air Force for the Indian Army, the AD system named Akashteer

is intended to provide real-time airspace situational awareness; however, it does not include small drones for border security purposes yet.⁴⁶ This would need the real-time transmission of the operational locations of authorised drones to the AD systems, allowing for easier separation of friendly, fake and hostile drones into separate categories. This is limited by the lack of any policy for their integration, the lack of real-time tracking on drones, the non-operationalisation of UTM systems, and the inability to transmit real-time positional information about drones into AD systems.⁴⁷

The Jammu incident took place below the radar and beyond the surveillance range optimised for manned aircraft; thus, neither the Akashteer system nor the IACCS system was able to build an integrated, composite picture of the small drone threats operating at low altitudes in the surroundings of the target site.⁴⁸ On the Punjab border, the authorised patrol drones of the Central Armed Police Forces (CAPFs) similarly do not provide real-time positional information to the system, thus inhibiting the automatic discrimination of friendly, simulated and hostile UAVs operating simultaneously.

Upgradation of Counter-UAS (CUAS) Systems

Counter-UAS (CUAS) systems aim to identify, locate and neutralise small unmanned aircraft systems that may not be detected by traditional air defence systems, which are designed to detect fast-flying high-flying aircraft.⁴⁹ In contrast, small UAVs operate at low speeds and altitudes, can be launched from confined spaces, and are easy to deploy, complicating detection and interception. Furthermore, most of the current CUAS capabilities lack the requisite capability to reliably detect friendly versus adversarial drones.⁵⁰ Therefore, existing CUAS systems require major upgradation for improving detection accuracy, identification and assured neutralisation of rogue or hostile UAVs in border areas.

As seen in the Jammu case, a commercially available drone got past the protected zone and delivered explosives successfully. In Punjab, a smuggling ring showed successful border crossing patterns that were detected only when the drones were recovered and not when they had successfully infiltrated. Such patterns reveal the need to develop trustworthy systems of detection, identification and differentiation between friendly and unfriendly drones, and collaborative development of CUAS modernisation in the armed forces and the CAPFs.

Despite the continued development of CUAS technologies, existing systems have limitations in detecting low-altitude UAVs and distinguishing

hostile and authorised drone flights.⁵¹ CUAS systems deal with the drone threat, which cannot be effectively detected by air defence systems.

Equally important is interoperability between civilian and military airspace control systems. A formalised data transfer between civilian and military systems is required in this regard to enable the separation of airspace, and identify malicious drones. At present, a lack of formalised data-sharing procedures between civilian air aviation control systems and military air defence systems is another factor that inhibits threat identification.⁵²

Addressing this gap calls for the coordinated implementation of UTM systems with the involvement of the MoCA, the armed forces, CAPFs, and defence R&D agencies. It is a critical function for capable UAV use and a credible defence system for armed and autonomous UAVs.

Fragmented Institutional Coordination <Level B>

The lack of a cohesive national cyber strategy still restricts interoperability between CERT-In, NCICI PC, National Technical Research Organisation (NTRO), and state cyber police cells, ten years after the National Cyber Security Policy (2013).⁵³ Such a fragmented structure significantly slows information sharing between agencies. CUAS operations are shaped by a similar coordination gap, where ambiguity arises during real-time drone incursions due to overlapping authority between the IAF/AFC (military airspace) and state police, DGCA, and anti-terror units (civilian airspace).⁵⁴ In the crucial early minutes of a hybrid attack, these ambiguous lines of command impede decision-making, leading to redundant assessments, uneven early warning, and delayed neutralisation. Moreover, despite NCSP 2013's emphasis on public-private collaboration, India's private digital infrastructure operators remain insufficiently embedded in national counter-terror protocols, leaving key capabilities under-utilised.⁵⁵ While India has developed a strong regulatory base, the rapidly evolving nature of technological terrorism demands an integrated and anticipatory security architecture rooted in real-time, rather than the current compartmentalised model. These coordination issues are compounded in the states, which have varying institutional capabilities, technical expertise, and effectiveness in implementing their own set of regulatory measures in the design of national counter-terror mechanisms.

