Countering Hostile Drone Activity on the India-Pakistan Border

Sameer Patil and Raj Arora

Abstract

Drone or unmanned aerial vehicles (UAVs) technology has become more accessible and affordable in recent years, and their increasing long-range capability, endurance, and applications, have made them integral for both civilian and military uses. At the same time, malicious elements such as criminal networks, drug smuggling syndicates and terrorist organisations, have exploited the technology to aid their activities. For India, the increased use of UAVs by smuggling syndicates and terrorist groups on the western border has emerged as a new challenge for national security. This brief examines the nature of hostile drone activity on the India-Pakistan border, discusses the countermeasures being taken by the security establishment, and recommends steps that India can take to mitigate this challenge and strengthen border security.
With their capability to provide real-time intelligence, surveillance and reconnaissance and carry payloads of different kinds that enable limited targeting, drones have become a significant tool for militaries and non-state actors alike. The rapid evolution of drone or Unmanned Aerial Vehicle (UAV) technology—and, in particular the increasing affordability of mini and micro drones—has led to their rapid proliferation, including among rogue non-state and proxy actors. India’s Ministry of Civil Aviation, in its ‘National Counter Rogue Drone Guidelines’ issued in 2019, has highlighted the subversive use of drones for surveillance and reconnaissance of sensitive defence installations, airspace interference, smuggling, and kinetic attacks.

Drones have also become a preferred tool for narcotics trafficking. Drug traffickers in Mexico, for instance, have frequently used drones for transporting drugs on the border with the United States (US). Indeed, these cartels depend on drones to an extent that they are themselves now manufacturing them. However, it was the drone attacks by Yemen’s Houthi rebels against two facilities of the Saudi Aramco oil company in Abqaiq and Khurais in September 2019, which have triggered alarm bells across the globe. The attacks involved as many as 10 drones, which managed to evade the Saudi Arabian air defence system. Meanwhile, in India, the attack on the Air Force base in Jammu by suspected members of the Lashkar-e-Taiba in June 2021 demonstrated for the first time the use of drones for terrorist attacks in the domestic context. Since these two events, much of the thinking within the security establishments has focused on ways to counter the use of armed or payload-carrying drones.
For years, certain areas along the India-Pakistan border have served as corridors for the flourishing smuggling of narcotic substances, counterfeit Indian currency, arms and ammunition, and other contraband. These corridors have proved resilient over the last 30 years, and criminal networks have employed multiple tactics to sneak contraband into Indian territory. These include: i) throwing packets of contraband over the fence across the border by involving the border population, who are ideal couriers as they are well-versed with the topography and local environment; ii) using 10-12-meter-long plastic pipes to move the drugs (packed in small packets) across the border while dodging the electrified fence; and iii) making cavities inside farming vehicles and appliances as these are allowed to cross the fence for farming activities.

The state of Punjab, in particular, has become the hub of smuggling activities with border points such as Fazilka, Firozpur, Tarn Taran, Pathankot, Gurdaspur and Amritsar serving as entry points. These activities are also spreading to the state's flanking regions of Jammu and Rajasthan. Multiple factors have played a role in sustaining these illegal corridors. These include Punjab's proximity to the so-called 'Golden Crescent'—the heroin-producing region comprising Pakistan, Afghanistan and Iran. According to Indian officials, the Pakistan Army's Inter-Services Intelligence (ISI) agency has been supporting the smuggling syndicates. Smugglers route only about five percent of the finished narcotics products through land in Indian territory. Yet it offers them enormous benefits as the product's price increases manifold once it crosses into Punjab, India. For example, anecdotal evidence from the field, gathered by security forces, suggests that the price of one kg of heroin is approximately US$ 6,000 in Pakistan, which increases to US$ 120,811 when it lands in Indian territory; the consignment’s worth rises to as much as US$ 604,043 if it reaches cities like Delhi or Mumbai.

