INSTITUTE FOR DEFENCE STUDIES & ANALYSES
रक्षा अध्ययन एवं विश्लेषण संस्थान

IDSA
Issue Brief

Comprehensive Integrated Border Management System: Issues and Challenges

Pushpita Das

October 5, 2017

Summary

The Comprehensive Integrated Border Management System (CIBMS) is viewed as a robust and integrated system that is capable of addressing the gaps in the present system of border security by seamlessly integrating human resources, weapons, and high-tech surveillance equipment. But the implementation of high-tech solutions without adequately trained personnel and without conducting a proper market survey is unlikely to help achieve the goal of foolproof border surveillance, besides draining the exchequer of precious resources. Instead of high-cost technological solutions that require extensive technical expertise, a mix of optimally trained manpower and affordable and tested technology is more likely to yield optimum results.

Introduction

On September 30, 2017, Border Security Force (BSF) personnel detected a cross-border tunnel in the forest area of Damala nullah in Jammu's Arnia sub-sector. The tunnel, reportedly 14 feet long, three feet high and 2.5 feet wide, was designed to facilitate the easy infiltration of terrorists from Pakistan into India. This was the second such tunnel discovered in the Jammu sector along the India-Pakistan international boundary during 2017 and the fifth since 2012. The four other tunnels discovered were in Ramgarh sub-sector (February 2017), Allah Mai de Kothe, R S Pura Sector (March 2016), Pallanwala sector (August 2014), and Shakkergarh area (July 2012).[1] Besides tunnels, the Jammu sector has also witnessed quite a few instances of successful infiltration by terrorists during the past couple of years as a prelude to attacks on strategic installations — prominent among these being the Pathankot and Uri terrorist attacks in 2016. These incidents have not only raised serious concerns about the efficacy of the existing border security system in thwarting such breaches but also a consequent demand for the deployment of high-tech border surveillance equipment by the BSF.

The use of high-tech solutions for border security was being considered by the Ministry of Home Affairs (MHA) since 2012 when it released an Expression of Interest (EoI) for a Comprehensive Integrated Border Management System (CIBMS). In 2014, the BSF also submitted a detailed report on CIBMS to the MHA, but no decision was taken to implement the system until January 2016. The trigger for implementing the CIBMS was the Pathankot terrorist attack, which took place on the intervening night of January 1-2, 2016,[2] and the subsequent warning by the division bench of the Punjab and Haryana High Court that if no decision to protect the India-Pakistan border were taken by February 16, 2016, stern action would be taken against the officials of the MHA.[3]

Following the High Court's intervention, the Union Home Secretary convened a meeting on January 29, 2016 and sanctioned the implementation of CIBMS through two pilot projects. The aim of the pilot projects was to test the CIBMS on various parameters such as requirement of manpower, user friendliness, technical training, repair and maintenance. At present, the CIBMS is being implemented along two stretches in the Jammu sector of the India-Pakistan border. The two stretches were selected for their difficult terrain characterised by several cross-border streams and

[1] "Day after India-Pakistan flag meet, BSF detects trans-border tunnel in Jammu's Arnia sub-sector", The Hindustan Times, Jammu, October 1, 2017, at http://www.hindustantimes.com/india-news/under-construction-tunnel-being-dug-from-pakistan-side-unearthed-by-bsf-in-jammu/story-B1qgulsJCMQ8FOxWs3LYyO.html (Accessed on October 3, 2017).

[2] "Pathankot attack: Here is what happened in last 42 hours", *The Indian Express*, January 3, 2016, at http://indianexpress.com/article/india/india-news-india/pathankot-air-force-attack-here-is-what-happened-in-last-42-hours/ (Accessed on October 3, 2017).

[3] "Pathankot terror attack: HC raps over inaction on BSF report", *The Hindustan Times*, January 13, 2016, at http://www.hindustantimes.com/punjab/pathankot-terror-attack-hc-raps-mha-over-inaction-on-bsf-report/story-LppUJK1EHTTpUjckvoAS7J.html (Accessed on October 3, 2017)

dense growth of elephant grass. The fact that several intruders were arrested with large consignments of heroin and fake Indian currency notes in these stretches highlights their vulnerability. A cross-border tunnel had also been discovered in one of the selected stretches. On March 22, 2016, the BSF issued a request for proposal inviting technological solutions for the CIBMS.[4]

That the MHA is keen on finding high-tech solutions to secure the border is further reinforced by its March 29, 2017 decision to constitute a high-level committee on Security and Border Protection under the chairmanship of Madhukar Gupta, a former Home Secretary. Besides finding gaps in the fencing and other vulnerabilities along the India-Pakistan border and strengthening manpower, the committee was explicitly tasked to recommend technological solutions to secure the international border.[5] To facilitate the task, two directors from the Indian Institute for Technology (IIT) were included in the committee. The Committee submitted its Report on March 14, 2017.