Underdeveloped Public–Private Integration in Cyber and Technical Security

The private sector owns and runs more than 80 per cent of India's digital infrastructure, but it is still not well integrated into the counter-terrorism

frameworks, according to MeitY's NCSP 2013⁵⁶ and CERT-In advisories. Cyberattacks on telecom networks, healthcare facilities and financial institutions show that private organisations frequently lack standardised cyber-audit frameworks, real-time coordination channels with national agencies, and mandatory threat-sharing obligations.⁵⁷ India's cyber-defence ecosystem will remain fragmented and susceptible to hybrid terror operations in the absence of institutionalised public-private partnerships, especially in industries like Fintech, cloud computing and telecommunications.

To deal with these challenges, there is a need to focus on a technology-driven and well-coordinated effort. The Ministry of Civil Aviation (MoCA) should focus on the development and implementation of enabling technologies including remote identification and UTM technology.⁵⁸ The progress made through the iDEX scheme, Mehar Baba Swarm Drone Competition and the indigenisation-based defence procurements, has helped in the advancements of drone and CUAS technology.⁵⁹ However, the next priority should be on the border force's adoption and inculcation of this technology, as the nature of the threat has increasingly begun to merge the differences between the challenges being posed in the aerial as well as the land-based security domains.

It is imperative that MoCA focuses on developing, validating and integrating such supporting technologies like remote identification and UTM solutions. At the same time, it is important that the BSF, ITBP and other CAPFs establish their own drone and anti-drone networks that are integrated with the Indian Army's CUAS' Akashteer Air Defence systems, as well as the IACCS of the IAF.⁶⁰ As the management of borders increasingly involves confronting challenges that are a result of land-based security concerns, as compared to more complex challenges that are driven by the low-key use of drones by rival nations for smuggling or other aggressions, it is important to ensure coordination between the institutions.

The proliferation of armed Small Unmanned Aerial Systems (sUAS) poses an acute security challenge for India, especially in terms of terrorist response, management of the borders, and securing strategic infrastructure. Technological progress in commercial drones along the lines of miniaturisation, autonomy and affordability has made them conducive for reconnaissance, delivery and precision strike missions, performed at low-level flights with radar and thermal signatures, low enough to go past established air defence systems intended for supersonic manned platforms. This gets further aggravated by the possible exploitation of 'drones swarms' that could create a huge asymmetry between the costs of 'attack' and 'defence'.⁶¹

In the Indian scenario, the danger of armed sUAS is more pronounced given the long, unguarded land borders, high-rise quasi-urban areas, as well as the mingling of military strategic assets with high-value civilian ones. There have been several instances where cross-border intrusion of drones, especially along the western frontier, have proved that these drones can be effectively utilised for surveillance, smuggling of arms and drugs, as well as kinetic strikes.⁶² Easy access to 'armed drones' also poses a credible risk of being employed by terrorist or insurgent groups for the execution of targeted assassinations or attacks on strategic installations. As evident in previous risk assessments, the asymmetric characteristics of sUAS warfare cause a disadvantage to the defender, given that conventional air defence assets, as well as expensive interceptors, are inadequate for engaging these aerial threats that are 'small, slow, & cheap'.⁶³

RECOMMENDATIONS

Although the following recommendations are assembled along short-term, medium-term and long-term timelines for analysis, the dynamic nature of technologically enabled terrorism dictates a response strategy that is less linear. The pace of technological advancement and its availability to non-State actors compresses response times and dictates a concurrent evolution of policy, technological, operational and institutional elements. India must transition from reactive counter-measures to an anticipatory technology-driven security architecture.

Short-term (0–2 years): Enhancing Detection, Regulation and Rapid Response

In the short term, India needs to concentrate on addressing operational weaknesses brought to light by events like the drone attack in Jammu in 2021 and the ongoing drone incursions throughout Punjab. This necessitates the quick expansion of low-altitude surveillance capabilities, including the installation of CUAS systems such as RF jammers and electro-optical tracking units, across vulnerable border belts and vital infrastructure, as well as the deployment of radar systems that are specifically calibrated to detect small UAVs. At the same time, India needs to bolster the Drone Rules 2021's regulatory framework, particularly by enforcing mandatory UAV tracking, component-level licensing, and stricter import restrictions on expensive drone parts that are commonly used by smugglers from Pakistan. Furthermore, as suggested in India's 2022 Parliamentary Standing Committee Report

on Home Affairs, which identified coordination gaps as a critical national security vulnerability, central and state agencies should adopt common SOPs for drone interdiction.⁶⁴