As the security forces intensify their crackdown on drug smuggling by erecting electrified fencing, deploying sensors, and installing floodlights at the border, criminal elements have added UAVs or drones to their inventory—a method that has been used for years by drug smuggling syndicates in Latin America. These smart, low-flying unmanned vehicles are becoming popular among criminal networks as they avoid detection and evade interference by law enforcement agencies by ensuring a safe and undetected supply of contraband packages in remote areas, mostly done at night, for pick-up by accomplices.
As far back as 2018, analysts had already noted the possibility of Pakistan-based drug cartels using drones on the India-Pakistan border in a similar pattern to the US-Mexico border. However, according to the Punjab government, the first recorded drone delivery of arms and ammunition was in August 2019. The threat has only expanded since then. According to both the Border Security Force (BSF) and open-source information, the instances of drones bringing drugs, arms and ammunition across the border more than doubled from 2021 to 2022 alone. Table 1 lists the drone sightings by the BSF, along the India-Pakistan border in Punjab, Rajasthan and Gujarat states along with Jammu of Jammu and Kashmir Union Territory (UT).

Table 1: Drone Sightings, India-Pakistan Border (2020-2022)

<table>
<thead>
<tr>
<th>Year</th>
<th>2020</th>
<th>2021</th>
<th>2022</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jammu</td>
<td>20</td>
<td>30</td>
<td>25</td>
</tr>
<tr>
<td>Punjab</td>
<td>48</td>
<td>65</td>
<td>267</td>
</tr>
<tr>
<td>Rajasthan</td>
<td>10</td>
<td>8</td>
<td>23</td>
</tr>
<tr>
<td>Gujarat</td>
<td>2</td>
<td>2</td>
<td>8</td>
</tr>
<tr>
<td>Total</td>
<td>80</td>
<td>105</td>
<td>323</td>
</tr>
</tbody>
</table>

Source: Authors’ own, using various sources

Note: The BSF records all of these as criminal uses of drones.

According to the data, Punjab is most active among the three Indian border states and one UT with Pakistan, witnessing more than a four-fold increase in cross-border drone activity between 2020 and 2022. In 2022, 267 drones detected in Punjab accounted for 83 percent of all drone activities reported along the India-Pakistan border; these are detected, and not necessarily intercepted. The increased sightings of drones in Punjab can also be attributed to the government allocating more resources to tackle the threat. As a result, security forces are more aware, increasing the chances of detecting drones.
Security forces have also noted that the increased use of counter-drone technologies and resources in Punjab has made smuggling syndicates and terrorist groups shift focus to Jammu and Rajasthan due to the “ballooning effect”. Increased drone sightings are now being reported in places such as Gurdaspur (bordering Jammu) and Abhor (bordering Rajasthan).

Figure 1: Drone Activities on India-Pakistan Border

Terrorist groups headquartered in Pakistan have also been using drones for the delivery of arms and ammunition. This was demonstrated in the June 2021 attack in Jammu, where drones were used to drop two improvised explosive devices in the technical area of Jammu Air Force Station. While drones and their components are available commercially off-the-shelf, the technical sophistication required to modify the drones to carry a certain amount of
payload shows the likely involvement of the Pakistani military. The Pakistani establishment stands to gain from the melding of terrorism and criminality, as it amplifies India’s threat canvas.

The smugglers, which according to Indian analysts are backed by Pakistan’s ISI, are using Chinese-made drones to smuggle drugs, arms, and ammunition from Pakistan into Indian territory. According to the BSF’s analysis of the drones used in these smuggling activities, the devices are mostly commercially available, assembled and modified by the saboteur elements. Many of these drones, according to Indian media reports, have chips similar to those used for computers and smartphones. Custom-built drones have also been used in some cases, where the criminal entities assembled the drones from locally available components.

