Content

Smart border management p4 / Responding to border management challenges p7 / Challenges p18 / Way forward: Smart border management p22 / Case studies p30

Smart border management

An Indian perspective

September 2016



www.pwc.in



Foreword

India's geostrategic location, its relatively sound economic position vis-à-vis its neighbours and its liberal democratic credentials have induced the government to undertake proper management of Indian borders, which is vital to national security. In Central and South Asia, smart border management has a critical role to play. When combined with liberal trade regimes and business-friendly environments, efficient customs and border controls can significantly improve prospects for trade and economic growth.

India shares 15,106.7 km of its boundary with seven nations—Pakistan, China, Nepal, Bhutan, Myanmar, Bangladesh and Afghanistan. These land borders run through different terrains; managing a diverse land border is a complex task but very significant from the view of national security. In addition, India has a coastal boundary of 7,516.6 km, which includes 5,422.6 km of coastline in the mainland and 2,094 km of coastline bordering islands. The coastline touches 9 states and 2 union territories.

The traditional approach to border management, i.e. focussing only on border security, has become inadequate. India needs to not only ensure seamlessness in the legitimate movement of people and goods across its borders but also undertake reforms to curb illegal flow. Increased bilateral and multilateral cooperation, coupled with the adoption of new technologies for border control and surveillance and the development of integrated systems for entering, exchange and storage of data, will facilitate the movement of people and products without endangering security.

The FICCI-PwC report on Smart border management: An Indian perspective explores how the Government of India can respond to border management challenges and adopt a proactive and resilient approach towards smart border management that should have four key elements: innovation and technology infrastructure, collaborative border management, capacity building and agile organisation. I sincerely hope that this report will offer important and useful insights to the government, enforcement agencies and all other stakeholders.

Dr A. Didar Singh

Secretary General, FICCI



Preface

Today, India is among the fastest growing economies in the world and is considered one of the emerging superpowers of the world. While on the one hand, India's central location and the trans-Indian Ocean routes have contributed to this growth, on the other hand, its large and complex border poses numerous challenges which need to be addressed for India's continued economic growth.

India shares its border with seven different countries. Most of these borders are man-made and do not follow any natural barrier. India's vast coastline and island territories also make it open to attacks and infiltration. In addition, political instability, cultural radicalism and patronage of mafia and terrorism in a few of the neighbouring countries make border management an important aspect to guard India's sovereignty.

Effective border management for such complex territorial conditions calls for proper planning and measures on the three main aspects: people, process and technology. We are very pleased to present this report where we identify the challenges which India encounters across the varying border conditions and introduce a framework to address those challenges.

The Smart border management framework presented in this report is based on our multiple years of experience in supporting governments to establish effective border management systems across the world. Under this framework, we introduce the key elements of border management and explain how these elements, when implemented effectively, can lead to sustainable and efficient border management.

At the end, we present two case studies on border management in other regions of the world, highlighting the specific challenges and solutions adopted by each region. We then present the impact and achievements of those solutions. This is followed by learnings from these case studies and how can they be applied to Indian border conditions.

We thank the participating domain experts for sharing their thoughts and strategies with us. We hope you find this report insightful and useful, and look forward to your feedback.

Neel Ratan

India Government Leader

PwC India

Chapter

1 Smart border management

1.1. Introduction

Border management is a security function that calls for coordination and concerted action by various government agencies within our country. The aim is to secure our frontiers and safeguard our nation from the risks involved in the movement of goods and people from India to other countries and vice versa.

Border management itself is a multifaceted term and may include, but is not limited to, the regulation of legal and illegal immigration, ensuring safe and secure movement of authorised people and goods, and prevention of smuggling, human trafficking, and infiltration.

The rapid growth that India is currently experiencing presents an array of opportunities and underlines the need for effective border management. In an increasingly globalised and service-oriented economy like ours, we rely heavily on the movement of goods and people. However, if these movements are uncontrolled, less regulated or without any supervision, smuggling, trafficking, crime, terrorism and illegal migration can increase.

Understanding and harvesting the economic benefits of border management is a challenge today. A competent border management system calls for the tight coupling of technology and infrastructure that is capable of handling the geopolitical, social and economic challenges we face in India owing to our vast border fronts.

India has a very large and complex border, covering around 15,106.7 km, which it shares with Bangladesh, China, Pakistan, Nepal, Myanmar and Bhutan, as well as a small portion with Afghanistan. What further increase the complexity and criticality are the varied terrain, climatic conditions and relationship with some of the neighbouring countries.

Owing to such peculiarities, having infrastructure and technology alone does not suffice for effective border management. The various agencies involved in border management, such as customs, immigration, armed forces, border security and intelligence agencies, are characterised by a need to cooperate with an expanding range of external information sources (technology driven and intelligence based) in order to develop a common operating picture of the movements within and beyond our borders.