Medium Term (2–5 years): Building Integrated Architecture and Domestic Technological Capability

India must develop an integrated national counter-technology terrorism architecture over the medium term, taking inspiration from global models like the United States CISA's Joint Cyber Defence Collaborative (JCDC)⁶⁵ and the EUROPOL TE-SAT Fusion Centre.⁶⁶ In order to monitor drones, cyber intrusions, darknet activity and encrypted propaganda networks, this architecture should combine intelligence from IB, NTRO, NIA, NCICI PC, CERT-In, BSF, and the armed forces, into a single real-time coordination platform. Systemic improvements are also necessary for cyber readiness: The cyberattack on AIIMS-Delhi in 2022 revealed India's lack of forensic preparedness and digital redundancy.⁶⁷ India should create a national framework for responding to ransomware, mandate cyber hygiene audits for vital industries (healthcare, power, telecom and finance), and institutionalise cyber-forensics training in frontline agencies over the course of the next five years. Additionally, as India develops its domestic technological capabilities, new tools like AI and machine learning can be used to improve predictive analysis. They can be used to map the evolution of extremist online ecosystems, identify patterns in drone flight paths, or detect anomalous network behaviour prior to a cyberattack. Early warning, quicker threat correlation, and more targeted response would be possible by integrating these capabilities into the national architecture.

Long term (5+ years): Building an Anticipatory Counter-Terror Posture

India will eventually need to switch from an incident-driven security model to a proactive, intelligence-driven counter-terrorism approach. To do this, a continuous, overlapping detection grid that can detect autonomous swarms, micro-UAVs and GPS-spoofing systems, must be established across the western border as a national low-altitude radar and sensor mesh. A Public–Private Security Consortium (PPSC), a national platform that links government cybersecurity agencies with significant private sector operators and is modelled after CISA-JCDC, should also be institutionalised in India.⁶⁸ Lastly, India's long-term counter-terrorism strategy needs to incorporate emerging technologies like deepfake detection, drone-forensics labs, behavioural analytics, and AI-assisted threat prediction. Extremist

networks are quickly embracing AI-enabled deception, autonomous drones and cyber-physical attack tools, according to UNODC⁶⁹ and NATO COE-DAT⁷⁰ reports. Therefore, India needs to improve its information resilience architecture in order to combat the increasing abuse of digital platforms for radicalisation and extremist propaganda. This entails setting up an integrated information-monitoring cell that can identify early indicators of online radicalisation, cross-platform extremist narratives, and misinformation produced using AI. Increased cooperation with technology firms is necessary to create automated detection tools and early warning systems that identify dangerous content before it spreads. Targeted digital literacy initiatives for at-risk youth can strengthen society's resistance to deceptive online messaging. In order to ensure that accurate narratives reach the public before misinformation spreads the government should implement rapid-response communication protocols to combat deepfakes, false-flag content, and coordinated disinformation campaigns during crises.

ENHANCING GLOBAL INSTITUTIONAL AND TECHNOLOGICAL COOPERATION

The manner in which India must counter and address the ever-unfolding CUAS scenario demands institutionalised coordination between the MoCA, MoD, and CAPF to overcome the civil/military gap in managing low-altitude airspace.⁷¹ There needs to be an overall national CUAS strategy that can effectively determine and establish a joint/mutual understanding on perceived threats, roles, and rules of engagement. It is important that acquisition strategies focus on acquiring comprehensive integrated CUAS solution sets and be less platform-dependent, allowing us to quickly modify and update our responses based on changing threats and scenarios. Indigenisation needs to be more focused through technology transfer and investment in research and development and long-term acquisition commitments to the private and MSME sectors.⁷²

