India Needs Smart Frontiers: An Assessment

Pannu, P. J. S.

Veröffentlichungsversion / Published Version
Zeitschriftenartikel / journal article

India Needs Smart Frontiers: An Assessment

P. J. S. Pannu

Abstract

In the era of Fourth Industrial Revolution, technology has transformed the ways of doing any business, including warfare. The human element is slowly giving way to machines who would perform major functions including substituting and supplementing rank and file in the Military. Over 22,500 kms of India's frontiers are guarded by various Border Guarding Forces including the Coast Guards to prevent surprise incursions by the adversaries' State, State-sponsored or Non- State Actors. The Border Guarding Forces act as eyes and ears of the frontiers and can take on basic defensive actions for which colossal manpower is used. For a Military threat, Regular Forces takeover the responsibility for the Defense of the Nation. There is a case for optimizing the manpower and increasing the efficiency by bringing in smart systems in delivering constant situational awareness and response solutions. This would also ensure that all stakeholders are networked in real time. A combination of sensors, electronic and digital platforms, Data and Communication centers, using Terrestrial and Non-Terrestrial means, would build 'system of systems' for Common Operational Picture at Strategic, Operational and Tactical levels. Data/intelligence analysis and automation would be possible if such systems are ubiquitous and part of overall National security apparatus. The smart frontiers would soon be inescapable necessity for the Defense of the nation.

Lieutenant General **P. J. S. Pannu** (Retd) is Distinguished Fellow at The United Service Institution of India (USI), New Delhi.

Introduction

The term Frontiers is being used in a generic manner to define the borders/ Frontline as being held, managed and guarded by respective forces. This expression in no way replaces conventional terms but is representative of de-facto ground positions being held. Currently, manpower is being extensively used to carry out patrolling, watch duties from towers by sentries. Generally, analogue systems and traditional means are being used to police or manage the frontier. Coastal areas are also managed by the Coast Guard along with other forces. Border Management is the responsibility of the MHA and skies being a mixed responsibility with the Indian Air Force being a major stakeholder.

Modern warfare is undergoing rapid change and becoming more dependent on advanced technology. Non-contact and non-kinetic domains of warfare have emerged as more relevant; however, these domains would overlap with the kinetic and contact domains. Hybrid warfare covers all domains and also includes sub-conventional operations by the state and non-state actors. India's frontiers, irrespective of the neighbour, remain tense and are prone to infiltration by terrorists, agents, insurgents, smugglers and migrants with cross-connections with one another.

The response to hybrid security scenarios necessitates that there is not only overlap between various security forces and other agencies of the government, but complete integration between them. In the current and future times, technology would offer the possibility to integrate through smart networks. In the event of a warlike situation, the defence forces would need to quickly stitch up with the border guarding forces taking them under command.

This can be made seamless through integrated smart networks. It is necessary that the Armed Forces remain integrated into the national security apparatus as the line between war and peace are being blurred. India should adopt a smart frontier concept which is built as one system

and integrated into a system of systems. Future threats are difficult to predict as also there would be a short/negligible 'warning period'. There would therefore be no luxury of time to designate a 'Preparatory Period', carrying out mobilisation and for taking over the operational responsibility.

Indian International Boundary

India's Borders with its neighbours have been defined by the Department of Border Management, Ministry of Home Affairs (MHA) and surveyed and marked on the maps by the Survey of India. The alignment of the International Borders (IB) includes all areas that describe the shape and size of the nation. India shares its borders with seven countries: 4,096.70 km with Bangladesh, 3,323 km with Pakistan, 3,488 km with China, 1,751 km with Nepal, 699 km with Bhutan, 1643 km with Myanmar and 106 kms with Afghanistan. However, the dynamics of disputes mainly with Pakistan and China makes it difficult to describe the exact alignment of the Line of Control (LoC) with Pakistan and the Line of Actual Control (LAC) with China due to many disputes even on the disputed alignments. The number of negotiations have failed to yield any settlement. India and Pakistan have fought several wars over the Jammu and Kashmir state, but the outcome has been only in militarisation.