To be sure, drones have notable limitations. For instance, drones have often crashed due to technical glitches and power failure, and therefore were unable to perform their assigned mission. In some cases, security forces have observed drone operators miscalculating the range and power of drones, leading to their malfunctioning. Weather conditions, too, play an important role in drone flight and battery capacity. In the winter season, for instance, low temperatures cause the battery to rapidly deplete, adversely impacting the drone’s capabilities.

Drones typically operate at frequencies between 900 MHz and 5.8 GHz, with the most common being 2.4 GHz and 5.8 GHz. Most remote-controlled drones use these frequencies. Many of these drones also feature Near Field Communication (NFC) capabilities. This allows users to control the drone remotely and send and receive data to and from the drone. NFC enables the drone to perform various functions such as taking pictures and streaming video. NFC can also provide secure authentication and authorisation, allowing users to securely access the drone and its data.

Drones use the Global Positioning System (GPS) to navigate accurately and fly autonomously. For applications that require increased accuracy, some drones may also be equipped with a multi-constellation Global Navigation Satellite System, which combines signals from multiple satellite constellations.

---

**Nature of Cross-Border Drone Activities**

a These are either hexacopters (UAVs with six rotors) or quadcopters (UAVs with four rotors).

b GPS is a satellite-based navigation system that provides the user with location and time information, enabling them to determine their position, velocity, and direction. This system comprises a constellation of 24 satellites orbiting the Earth and is used by several devices, including drones.
for increased accuracy. (Table 2 details the specifications of the drones used by drug cartels working along the India-Pakistan border.)

Table 2:
Technical Specifications of Drones Sighted on the India-Pakistan Border

<table>
<thead>
<tr>
<th>Sighted on the India-Pakistan Border</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Frequencies used</strong></td>
</tr>
<tr>
<td>2.4 GHz ISM, 5.8 GHz ISM, 433 MHz and 915 MHz</td>
</tr>
<tr>
<td><strong>Navigation systems</strong></td>
</tr>
<tr>
<td>GPS or BeiDou Navigation Satellite System</td>
</tr>
<tr>
<td><strong>Heights operated at</strong></td>
</tr>
<tr>
<td>Between 1000 to 4000 ft</td>
</tr>
</tbody>
</table>

Source: Authors’ own

The threat of drone use for criminal and terrorist activity across the India-Pakistan border is only expected to grow. Pakistan is investing in developing its domestic drone capability, and has recently procured CH-4B drones from the China Academy of Aerospace Aerodynamics. While much of Pakistan’s focus is on military use, there are also fledgling efforts to develop the civilian drone industry.

Moreover, the current use of drones is restricted to flat terrains. This may change as drone technology advances in terms of endurance and range, which could enable their deployment in other terrains like mountainous and maritime zones. The development of swarming drones can also be a game changer. This can include loitering systems, which can stay in the air for an extended period of time. The International Narcotics Control Board has already flagged the use of the maritime routes around India’s coast for drug smuggling. This expansion in the application of drones by criminal and terrorist elements in other terrains and circumstances will be significantly determined by their cost-effectiveness in delivery.
With their agility, ability to evade detection, support from the Pakistani establishment and fusion of criminal-terrorist threat elements, drone activity along the Pakistan-India border presents a serious challenge for India’s border security and law enforcement agencies. In response, India’s security agencies are developing strategies to detect and intercept these drones, including using counter-drone technology, increasing surveillance, and expanding inter-agency cooperation.

At the border, security agencies are employing various counter-UAV systems. These include the system that can detect, identify and neutralise different types of drones, including Small Hybrid UAVs, Micro UAV/Multirotor, and Nano UAVs. A typical counter-drone system comprises the following elements:

- Drone detection and tracking radar
- Day and night camera with laser ranging for detection and tracking of a drone target
- Communication channel detection and jamming system (soft kill)
- GPS jamming/spoofing system (soft kill)
- Laser-directed energy weapon system (hard kill).