A shift from being merely reactive to offering a doctrine-developed and fully networked CUAS solution is necessary, integrating it fully with UTM, tracking systems and cyber-electronic warfare networks, to contend adequately with drone attacks and technology-assisted terrorism in Indian conditions. The present deficiency in detection and common awareness and tracking capabilities results in reduced operational efficiency and hinders rapid action response to congested and class-C air zones.⁷³ Enhanced preparedness requires rapid development and implementation plans by sensors to detect

and differentiate civilian, friendly and unfriendly drones through electro-optic/infra-red and RF sensors through sensor-fusion technology, to deal with autonomous and swarm drones. The neutralisation capabilities have to balance scalable soft-kill options—RF/GNSS jamming, spoofing and electronic disruption—with hard-kill solutions like kinetic interceptors, high-energy lasers and microwave systems, while minimising collateral risks. These technological advances should be anchored in a dedicated national CUAS doctrine, standardised procurement and deployment frameworks, faster acquisition cycles, and joint command-and-control mechanisms across services and CAPFs.⁷⁴ Finally, sustained indigenous Research and Development (R&D), coupled with integration of CUAS networks into civil UTM and air-defence grids, will become operationally effective capabilities against evolving drone and cyber-enabled threats.⁷⁵ Accordingly, India's counter-terrorism strategy needs to be adaptive, iterative and evolutionary in nature.

CONCLUSION AND STRATEGIC OUTLOOK

From the 2021 drone attack at Air Force Station Jammu and the development of a drone-enabled smuggling network in India's western frontier, it is evident that new technologies are changing the face of terror operations. The aforementioned incidents showcase how available technologies can be modified by terrorist organisations for espionage and asymmetric attacks at a relatively low threat level. In these instances, the application of drone technology transcends its mandate in providing a capability for signature-less attacks on military objects to its enablement of the decentralised logistics chains of militant movements in the transfer of weapons, narcotics, funds and IED components across the Indian border. The technology-driven narratives converge to suggest vulnerabilities in surveillance coverage in the lower strata of the skies, the reactive applications of CUAS measures on an ad-hoc basis, ambiguities pertaining to the application of the Drone Rules of 2021, along with a lack of coordination among the various agencies of the Indian state in diverting the crisis-driven strategy to a doctrine-driven framework of preparedness in the face of the quantum leap in UAS-related threats.

The Jammu drone attack as well as the Punjab drone smuggling case highlight the speed at which hostile actors innovate in contrast to the slower institutional pace of procurement, regulation and policy reform. They also reveal persistent gaps in India's cyber-forensic capabilities, intelligence fusion, inter-agency coordination and counter-UAS coverage. However,

India's course is dynamic. An evolving strategy that increasingly reflects the complexity of technology-enabled terrorism is indicated by investments in counter-drone systems, increased cyber monitoring, increased protection of critical infrastructure, and growing collaboration with private technology partners. An indicator of this can be seen in the expansion of India's regulated drone environment and training programmes, which not only points to an increasing capacity to deal with UAV technology but also to an increasing regulatory environment. India must move from incremental reforms to an integrated technology-driven security posture. The findings of the current study suggest a larger structural problem facing India's security architecture. This problem is the rate of technological advancement among adversary states/countries surpassing the rate of institutional adaptation. Although India has developed a set of regulations, CUAS programmes, and cyber security agencies, the success of such programmes depends on the integration of technological capabilities, intelligence agencies and operational doctrines. This can be achieved not only through the improvement of technology, but also through institutional reform.

It is clear that India's future readiness against technology-enabled terrorism would be based on its ability to foresee emerging threat vectors instead of just reacting to them. This would necessitate continued investment in indigenous technology capabilities, enhanced CUAS capabilities, improved cyber resilience, and cooperation between government agencies, technology companies and research institutions. As technologies including AI, autonomous systems and advanced cyber capabilities continue to advance, integrating technology foresight into Indian security would be a critical dimension of its counter-terrorism strategy. Recent doctrinal developments, such as the PRAHAAR strategy, only serve to reinforce the need to integrate institutional capabilities through a whole-of- government and whole-of-society approach.

In the end, the security resilience of India will depend not only on eliminating the existing challenges but also on being able to anticipate the next round of technological disruptions that will define the future of terrorism. To ensure that the State stays ahead of adversarial actors utilising the future of technology more quickly than ever before, it will be crucial to strengthen this anticipatory posture across policy, institutions, intelligence and innovation.