India and China fought a war in 1962 over the border dispute. After capturing certain Indian border posts and running over large territories during the war, the Chinese unilaterally withdrew to their bases some 20 km behind the claimed areas. 22 boundary negotiations between the two countries have failed to resolve the boundary question. Frequent incursions by the PLA have attempted over years to press their claims to certain areas. The year 2020 saw PLA coming to the areas of their perception, which were earlier patrolled, but in April the strength and the intention made it clear that the PLA consolidated their positions. Meetings of Corps Commander level could only achieve the partial

withdrawal of the troops; however, certain sensitive areas still continue to be held by the Chinese. The troops from both sides have been building up, hardening the positions from both sides on the LAC.

Other than the active military situation that prevails on the LC and the LAC, the international borders are held by the Border Guarding Forces, essentially for Border Policing duties to check the illegal transborder movement such as smuggling, transborder crime and movement of the population with common ethnic connections across. The entire Western International has been fenced to ensure there is no infiltration of terrorists. Similarly, the entire border with Bangladesh has also been fenced to prevent trans-border movement of migrants and Insurgents operating in the Northeast region.

Management of Indian Borders

Border Surveillance and Policing during peacetime are globally the responsibility of the Ministry of Interior (MHA). Protection of borders from surprise incursions is the responsibility of the Border Guarding forces, which are primarily the Central Armed Police Forces (CAPFs). These forces use conventional means of carrying surveillance across the borders from watchtowers and the gaps between towers are covered by foot patrols, sometimes using a combination of Vehicle/Animal mounted patrols. The sentries on the watchtowers use day/night binoculars and maintain daily observation logs. Immediate suspicious movement is reported by the radio/telephones.

The MHA under the concept of 'One Border-One Force' has raised a number of forces for Border Guarding i.e., Border Security Force (BSF) for Guarding the India-Pakistan and India-Bangladesh borders. Indo-Tibetan Border Police (ITBP) for the Northern Borders (Indo-Tibetan borders). Seema Suraksha Bal (SSB) has been given the responsibility of India- Nepal and India- Bhutan Borders. While the Assam Rifles is responsible for the Indo- Myanmar Border. Indian Coast Guard is

responsible for coastal protection. Under the 'Single Point Control' concept of MHA, the responsibility of conduct and coordination of any activity or operations to be carried out on a particular border would be under the authority of that designated force. However, the activities on the LoC and the LAC are under dual responsibility where the Army is the primary responder to a Military Threat.

The Union War Book is the guiding document of the Government of India that contains the provisions that would dictate the activities to be undertaken on declaration of war. Under these provisions, once invoked, all the border guarding forces and the designated police forces of the country are placed under the operational control of the Army/ Ministry of Defence (MoD). The Military formations and units takeover the responsibility of any activity on the borders in Defence of the Nation and by implication the responsibility of border guarding/Defence gets transferred to the MoD.

The management of the LoC has unique dynamics. This was referred to as a Cease-Fire Line (CFL) until 1972 when the Shimla Agreement was signed. It was expected that after 1972, the forces from both sides would disengage/reduce as the agreement was signed on a map. However, the tenants of CFL based on the grabber-holder concept have continued on account of Pakistan being uneasy about the Shimla agreement. Ironically, occasional Cease fire Agreements do get announced and broken over these active frontiers. The occupation of Kargil heights by Pakistan in 1999 was a case in point of Pakistan going against the principles of the Shimla Agreement. Indian Army however conducted the Kargil Operations keeping the spirit of the Shimla Agreement alive.

The LAC separates India and Tibetan China and is generally referred to as the Northern Boundary. This line is referred to as the Mc Mahon line in the Arunachal Pradesh Sector, IB/LAC in Sikkim sector and LAC in the central and Ladakh sectors. The Chinese have gradually built roads and infrastructure that connect all the forward military outposts,

whereas on the Indian side the connectivity is basically up to formation/ Unit HQs and gradually expanding to connect the forward posts. Both sides carry out regular patrolling of the passes from where crossing over the boundary is possible. However, many other open areas also exist where vehicle-mounted patrols carry out area domination. The PLA has built a digital wall all along their side comprising Radomes, day and night electro-optical cameras and digital sensors connected with OFC – 5G terrestrial and Non-terrestrial networks. These walls provide a constant EW and surveillance grid that alerts the forward posts and the commanders in-depth whenever the significant activity of their concern happens. The PLA troops not only react to these by physical action but also use this data for analysis which they use for institutional memory. Over the last three decades, China has been following a process of digitisation and referring to it as 'fighting under the conditions of Informatisation'.