For detecting drones and disrupting their flight, the BSF has utilised detection systems (use of radar, cameras, or other sensors) and jamming systems that disrupt the communication between the drone and its operator. While it is difficult to detect the audio signature of the drone, reports from the ground suggest that security personnel rely on this audio signature for detection. The BSF is also carrying out continuous patrolling throughout the day and night, in an area that stretches for around 5 km behind the border. This ‘depth area patrolling’ is designed to monitor the border region and prevent the local population from accessing any illicit consignments that may be dropped by drones.

The BSF is also working with local police agencies. In Punjab, the state police have deployed some 300 personnel for patrolling, and have raised permanent and temporary check posts to monitor suspicious movements. Police personnel
are also working with local communities to increase awareness of the threat posed by drones and encourage reporting of threatening drone activity.

The BSF has deployed handheld Radio Frequency (RF) jammer systems at the international border to disrupt and block drone flights. As a static, mobile, or handheld device, the RF jammer transmits a large amount of RF energy towards the drone, masking the controller signal. Using this system against a detected drone in flight leads to it either making a controlled landing in its current position, returning to the user-configured home location, falling uncontrolled to the ground, or flying off towards a random uncontrolled location.\(^{31}\)

Furthermore, BSF is developing and deploying physical interception methods, such as using trained personnel and nets to capture drones. Besides these, BSF has experimented with kinetic means using directed energy against or launching projectiles to disable intruding drones. However, due to technical limitations, their effectiveness is yet to be affirmed. In November 2022, then BSF Director General Pankaj Kumar Singh noted that of all sighted drones, the force had shot down 16 in 2022, compared to one in 2021, at the international border.\(^{32}\)

Drones that are shot down and recovered are analysed in a forensics laboratory in New Delhi set up in November 2021 by the BSF.\(^{33}\) The forensics facility has proven useful in analysing the mechanical and navigational components of recovered drones to determine their capability and flight path.\(^{34}\) Furthermore, BSF has established a new training centre under the Western Command to train its personnel for handling drone activities. The training module includes instructing personnel to detect drones “manually or through anti-drone systems and measures to neutralise hostile drones.”\(^{35}\)

In keeping with the Indian government’s ‘AatmaNirbhar Bharat (Self-Reliant India)’ mission, the BSF has tapped into the Indian start-up ecosystem to develop indigenous counter-drone technologies. In July 2021, the force, in partnership with the Ministry of Electronics and Information Technology (MeitY) Startup Hub, launched the BHUMI challenge (BSF High-tech Undertaking For Maximising Innovation) for exploring new technologies and sourcing incubation programmes to provide solutions for border security.\(^{36}\) A successful outcome of this initiative is the development of the indigenous counter-drone gun solution. Developed by Gurutvaa Systems, a Pune-based
start-up with support from the Indian Institute of Technology (IIT) Bombay, the equipment was handed over to the BSF in June 2022.\(^\text{37}\)

The BSF has also tied up with organisations such as the Defence Research and Development Organisation (DRDO) and Bureau of Police Research and Development to develop indigenous solutions. It has also reached out to start-ups like Skylark Labs India to research and develop Artificial Intelligence (AI)-based counter-drone detection and neutralisation technologies to secure the borders.\(^\text{38}\) These AI-based system uses sensors like radar, light detection and ranging, and cameras to detect drones and machine learning (ML) to identify threats. It distinguishes authorised drones from the unauthorised ones, and can intercept threats using jamming, GPS disruption, or physical measures. It provides real-time alerts and integrates with other security systems.\(^\text{39}\) Some of these have already been tested. For instance, during the August 15 Independence Day celebrations in 2022 at the Red Fort in New Delhi, authorities deployed the DRDO-developed anti-drone system. Its claimed range is up to 4 km.\(^\text{40}\)

Even as these measures are being implemented, however, saboteur elements have also adapted. For instance, drug smuggling syndicates and terrorist organisations have shifted their focus to other vulnerable areas to avoid security agencies that conduct depth area patrolling and deploy anti-drone equipment.