NOTES

1. *National Cyber Security Policy – 2013*, Ministry of Electronics and Information Technology (MeitY), Government of India, New Delhi, 2013, available at

- https://www.meity.gov.in/static/uploads/2024/02/National_cyber_security_policy-2013_0.pdf, accessed on 27 November 2025.
2. 'Countering Cyber Terrorism: Public-Private Partnership — Need of the Hour', Observer Research Foundation, 20 May 2016, available at <https://www.orfonline.org/article/countering-cyber-terrorism-public-private-partnership-need-of-the-hour#:~:text=There%20are%20few%20takeaways%20for,security%20will%20become%20a%20reality>, accessed on 27 November 2025.
 3. 'Technology and Terror: A New Era of Threat in a Borderless Online World', Observer Research Foundation, 21 May 2019 available at <https://www.orfonline.org/expert-speak/technology-and-terror-a-new-era-of-threat-in-a-borderless-online-world-51079>, accessed on 27 November 2025.
 4. Antonia Ward, 'ISIS's Use of Social Media Still Poses a Threat to Stability in the Middle East and Africa', Commentary, RAND Corporation, 11 December 2018, available at <https://www.rand.org/pubs/commentary/2018/12/iss-use-of-social-media-still-poses-a-threat-to-stability.html>, accessed on 27 November 2025.
 5. Imran Awan, 'Cyber-Extremism: ISIS and the Power of Social Media', *Society*, Vol. 54, April 2017, pp.138–149, available at <https://doi.org/10.1007/s12115-017-0114-0>, accessed on 27 November 2025.
 6. Christina Schori Liang, 'Preventing Terrorists from Using Emerging Technologies', *Vision of Humanity*, Institute for Economics & Peace, 11 September 2023, available at <https://www.visionofhumanity.org/preventing-terrorists-from-using-emerging-technologies/>, accessed on 27 November 2025.
 7. Shravishtha Ajaykumar, 'Emerging Technologies in the Development and Delivery of CBRN Threats', Issue Brief No. 768, Observer Research Foundation, December 2024, available at <https://www.orfonline.org/public/uploads/posts/pdf/202411227111028.pdf>, accessed on 27 November 2025.
 8. 'Annual Report 2022-23', Ministry of Home Affairs, Government of India, New Delhi, 2023, available at https://www.mha.gov.in/sites/default/files/AnnualreportEnglish_04102023.pdf, accessed on 23 January 2026.
 9. Sameer Patil and Raj Arora, 'Countering Hostile Drone Activity on the India-Pakistan Border', Issue Brief No. 640, Observer Research Foundation, May 2023, available at <https://www.orfonline.org/public/uploads/posts/pdf/20240610195421.pdf>, accessed on 23 January 2026.
 10. Surjit Singh, 'BSF Seized 200 Drones, 287 kg Heroin along Indo-Pak Border So Far This Year', *Hindustan Times*, 15 October 2025, available at <https://www.hindustantimes.com/cities/chandigarh-news/bsf-seized-200-drones-287-kg-heroin-along-indo-pak-border-so-far-this-year-101760471748858.html>, accessed on 23 January 2026.
 11. '10 Held in J&K for Using Encrypted Apps to Aid Terror; Pak Handlers Guiding Them, Say Officials; Police Seize Digital Evidence in UAPA Case', *The Times of India*, 19 July 2025, available at <https://timesofindia.indiatimes.com/india/10-held-in-jk-for-using-encrypted-apps-to-aid-terror-pak-handlers-guiding-them-say->