India shares Maritime Boundary with Pakistan, Sri Lanka, Bangladesh and Myanmar. Due to disputes on the Indo-Pakistan boundary at the Sir creek (the Indian state of Gujarat and Pakistan Sindh) the International Maritime Boundary Line (IMBL), as the extension of IB is also unsettled. Similar disputes are there on the claim of a small island between India and Sri Lanka making the IMBL also open to interpretations. Other Borders of India with Myanmar Nepal and Bhutan are being manned in traditional manner of domination by patrols, watchtowers surveillance and occasional border meetings for coordination.

The responsibility of guarding the Sea Frontiers rests with the Indian Coast Guards (MHA), under the operational control of the Indian Navy (MoD). The National Waters, up to 12 nautical Miles are considered as the Indian territory and up to 200 nautical miles is the EEZ, where the international shipping transit is permitted but no foreign exploration of economic assets including fishing by any foreign national is permitted. The responsibility of sea vigil is divided between coastal states, who use

Marine Police for the immediate coastline and the Coast Guards who patrol up to the EEZ. The Coast Guard also is responsible to protect offshore assets of the country. BSF Water Wing is responsible for guarding the disputed Indo-Pak coastal and creek areas. An established coordination mechanism exists between the Indian Navy, Indian Coast Guards, State Marine Police, the BSF and the state police so that there is no infiltration from the coastal and creek areas.

Operational Environment and Imperatives

India is known to have active borders even though there is an absence of war. One can best describe this condition as No War – No Peace. The Western and the northern borders have a large deployment of Border Guarding and Military forces. While the portion of IB where there is no dispute largely remains peaceful, however, the threat of infiltration of terrorist groups remains not only from the land borders but also from the sea frontiers (attacks of 1990 and 2008 in Mumbai).

The situation on LoC and the LAC remains warlike. Exchange of trans-LC firing with intermittent mortar and Arty duels is a regular feature. LAC, especially in Eastern Ladakh has seen a military build-up since early 2020, the frequency of patrolling has been on the rise for almost a decade from both sides. Similarly, border movements all across the northern borders have seen a sharp increase resulting in frequent clashes between the Indian and the Chinese troops. China has taken up large infrastructure development programmes in Tibet that bring the roads, villages and communication installation right up to the Indian borders that support military deployment.

While ITBP is responsible for guarding the northern borders of India, the large deployment of the Indian Army creates many coordination issues between the two. Similarly, on the Chinese side, the PAP (People's Armed Police) is responsible for border policing, however, the PLA has the responsibility for border guarding. Lately, the People's Congress has

passed a new law, where the PLA and the citizens would have a role in the protection of their borders, making the PLA a direct stakeholder. The PLA units are already connected with the digital wall created by the Chinese for surveillance.

The IB between India – Pakistan has been completely fenced with two layers of barbed wire. The Border fence has been built towards the Indian side leaving a reasonable distance ahead of the fence up to the IB which is patrolled. The Border fence has been electrified with generators and has beamed lights to cover the areas ahead of the fence with 1,50,000 floodlights to ensure clear visibility at night. There are a number of BSF posts along the border, generally in alignment to the border fence. The LoC also has the Anti- Infiltration Obstacle System (AIOS) which comprises strands of barbed wires, lighting systems and a number of sensors for day and night surveillance. However, as the altitude of mountains along the LC rises, the snow levels being a major obstacle, the dynamics of LC management differ where AIOS has not been found fully satisfactory as infiltration still takes place over the snow or by cutting the fence. There are a number of places where tunnels have been dug under the Border/LoC fence for infiltration. Lately, drones have increasingly been used for smuggling or dropping arms and ammunition across to resupply the terrorists. The LoC in Kargil, Ladakh and Siachen (Actual Ground Position Line called the AGPL) is defended with the physical deployment of troops.