Smart border management is an attempt to identify and implement controls which aim to improve border security by:

- Enabling effective communication and coordination among all security agencies to arrive at a common entity picture
- Controlling illegal trafficking of people and goods
- Neutralising threats linked to terrorism and organised crime
- Checking illegal migration

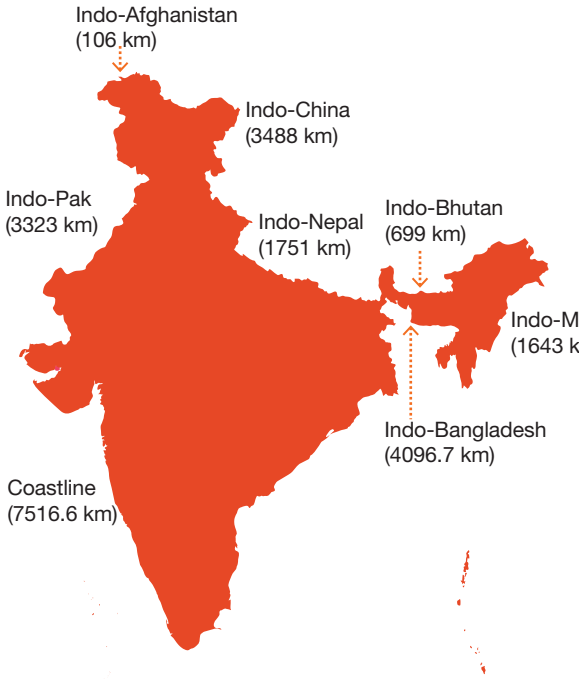


1.2. Border management: Complexity, enormity and implications

We understand that economic prosperity and globalisation require the free movement of people, goods and ideas; however, the growing number of border threats necessitates increased vigilance and more robust controls to secure borders.

We share our borders with seven different countries (Bangladesh, China, Pakistan, Nepal, Myanmar, Bhutan and Afghanistan) with all possible terrains—namely deserts, fertile lands, swampy marshes, snow-covered peaks and tropical evergreen jungles. This kind of vast terrain makes us vulnerable to insurgency, illegal migration and smuggling.

Indian borders



Name of the country Length of the border	(in Km)
Bangladesh	4,096.70
China	3,488
Pakistan	3,323
Nepal	1,751
Myanmar	1,643
Bhutan	699
Afganistan	106
Total	15,106.70

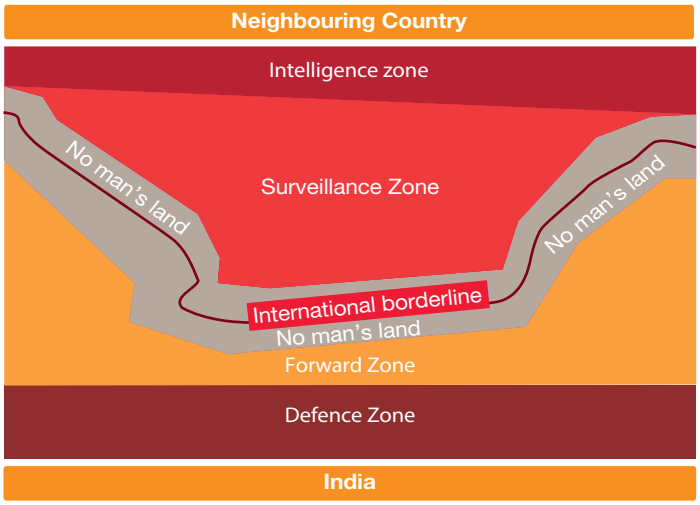
Source: http://mha.nic.in/annualreports

In the case of our coastal border line, our territorial boundary is defined up to 12 nautical miles. This zone is our sovereign territory and other countries have to take permission from India to entering this area. Contiguous to this is the zone of hot pursuit, and it extends up to 24 nautical miles. Any infringement of customs, sanitary, immigration and fiscal regulations in the contiguous zone can also attract punishment from coastal states.

The exclusive economic zone (EEZ) extends from the outer limit of territorial sea up to 200 nautical miles. This is the zone where coastal states hold the right to natural and economic resources such as minerals, oil exploration and fishing. Ships of other countries can pass through this zone as long as they do not pose any threat to the coastal states.



Illustration to creative a common entity picture





While our coastal borders are still relatively stable, our land borders pose a unique complexity.

India has three types of land border: international borderline (IBL), line of control (LoC) and line of actual control (LoAC).