- officials-police-seize-digital-evidence-in-uapa-case/articleshow/122782493.cms., accessed on 23 January 2026.
12. R.K. Narang, 'Counter Drone Systems: An Opportunity for Self-Reliance', India Foundation, 6 September 2021, available at <https://indiafoundation.in/articles-and-commentaries/coounter-drone-systems-an-opportunity-for-self-reliance/>, accessed on 23 January 2026.
13. Surjit Singh, 'BSF Seized 200 Drones, 287 kg Heroin along Indo-Pak Border So Far This Year', n. 10.
14. 'Comprehensive Update on Terrorist Financing Risks 2025', Financial Action Task Force (FATF), Paris, 8 July 2025, available at <https://www.fatf-gafi.org/en/publications/Methodsandtrends/comprehensive-update-terrorist-financing-risks-2025.html>, accessed on 23 January 2026.
15. 'Ransomware Attack on AIIMS a Conspiracy Planned by Forces That Are Significant, MoS IT Chandrasekhar Says', *The Hindu*, 2 December 2022, available at <https://www.thehindu.com/news/cities/Delhi/ransomware-attack-on-aiims-a-conspiracy-planned-by-forces-that-are-significant-mos-it-chandrasekhar/article66214950.ece>, accessed on 23 January 2026.
16. 'Confronting White-Collar Terrorism in India', Observer Research Foundation, 5 December 2025, accessed on 23 January 2026.
17. 'Major Terror Bid Foiled as NIA Busts Kerala-based ISIS Module', *The Times of India*, 20 July 2023, available at <https://timesofindia.indiatimes.com/india/major-terror-bid-foiled-as-nia-busts-kerala-based-isis-module/articleshow/101994421.cms>, accessed on 23 January 2026.
18. 'Suspects Used Encrypted Swiss App to Share Maps, Plans for Delhi Blast Probe', *Hindustan Times*, 13 November 2025, available at <https://www.hindustantimes.com/india-news/suspects-used-encrypted-swiss-app-to-share-maps-plans-for-delhi-blast-probe-101763052818934.html>, accessed on 23 January 2026.
19. R.K. Narang, 'Integration of Small Drones for Effective Border Management by India', in Debojit Mazumder (ed.), *Seemanta' 25: A Collection of Articles on Effective Border Management*, Seemanta Chetana Mancha Purvottar, Guwahati, 26–27 July 2025, available at <https://www.idsa.in/wp-content/uploads/2025/09/rknarang-Drones-for-Border-Management-red.pdf>, accessed on 23 January 2026.
20. Ibid.
21. Ibid.
22. 'India's Drone Ecosystem: From Policy to Public Service Transformation', Backgrounder, Press Information Bureau, Government of India, 17 February 2026, available at <https://www.pib.gov.in/PressReleaseDetailm.aspx?PRID=2228954®=3&lang=2>, accessed on 23 January 2026.
23. 'Drone-Driven Drug Smuggling Cases Along India-Pakistan Border Skyrocket from three in 2021 to 179 in 2024, Says NCB Report', *The Hindu*, 16 September 2025, available at <https://www.thehindu.com/news/national/drone-driven-drug-smuggling-cases-along-india-pakistan-border-skyrocket-from-three-in-2021-to-179-in-2024-says-ncb-report/article70057513.ece>, accessed on 25 January 2026.

24. Sameer Patil and Raj Arora, *Countering Hostile Drone Activity on the India-Pakistan Border*, n. 9.
25. 'India's Drone Ecosystem: From Policy to Public Service Transformation', n. 22.
26. 'India Probes Suspected Use of Drones in Blast at Jammu Air Base – Officials', *Reuters*, 27 June 2021, available at [https://www.reuters.com/world/india/india-probes-suspected-use-drones-blast-jammu-air-base-officials-2021-06-27/#:~:text=SRINAGAR%2C%20June%2027%20\(Reuters\)](https://www.reuters.com/world/india/india-probes-suspected-use-drones-blast-jammu-air-base-officials-2021-06-27/#:~:text=SRINAGAR%2C%20June%2027%20(Reuters),), accessed on 19 November 2025.
27. Sushant Sareen, 'Drone Terror Attack on Jammu Airport: A Deadly and Dangerous Dare', Observer Research Foundation, 30 June 2021, available at <https://www.orfonline.org/research/drone-terror-attack-on-jammu-airport-a-deadly-and-dangerous-dare>, accessed on 20 November 2025.
28. 'National Counter Rogue Drone Guidelines', Directorate General of Civil Aviation, Ministry of Civil Aviation, Government of India, 18 October 2019, available at https://www.civilaviation.gov.in/sites/default/files/migration/Counter_rogue_drone_guidelines_NSCS.pdf, accessed on 20 November 2025.
29. Surjit Singh, 'BSF Seized 200 Drones, 287 kg Heroin along Indo-Pak Border So Far This Year', n. 10.
30. Harpreet Bajwa, 'BSF Shares List of 136 Drone-Using Drug Traffickers with Punjab Police', *The New Indian Express*, 1 December 2024, available at https://www.newindianexpress.com/nation/2024/Dec/01/bsf-shares-list-of-136-drone-using-drug-traffickers-with-punjab-police?utm_source=copilot.com, accessed on 20 November 2025.
31. 'BSF Countermeasures Help near Pakistan Border in Punjab: 4 Drones Crash, Seized', *The Times of India*, 22 April 2025, available at <https://timesofindia.indiatimes.com/city/chandigarh/bsf-countermeasures-help-near-pakistan-border-in-punjab-4-drones-crash-seized/articleshow/120496790.cms>, accessed on 20 November 2025.
32. 'Drone Rules, 2021, G.S.R. 589(E), notified under the Aircraft Act, 1934', Ministry of Civil Aviation, Government of India, 25 August 2021, available at <https://thc.nic.in/Central%20Governmental%20Rules/Drone%20Rules,%202021.pdf>, accessed on 20 November 2025.
33. 'India's Drone Ecosystem: From Policy to Public Service Transformation', n. 22.
34. Manish Godha, 'NIA Files Chargesheet Against Pakistan-Linked Kingpin Using Drones to Smuggle Arms, Drugs Into India', *The Free Press Journal*, 15 November 2025, available at https://www.freepressjournal.in/india/nia-files-chargesheet-against-pakistan-linked-kingpin-using-drones-to-smuggle-arms-drugs-into-india?utm_source=copilot.com, accessed on 20 November 2025.
35. 'About CERT-In', Indian Computer Emergency Response Team (CERT-In), Ministry of Electronics and Information Technology (MeitY), Government of India, available at <https://www.cert-in.org.in/>, accessed on 29 January 2026.
36. 'NCIIPC: It's Time to Step Forward and Protect Our Critical Infrastructures from Cyber Attacks', *The Hacker News*, 27 January 2017, available at <https://>