These efforts are not unique to India. In other parts of the world, security agencies are countering the use of drones by criminal networks and terrorist organisations. The International Criminal Police Organization or Interpol has held an annual international expert conference on drones for the past few years, helping member states manage the threats posed by the use of drones for criminal activity and imparting lessons on utilising drones for law enforcement.\(^\text{41}\) In September 2021, Interpol conducted a testing exercise in Norway for counter-UAS systems to assess their performance.\(^\text{42}\) The June 2022 experts’ conference on drones highlighted the need for more robust industry standards to illustrate the counter-UAS systems’ capabilities in helping law enforcement agencies make appropriate decisions in purchasing particular systems.\(^\text{43}\) The organisation has also emphasised the need for forensic analysis of the recovered drones for criminal investigation purposes.\(^\text{44}\)
The United Nations Security Council’s Counter-Terrorism Committee (UNCTC) is also giving attention to the misuse of drone technology as part of its broader focus on the growing threats posed by new and emerging technologies. The UNCTC is working, in particular, to gather best practices from the member states in addressing the misuse of emerging technologies by terrorist organisations. Its Delhi Declaration from the meeting in October 2022 announced plans to develop a set of non-binding guiding principles in countering the security challenges posed by drones.

“As India’s security agencies deploy counter-measures vs. hostile drones on the India-Pakistan order, saboteur elements have also adapted.”
Border security agencies must forecast in advance, remain vigilant, and adapt their strategies to stay ahead of the threat posed by the use of drones for criminal and terrorist activities. While it is difficult to build impregnable defence against cross-border drones, the Indian security establishment could explore executing the following additional steps to safeguard the country’s borders from hostile drones.

1. **Strengthen integrated border security.** Countering hostile drone activity is integral to the overall strengthening of India’s border security. Therefore, the Indian security establishment needs to reconfigure border security from a ‘guards and fences’ mindset to one that takes an integrated approach combining technology-based resources and skilled personnel. Security agencies could explore the idea of raising dedicated drone battalions for border security, which can be utilised for specialised tasks like border surveillance to help detect and track suspicious drone activity. Such surveillance can be round-the-clock as drones can be equipped with day and night payloads. This will be particularly useful given that most drone flight activity happens at night. Establishing restricted airspace or geofencing can also help limit the potential for drones to be used for malicious purposes. However, their execution at the border points will require additional deliberation.

2. **Technology training:** For the optimum utilisation of modern gadgets amidst technological advancements in border security and the changing nature of warfare, the curriculum of training institutes for border guard forces should include technical training as a mandatory component of all programmes and courses. They could also explore opportunities to collaborate with border guard forces domestically and internationally to learn best practices from each other.

3. **Develop counter-drone capabilities:** As BSF has employed RF jamming against hostile drones, criminal syndicates have switched to autonomous drones. To jam and disable these autonomous drones, the Indian security establishment could explore deploying Electronic Warfare (EW) capabilities. There are lessons to learn from the ongoing Russia-Ukraine war, where the Russian military has effectively utilised its EW capabilities against smaller Ukrainian drones by preventing them from navigating and communicating. India must develop such EW capability to protect vital installations from standalone or swarming drones.
4. **Maintain a database of drones operating in India:** Since most of the drones used by criminal networks in India are China-made which are commercially available and are subsequently modified, India should maintain a database of the micro and small drones imported or sold for personal and commercial purposes. Perhaps something along the lines of the IMEI number (International Mobile Equipment Identity) assigned for each imported mobile phone can be allotted to every drone that is either imported or sold domestically. Such measure will help security agencies keep track of these drones and potentially deter the saboteur elements that intend to use them for malicious activities.

5. **Create a hybrid environment for R&D:** Keeping in view the partial success of the BHUMI challenge discussed earlier in this brief, this type of mechanism and support must be expanded and institutionalised for border security organisations. This can be done by creating a dedicated hybrid platform to encourage innovation of indigenous counter-drone technologies. Lack of appropriate financial support need not thwart innovation.