Existing System of Border Guarding

The emphasis on the use of high-tech gadgets for border security is not new. The need for effective technical means to prevent infiltration along the India-Pakistan border first arose during the 1980s when Punjab was in the grip by militancy and numerous incidents of infiltration by Sikh militants were observed. At that time, the BSF was provided with night surveillance capabilities such as Passive Night Vision Goggles (PNG), Night Weapon Sights (NWS), Hand Held Search Lights (HHSL), Hand Held Deep Search Metal Detectors (HHMD), etc. In subsequent years, as cross-border threats increased and the BSF embarked on a modernisation process, the organisation acquired more sophisticated devices such as Hand Held Thermal Imagery (HHTI) systems, Long Range Reconnaissance Observation Systems (LORROS), Battle Field Surveillance Radars (BFSR), etc.[6] These equipment proved to be game changers and force multipliers by enhancing the detection capabilities of BSF personnel and resulted in many apprehensions.

Despite these successes, sustained and successful attempts by infiltrators in breaching the international border continued, which, in turn, compelled the BSF to review the effectiveness of the existing electronic surveillance systems. An in-depth assessment of the existing border management system revealed that it suffered from a number of shortcomings which hampered effective functioning. Some of the

[4] Border Security Force, "Technological Solutions For Comprehensive Integrated Border Management System", *Request for proposal (Part I)*, March 22, 2016, at http://tenders.gov.in/viewtenddoc.asp?tid=del816186&wno=1&td=TD (Accessed on October 4, 2017).

[5] *Starred Question No. 421* "Security of the Border", *Lok Sabha*, New Delhi, April 26, 2016, at http://mha1.nic.in/par2013/par2016-pdfs/ls-260416/421.pdf (Accessed on October 3, 2017).

[6] Deshpande, Anirudh (ed.), *The First Line of Defence: Glorious 50 Years of the Border Security Force*, (Delhi: Shipra Publications, 2015), pp. 241-244.

shortcomings highlighted were: a) the high-tech equipment being used did not provide all-round security and did not work in adverse climatic conditions; b) significant gaps remained at rivers and nullahs running along the fences; c) being manpower intensive, the system was not effective in providing rest and relief to BSF troops; and, d) it is not an integrated system and therefore failed to provide a common operating picture at all levels.[7] Given these shortcomings, the BSF argued that a new, efficient and high-tech surveillance system for border guarding is urgently required to prevent infiltration by terrorists and smugglers.

The CIBMS

The CIBMS is touted as a more robust and integrated system that is capable of addressing the gaps in the present system of border security by seamlessly integrating human resources, weapons, and high-tech surveillance equipment. It has three main components: a) new high-tech surveillance devices such as sensors, detectors, cameras, ground-based radar systems, micro-aerostats, lasers as well as existing equipment for round-the-clock surveillance of the international border; b) an efficient and dedicated communication network including fibre optic cables and satellite communication for transmitting data gathered by these diverse high-tech surveillance and detection devices; and c) a command and control centre to which the data will be transmitted in order to apprise the senior commanders about the happenings on the ground and thus providing a composite picture of the international border. A composite picture would help senior commanders analyse and classify the threat and mobilise resources accordingly to assist the field commander in his response. The purpose of the CIBMS is to eventually replace manual surveillance/patrolling of the international borders by electronic surveillance and organising the BSF personnel into quick reaction teams to enhance their detection and interception capabilities. Other factors such as power back up, training of the BSF personnel in handling the sophisticated equipment, and maintenance of the equipment are incorporated into the CIBMS project.[8]

The use of high-tech equipment as an integrated instrument for border security has been experimented in various countries. Many, including the United States, have tried high-tech solutions for securing their borders, but with mixed results. In this context, a review of the Secure Border Initiative *net* (SBI *net*) of the United States provides a clearer picture of the likely problems that the BSF might face while implementing the CIBMS.

[7] Sharma, Ram Niwas, "Present Integrated Surveillance System on Jammu IB vs Pilot Project Sanctioned By Government of India", (Unpublished dissertation). Also author's discussions with senior BSF Officials in New Delhi, September 20, 2017.

[8] K K Sharma, DG BSF, "Review of Implementation of Comprehensive Integrated Border Management System (CIBMS)", *Smart Border Management 2017*, FICCI, New Delhi, September 18, 2017.