- thehackernews.com/2017/01/protect-critical-infrastructure.html., accessed on 29 January 2026.
37. 'Home', Ministry of Electronics and Information Technology (MeitY), Government of India, available at <https://www.meity.gov.in/>, accessed on 29 January 2026.
38. 'National Counter-Terrorism Policy and Strategy: PRAHAAR', Ministry of Home Affairs, Government of India, 23 February 2026, available at https://www.mha.gov.in/sites/default/files/PRAHAAREng_23022026.pdf, accessed on 29 January 2026.
39. 'India Probes Suspected Use of Drones in Blast at Jammu Air Base – Officials', n. 27.
40. 'Draft Civil Drone (Promotion and Regulation) Bill, 2025', Ministry of Civil Aviation, Government of India, 16 September 2025, available at <https://www.civilaviation.gov.in/sites/default/files/2025-09/Draft%20Civil%20Drone%20%28Promotion%20and%20Regulation%29%20Bill%202025.pdf>., accessed on 29 January 2026.
41. *National Cyber Security Policy – 2013*, n. 1.
42. 'Cyber Crisis Management Plan (CCMP) Launched to Deal with Cyber-Related Incidents', Press Information Bureau, Ministry of Electronics & Information Technology (MeitY), Government of India, 22 February 2019, available at <https://www.pib.gov.in/PressReleasePage.aspx?PRID=1565959>., accessed on 29 January 2026.
43. Ibid.
44. Sushant Sareen, 'Drone Terror Attack on Jammu Airport: A Deadly and Dangerous Dare', n. 27.
45. Surjit Singh, 'BSF Seized 200 Drones, 287 kg Heroin along Indo-Pak Border So Far This Year', n. 10.
46. 'Akashteer: The Unseen Force behind India's New War Capability', Press Information Bureau, Ministry of Information & Broadcasting, Government of India, 16 May 2025, available at <https://www.pib.gov.in/PressReleasePage.aspx?PRID=2129132®=3&lang=2>, accessed on 29 January 2026.
47. Ibid.
48. Sushant Sareen, 'Drone Terror Attack on Jammu Airport: A Deadly and Dangerous Dare', n. 28.
49. Bradley Wilson, Shane Tierney, Brendan Toland, Rachel M. Burns, Colby Peyton Steiner, Christopher Scott Adams, Michael Nixon, Raza Khan, Michelle D. Ziegler, Jan Osburg and Ike Chang, 'Small Unmanned Aerial System Adversary Capabilities', RAND Corporation, 2020, available at https://www.rand.org/content/dam/rand/pubs/research_reports/RR3000/RR3023/RAND_RR3023.pdf, accessed on 31 January 2026.
50. Ibid.
51. Ibid.