Post-1962 war, the LAC has been largely peaceful barring a few skirmishes and incursions by the PLA. The agreements based on the principles of *Panchsheel* have been holding out where both sides had agreed to resolve the boundary question peacefully without using any military means. Regular Border Post meetings have been held at designated spots in Eastern Ladakh, Sikkim and Arunachal Pradesh to resolve any tactical or operational disputes. At the national level, regular meetings at the Special representative levels have been taking place to resolve the

boundary disputes, but have had suboptimal results. Due to continuing disputes on the LAC, there has been an increase in PLA activities all along the LAC especially in the last decade. However, during these activities, the protocols were maintained where banner drills were carried out by patrols in case of any face-off. In 2020, the PLA has militarised the Northern borders post their forward movement into their claimed areas, resulting in fatal engagement at Galwan between two troops who used clubs to fight rather than the firearms. The patrolling activity and surveillance from both sides have been intensified.

During a conventional war, the responsibility to defend the borders would be transferred to the Army. The Hot War re-deployment would include the deployment of Border Guarding Forces preferably in the same Area. However, the modalities of border surveillance would undergo a change. The peacetime surveillance resources would need augmentation and conduct of routine would be in readiness to face a threat from conventional military forces. The Preparation of Battle Area would entail shaping up the tactical battle areas and war zones aligned with the Military commander's intent in their Area of responsibility. The Areas of interest and Areas of Influence would extend into the enemy territory and surveillance resources deployed accordingly.

India faces a 'two-and-a-half-front' challenge. The Western and Northern borders already have troops facing adversaries. Insurgency and internal threat is always simmering. There is a threat of infiltration from all sides from land borders and sea fronts. The forces are also involved with internal security duties within the states of J&K, Northeast and LWE in Chhattisgarh. The borders with Nepal, Bhutan, Bangladesh and Myanmar are relatively calm, but intermittent cross border activities by the Anti-national Elements/illegal migrants have been prevalent. With multifarious agencies, ministries and forces deployed there is a need for 'whole of a nation' response. It is essential that a Common Operational Picture is available at the Apex level and networked with subordinate and

related agencies. It is time that smart systems are developed for national security.

Need for Smart Systems

It is already ascertained that today the threats to National Security are Hybrid in nature that include traditional and non-traditional threats. While the traditional and physical threats have continued to manifest, technology has added a new paradigm to the threat dynamics. The advent of Information Communication and Technology (ICT) has brought in exponential growth in digital platforms. The neo-millennium generation has brought in innovation culture to fuel the fourth industrial revolution.

Space and Cyber domains combined with Artificial Intelligence (AI) has brought robotics to play a major role in how the future of wars would be fought. The niche and disruptive technologies would contribute to supplement manpower for surveillance and border guarding duties. Israel and China have increasingly introduced technology to replace soldiers to give Early Warning and be the first responders. The digital frontiers and Geo-fencing would replace physical systems to recognize or respond to threats.

India with over 2,2700 km frontier including the coastal areas needs round the clock surveillance to ensure any threat is detected ahead of time. With the availability of technology, it would be possible to build a smart detection and response mechanism for threat mitigation. Different Border Guarding Forces would need to adopt smart systems for border guarding. The technology used should meet the needs of Armed Forces and be compatible with military platforms once deployed. Currently, the MHA has been investing in technologies that may not be suitable and meet the requirements of the Armed and Strategic Forces.

The first and the outer layer of smart frontier should be able to carry out round the clock Strategic Surveillance that provides a multi–dimensional

scan. This layer should be built on 360-degree dome architecture that should cover land, sea, subterranean (sub-surface/undersea), threats from space and cyber-attacks. The targets for surveillance would be in the depth areas and beyond the area of interest of military field commanders. This architecture is based on space, aerospace, aerial, cyber systems and dove-tails the Ballistic Missile Defence (BMD) and Air Defence (AD). Due to the exponential increase in the range and speed of missiles and 5/6 Generation Aircraft, the response mechanism has to be built on rapid and instant neutralisation and counter-attacks. There are means to detect the Cyber and electronic signatures and these would be used to lock the critical targets. The precision strikes on the locked targets especially of critical infrastructure can be achieved through direct hits and indirect neutralisation. The strategic digital/smart frontiers created would become the essential part of Cyber Defence and Cyber deterrence. The strategic smart outer layer and subsequent inner layers would need a plethora of assets at the national level consuming large budgets. This may need a separate controlling entity such as Strategic Surveillance and Defence Agency as part of the Strategic Command.