The SBI*net* Programme

Following the September 11, 2001 terrorist attacks, the Department of Homeland Security (DHS) launched the Secure Border Initiative (SBI) in November 2005 and described it "as a departure from the traditional ways of thinking about border security".[9] In April 2006, the DHS launched the high-tech component of the Secure Border Initiative-network called SBI*net*. SBI*net* was to comprise of "surveillance technologies, such as sensors, cameras, and radars, as well as command, control, communications, and intelligence (C3I) technologies, including software and hardware to produce a Common Operating Picture (COP)."[10] SBI*net* was implemented as a pilot project along two stretches of the US-Mexico border spanning 53 miles in the Tucson sector. The projects were operationalised in February and August 2010 in Tucson and Ajo respectively.

But the programme did not prove to be a success story in border surveillance. In 2010, the DHS conducted an assessment of the SBI*net* programme to evaluate its viability and cost effectiveness based on inputs from field agents at the border, quantitative and science-based analysis of alternatives, and scientific analysis of in-house experts.[11] The assessment brought out a number of lacunae. It revealed that the system suffered numerous technical glitches such as a large number of false alarms, line of sight constraints, unreliable information transmission, and equipment malfunction. The programme also suffered from shoddy testing and missed deadlines. Based on the assessment, the DHS concluded that the SBI*net* programme was not viable and cost effective as it had resulted in tremendous cost escalation to the tune of US$ 1.4 billion. It further stated that the programme did not and could not provide a single technological solution to border security. In light of the poor assessment report, the SBI*net* was finally shelved on January 14, 2017.

It is noteworthy that SBI*net* was not the first high-tech border surveillance programme to have failed. Between 1997 and 2006, the US Department of Justice and the DHS had spent US$ 439 million on two electronic surveillance projects — the Integrated Surveillance Intelligence System (ISIS) and its successor American Shield Initiative — only to abandon them because of system failures.[12] The assessment reports of those two programmes had similarly stated that 90 per cent of the sensor alerts were 'false alarms'. Only two per cent of sensor alerts along the Mexican border resulted in apprehension, while along the Canadian border the figure

[9] Barry, Tom "Fallacies of High-Tech Fixes For Border Security", *International Policy Report*, April 2010, p.2.

[10] "Secure Border Initiative: DHS Has Faced Challenges Deploying Technology and Fencing Along the Southwest Border", *United States Government Accountability Office*, May 10, 2010, athttp://www.gao.gov/assets/90/82411.pdf (Accessed on October 4, 2017).

[11] "Report on the Assessment of the Secure Border Initiative- Network (SBI*net)* Program", *Department of Homeland Security*, 2010, at http://www.globalexchange.org/sites/default/files/DHS_Report.pdf (Accessed on October 4, 2017).

[12] Barry, Tom, "Fallacies of High-Tech Fixes For Border Security", *International Policy Report*, April 2010, p.4.

was less than one per cent.[13] Like SBI*net*, these surveillance programmes were touted as force multipliers, but border patrol could not quantify the force multiplication benefits. Besides its many flaws, the ISIS was severely undermanned, especially in monitoring the output of the surveillance system.[14]

Criticisms of *SBInet* and parallels with the CIBMS

One of the criticisms levelled against the SBI*net* programme was that while the DHS was clear that it wanted a technical infrastructure that would complement the two other components, i.e., tactical infrastructure (border fence) and personnel, it was vague about the kind of electronic surveillance system it was seeking. So, instead of formulating well defined objectives and providing clear specifications, the DHS asked prospective contractors to create their own vision for the project. The DHS also failed to specify performance metrics to judge the final product.[15]

In the case of the CIBMS, a similar dependence on vendors for designing a suitable surveillance system can be observed. Thus, the BSF's request for proposal advertised on March 22, 2016 clearly states that, based on the information provided by the BSF, bidders must arrive at their own conclusions about the solution needed to meet the requirements projected. Bidders were also asked to quote their own prices for the products they were offering.[16] This clearly demonstrates that the BSF does not have the required technical expertise to offer clear guidelines to the vendors so that they can provide suitable products. This fact is further evidenced by media reports that the two attempts at testing the system were stalled due to technical mismatch and budgetary projections. It has also been alleged that because of lack of technical knowledge and market research, the BSF decided to waive off 50 per cent of the scores for critical requirements in order to accommodate vendors quoting low prices, thereby compromising surveillance capabilities.[17]

Another criticism of the SBI*net* was that the Custom Border Patrol (CBP) had claimed that its own officers were capable of managing the SBI*net* from command and control centres. In reality, they did not have the required expertise and handed over electronic surveillance to the contractors with little direction or oversight. Various reports highlighted the department's over-reliance on contractors not only for carrying out departmental functions but also to oversee the management and

[13] "Mismanagement of the Border Surveillance System and Lessons for the New America's Shield Initiative Part I, II, and III", (Washington: US Government, 2007), p. 57.