52. 'Unmanned Aerial Systems and Counter-Unmanned Aerial Systems: Challenges and Opportunities for India', *Air Power Journal*, Vol. 19, No. 3, 2024, available at <https://journals.capsindia.org/index.php/apj/article/view/5>, accessed on 31 January 2026.
53. R.K. Narang, 'Integration of Small Drones for Effective Border Management by India', n. 19.
54. Ibid.
55. Swapnil S. Kumare, 'Evaluating the Effectiveness of India's National Cyber Security Policy (2013) in the Era of AI and IoT', *International Journal of Creative Research Thoughts*, Vol. 12, No. 11, November 2024, available at <https://www.ijcrt.org/papers/IJCRT2411878.pdf>, accessed on 31 January 2026.
56. *National Cyber Security Policy – 2013*, n. 1.
57. 'Telecommunication Sector Advisory', Maharashtra Cyber, Government of Maharashtra, available at <https://mhcyber.gov.in/documents/20117/84669/Telecommunication+Sector+Advisory.pdf>, accessed on 31 January 2026.
58. R.K. Narang, 'Integration of Small Drones for Effective Border Management by India', n. 19.
59. Ibid.
60. R.K. Narang, *India's Quest for UAVs and Challenges*, KW Publishers Pvt Ltd., New Delhi, 2020, available at <https://www.perlego.com/book/3538185/indias-quest-for-uavs-and-challenges-pdf>, accessed on 31 January 2026.
61. R.K. Narang, 'Armed sUAS Swarm: Big Threat of Small UAS – C-sUAS Development and Threat Mitigation by India', *Asian Defence Review*, 2019, available at <https://im.rediff.com/news/2021/jul/armedsuaswarmbigthreatofsmalluas.pdf>, accessed on 31 January 2026.
62. Ibid.
63. Ibid.
64. '240th Report on "Action Taken by Government on the Observations/Recommendations of the Committee on Petitions"', Rajya Sabha Secretariat, Parliament of India, 2022, available at https://dspstg.sansad.in/getFile/rsnew/Committee_site/Committee_File/Press_ReleaseFile/15/169/645P_2023_5_17.pdf, accessed on 31 January 2026.
65. 'Joint Cyber Defense Collaborative', Cybersecurity and Infrastructure Security Agency (CISA), available at <https://www.cisa.gov/topics/partnerships-and-collaboration/joint-cyber-defense-collaborative>, accessed on 31 January 2026.
66. 'European Union Terrorism Situation & Trend Report (EU TE-SAT) 2025', Europol, Publications Office of the European Union, 2025, available at <https://www.europol.europa.eu/publications-events/main-reports/tesat-report>, accessed on 31 January 2026.
67. 'Ransomware Attack on AIIMS a Conspiracy Planned by Forces That Are Significant, MoS IT Chandrasekhar', *The Hindu*, 2 December 2022, available at <https://www.thehindu.com/news/cities/Delhi/ransomware-attack-on-aiims>

- a-conspiracy-planned-by-forces-that-are-significant-mos-it-chandrasekhar/article66214950.ece., accessed on 31 January 2026.
68. 'Joint Cyber Defense Collaborative', n. 65.
 69. 'UNODC Launches Report to Assist Member States to Counter the Use of the Internet for Terrorist Purposes', *UNODC News*, 23 October 2012, available at <https://www.unodc.org/unodc/en/frontpage/2012/October/unodc-launches-report-to-assist-member-states-to-counter-the-use-of-the-internet-for-terrorist-purposes.html>, accessed on 31 January 2026.
 70. "Emerging Technologies and Terrorism: Emerging Threats in the Next Five to Ten Years", NATO Centre of Excellence Defence Against Terrorism (COE-DAT) and United States Army War College Strategic Studies Institute, 2024, available at <https://www.nspcoe.org/wp-content/uploads/2024/07/DATCOE18-EmergingTech.pdf>, accessed on 31 January 2026.
 71. R.K. Narang, 'Armed sUAS Swarm: Big Threat of Small UAS— C-sUAS Development and Threat Mitigation by India', n. 61.
 72. Ibid.
 73. R.K. Narang, *India's Quest for UAVs and Challenges*, n. 60.
 74. Ibid.
 75. Ibid.