6. **Institutionalise inter-agency coordination:** Hostile drone activities are currently concentrated on the land border between India and Pakistan. However, considering the innovative capabilities of drug smuggling networks and terrorist organisations, it is likely that these activities will extend to maritime borders in the near future. To get a comprehensive picture of hostile drone activity and promote the timely sharing of actionable intelligence, authorities should institutionalise inter-agency coordination on the lines of the Multi-Agency Centre for Counter-Terrorism Coordination, Narco Coordination Centre for drug smuggling, and Fake Indian Currency Notes Coordination Group. This inter-agency body must necessarily include the Coast Guard.

7. **International collaboration to boost ‘Make in India’ mission:** International partners like Israel, United States, Japan and South Korea can play a significant role in supporting India’s ‘Make in India’ efforts in developing counter-drone technologies. First, the thriving drone industry in these countries can collaborate with their Indian counterparts and invest in research and development activities in the counter-drone technology sector. This can lead to the creation of new and innovative technologies that can help India counter the drone threat effectively. Second, these countries can share with India their expertise and knowledge in the field of counter-drone technologies. This will help Indian companies and researchers learn from the experiences of other countries and incorporate those best practices in their own efforts. Third, these countries can provide a platform for India to showcase its capabilities in the counter-drone technology sector, and thereby provide potential opportunities for expanding their business globally.
The subversive use of drones on the India-Pakistan border reflects the larger global trend of the increased use of dual-use technologies for asymmetric warfare. Security and law enforcement agencies, including BSF, are implementing measures to actively counter the threat. As drone technology is becoming more affordable and accessible, the threat is only set to heighten, requiring the Indian security establishment to devise additional countermeasures. India must examine policy responses from other like-minded partners in response to this menace. Developing these counter-drone capabilities will go hand in hand with India’s efforts to build the national drone industry.

Sameer Patil is Senior Fellow, Observer Research Foundation, Mumbai.

Raj Arora, PhD. Professor (Visiting) IIT Delhi, has almost three decades of experience as a field practitioner of border security, cybersecurity, counterinsurgency and counterterrorism in various parts of India and abroad.


10 Patil, “Punjab’s unshakable drug smuggling networks”


12 Authors’ own information, gathered from sources.

13 Patil, “Punjab’s unshakable drug smuggling networks”

Endnotes


18 Chauhan, "Use of drones by terrorists poses challenge: BSF chief”


21 Yudhvir Rana, “Pakistan sends high-end drone to airdrop drugs in Punjab; it is capable of spying too,” The Times of India, February 20, 2023, https://timesofindia.indiatimes.com/city/chandigarh/pakistan-sends-high-end-drone-to-airdrop-drugs-it-is-capable-of-spying-too/articleshow/98076513.cms


28 Mohan, “Drone activity along International Border in Punjab increased nearly four times over last year, reveals BSF data”


33 “Drones from across border more than doubled in this year: BSF DG”

34 Mohan, “Drone activity along International Border in Punjab increased nearly four times over last year, reveals BSF data”

35 Mohan, “Drone activity along International Border in Punjab increased nearly four times over last year, reveals BSF data”


37 MeitY Startup Hub (@MSH_MeitY), "#successstory We are delighted to announce @gurutvaa as the winner of 'Anti-Drone Technology' under the BHUMI challenge organized by @MSH_MeitY In collaboration with the @BSF_India @GoI_MeitY @AshwiniVaishnaw @Rajeev_Goi," Twitter Tweet, October 25, 2022, https://twitter.com/MSH_MeitY/status/1584782807073274188.


39 Chauhan, “Use of drones by terrorists poses challenge: BSF chief”


44 INTERPOL, “INTERPOL convenes global summit on the use of drones”


Images used in this paper are from Getty Images/Busà Photography.