Operational surveillance and response mechanism is relevant to the military commanders once warning orders are received. Effective strategic surveillance on the outer layer would be a trigger in sounding a military warning. The smart systems would be able to detect any threat or pick up suspicious activity instantaneously in the Areas of Interest of the Military commanders. The smart frontiers do not mean a physical obstacle system or a visible line of sensors. The smart frontier would comprise static, mobile and rapidly deployable assets. A set of drones with payloads of sensors would be sufficient to deploy the rapid surveillance sensors. These can also be deployed by aerial or artillery means. Similarly, electronic and laser energy based on the space, land and aerial means would be able to generate digital intelligence mosaics on the GIS platforms to be part of C5-I2-STAR2.

C5 (Command, Control, Computers, Communications, and Cyber) would build Common Operating Picture and link up the strategic and Operational Command and Control centres for clear, swift, instant and integrated picture. The Information and Intelligence (I2) would allow informed decision making, cutting down OODA loop and preparing the Surveillance, Target Acquisition, Reconnaissance and Robotics (STAR2) to activate the sensor-shooter element during the warning period. Since most of the future battles would be non-contact, engagement or kill chain of Cyber targets would give first strike advantage to the initiator. Smart Frontiers would be able to transmit the information and Intelligence directly to the War Rooms. A combination of precise Space surveillance, aerial/drone reconnaissance and ground/sea-based sensors would be necessary for IPB (Intelligence Preparation of Battlefield) to give ability to the field commanders to make precise assessments and for asset and priority allocation. The use of ballistic missiles and aerial attacks would far precede the engagement of ground forces.

Smart frontiers are not about a physical obstacle system like Border Fencing or AIOS, which have the primary role of stopping infiltration. These frontiers are not physical barriers but a combination of all-encompassing systems that are working across periods such as Peace, NWNP, Hybrid and conventional scenarios. These frontiers have to be ubiquitous in nature and cross-connect with Border-policing, Border Guarding and Military forces asking for total synergy between the MHA and MoD. The designs and configuration of smart frontiers would differ for plains, riverine, mountains, jungles and super High Altitudes as the terrain and threat dynamics differ in India on different fronts. These systems would need a dedicated power supply preferably through renewable energy. The sensors would need to be custom made to detect threats at different ranges, visibility and electronic spectrums. They would need to detect subterranean threats such as tunnels, undersea threats and equally cover the land, air, sea and space scanning facility. These systems

would need to be part of other domains and systems to facilitate a seamless switch of responsibility between the Police/Border Guarding forces and the Armed/strategic Forces that report to different ministries.

Smart systems are also vulnerable to hacking, cyber-attack disruptions and data deaths. These systems are prone to be manipulated and suffer from insider attacks and inept handling. It may be prudent that the system handling is done by specialists of Cyber Corps working under the DMA/MoD. The border Guarding Forces under the MHA should be the user of the same system for counter-infiltration and for detection of minor threats. To make the switching of responsibility easy during hot war, different applications can be made to work on the common platforms. The complication of switching ownership would by itself be a security risk and should not be allowed. Incident reporting, Data Recovery and redundancies would need to be carefully built-in.

The implementation of 5G and IOT in the civilian sector would allow industry 4.0 to easily build indigenous solutions for running the IoMT Internet of Military Things (IoMT) and Internet of Battle Things (IoBT) for the digital hot war. Since India neither has material nor fabrication capability for making semiconductors, supply chain infections of imported Chipsets remain a major concern as these could facilitate trigger system attacks or compromise smart frontiers. All units need to train and employ Chief Info Security Officers (CISOs) who would be able to exploit the smart systems fully but ensure the cyber hygiene is maintained at all times.