[14] Ibid

[15] n. 14.

[16] Border Security Force (2016, March 22), "Technological Solutions For Comprehensive Integrated Border Management System", *Request for proposal (Part I)*, Retrieved from http://tenders.gov.in/viewtenddoc.asp?tid=del816186&wno=1&td=TD

[17] "BSF's border management plan runs into rough weather", *Businessline*, New Delhi, March 28, 2017, at http://www.thehindubusinessline.com/news/bsfs-border-management-plan-runs-into-rough-weather/article9604967.ece (Accessed on October 4, 2017)

outsourcing of these projects. In short, there were no systems in place to "oversee and assess contractor performance and effectively control cost and schedule."[18]

In the case of India, it is widely accepted that the operation and maintenance of the existing sophisticated equipment remain a problem. At present, many of the high-tech surveillance devices deployed by the BSF are not optimally utilised because the required technical expertise is not uniformly available among the force's personnel. Furthermore, the exorbitant cost of the electronic devices and the lack of easy availability of spare parts act as a deterrent against their use.[19] As regards the establishment of a command and control centre, it is to be seen whether BSF officials have the required competence to manage it. Even if the control centres are manned by BSF officials, centralised decision making could hamper timely and effective response on the ground given that detection and interception of infiltrators at the border require a quick response which is achieved only through a decentralised decision making process. Besides the lack of technical expertise, erratic power supply and adverse climatic and terrain conditions in the border areas could potentially undermine the functioning of the sophisticated system.

The Arizona Border Surveillance Technology Plan

Learning from the failures of the SBI*net* programme, the CBP launched the Arizona Border Surveillance Technology Plan (ATP) in 2011 in the form of two pilot projects at Nogales and Douglas in Arizona. The focus of the ATP is on the following: a) technology that meets the needs of local border conditions; b) a multi-year effort to make it cost effective; c) a mix of fixed and mobile technology; and d) the use of non-developmental, that is pre-existing and tested, technology.[20] While issuing the RFP, the CBP also clearly stated that the "sensor should be able to detect a single, walking, average size adult, and provide sufficient high resolution video of that adult at a range up to 7.5 miles in daylight and darkness."[21] The project is being implemented by Elbit System of America at a cost of US$ 145 million.

Conclusion

Technical solutions are necessary to augment and complement the traditional methods of border guarding. They not only enhance the surveillance and detection

[18] Barry, Tom (2010, April), "Fallacies of High-Tech Fixes For Border Security", *International Policy Report*, p.4.

[19] Author's observations during field visits to India-Bangladesh border in 2007, 2014 and author's discussion with senior BSF officials in New Delhi, October 21, 2016 and September 20, 2017.

[20] "Better than wall: A New Detection System Can Help Monitor the US-Mexico Border, *Popular Mechanics*, January 28, 2016, at http://www.popularmechanics.com/technology/security/a18622/border-control-integrated-towers-system-invisible-wall/ (Accessed on October 4, 2017).

[21] Ibid

capabilities of the border guarding forces but also improve the impact of the border guarding personnel against infiltration and trans-border crimes. However, caution must be exercised while advocating the use of high-tech and high-cost electronic devices for border security. The experiences of countries such as the United States that have employed high-tech devices demonstrate that not only are the costs of such devices prohibitive but that they also fail to provide a comprehensive solution to border security problems. Instead of high-cost and innovative technological solutions that require extensive technical expertise, a judicious mix of properly trained manpower and affordable and tested technology is likely to yield better results.

About the Authors

Dr. Pushpita Das is Research Fellow at the Institute for Defence Studies & Analyses, New Delhi.

The Institute for Defence Studies and Analyses (IDSA) is a non-partisan, autonomous body dedicated to objective research and policy relevant studies on all aspects of defence and security. Its mission is to promote national and international security through the generation and dissemination of knowledge on defence and security-related issues.

Disclaimer: Views expressed in IDSA's publications and on its website are those of the authors and do not necessarily reflect the views of the IDSA or the Government of India.

Institute for Defence Studies and Analyses
1, Development Enclave, Rao Tula Ram Marg
New Delhi 110 010 India
T +91-11-2671 7983 F +91-11-2615 4191
contact.idsa@nic.in www.idsa.in
Twitter @IDSAIndia
www.facebook.com/InstituteforDefenceStudiesAnalyses