- IBL is the demarcation that has been agreed upon and ratified by both the neighbouring countries, and has been accepted by the rest of the world.
- LoC is the de facto border and separates Pakistan-occupied Kashmir from India's state of Jammu and Kashmir.
- LoAC is the boundary line that separates Indian-held lands from Chinese-controlled territory. The disputed and unsettled nature of our boundaries (both land and maritime) has made their security much more difficult.

While multiple initiatives have been undertaken by the government, such as constructions of roads, fencing, floodlighting and installation of ground radars, the use of technology, intelligence gathering and integration of information from various sources to form a common entity picture remain a challenge. This can be further explained with the help of an example. Consider the scenario of infiltration across the IBL during peacetime. On either side of the international boundary, there exists a no man's land, which can be marked as a zone for infiltration.

On our side, to secure the borders from infiltration, two other virtual zones exist—the forward zone and the defence zone. The forward zone is the zone of first response and most infiltration attempts will be neutralised within this zone. The zone behind this is the defence zone, where our forces are stationed. For our forces to remain alert and informed, two virtual zones can also be identified within the neighbouring country. The surveillance zone, which is monitored continually by our forces to gather cues of any potential movement/infiltration attempts and the zone behind this, the intelligence zone, which is the area our intelligence agencies actively monitor for early warning signs. Thus, it is evident that multiple controls and mechanisms are used to gather information to neutralise any infiltration attempts. With such a set-up, building a common entity picture using various information sources (such as radars, satellite images and intelligence inputs) and then sharing this information for secure communication, dispatch and deployment by security agencies are extremely complex tasks.

Chapter

2 Responding to border management challenges

Current border management schemes by the Government of India cover articles of trade and people, points of entry and borders, and strategic and operational facets. A variety of measures are taken to safeguard land borders.

These measures are grouped into three categories—people, process and technology.

People

comprises the various types of forces and manpower deployed for safeguarding our borders.

Process

outlines a few initiatives taken by the Government of India to streamline the process of border control and management.

Technology

lists the technological controls into which the Government of India continues to invest in order to strengthen border management.







2.1. People

Three different types of situations can exist along the border: peacetime, less than wartime and wartime. Armed forces, which include the army, navy and air force, are engaged in border management during wartime or less than wartime, whereas paramilitary forces such as the Border Security Force (BSF), Indo-Tibetan Border Police (ITBP), Assam Rifles (AR) and coast guard operate on border during peace time.

Intelligence agencies provide inputs to border management organisations to deal with counter-intelligence and counter insurgency. The principle of 'One Border, one border–guarding force" is followed by the Government of India to secure the border. In line with this philosophy, the Bangladesh and Pakistan border is looked after by BSF, the security of the China border is entrusted to (ITBP), the Nepal and Bhutan border is looked after by Sashastra Seema Bal (SSB) and Assam Rifles have been deployed at the Myanmar Border. The LoC on the Indo-Pakistan border and the LoAC on the Indo-China border is protected by the Indian Army, while the security of the coastal borders lies with the Indian Navy and Coast Guard, with the State (Marine) Police acting as the second line of defence.



Government of India

Ministry of Home Affairs (MHA)

Paramilitary forces

- Special Frontier Force
- Assam Rifles
- National Security Guard

Central Armed Police Force

- Border Security Force
- Central Rescue Police Force
- Indo-Tibetan Border Force
- Sashastra Seema Bal
- Central Industrial Security Force

Ministry of Defence (MoD)

Indian Armed Forces

- Special Frontier Force
- Assam Rifles
- National Security Guard

2.2. Process

Efficient border management and border security essentially entail the effective control and regulation of the movement of people and goods and are of exceptional importance for the country. The processes that define and control the regulatory strategy for the borders and help the government facilitate legitimate travel and trade while simultaneously preventing illegal migration, smuggling and infiltration of insurgents and terrorists are the hallmarks of god border management.

Consequently, the two basic tenets that help define the processes for border management are:

- **Porousness of borders for legitimate trade and movement of persons**
- **Non-porousness of borders for all criminal activities** and other activities that jeopardise stability in the region

Border management is an integral part of military security and demands proactive intelligence, inclusion of technological advancements, and coordinated action by bureaucrats, politicians, economic agencies, security personnel and other related stakeholders of the nation in order to safeguard our borders from any sort of infiltration and attack.

Thus, integrated border management processes can be viewed as a large package of activities aimed at solving the strategic and practical challenges in border management, not as independent modules having no cause-effect relation with one another. The main facets of border management are as follows:

- Coordination within services
- Coordination between services
- International coordination

Coordination within services refers to proper communication and integration across ministries (such as the Ministry of Defence and Ministry of Home Affairs) and services authorised to perform certain duties pertaining to border management (various stakeholders like paramilitary forces and armed forces). Coordination within services has two aspects—vertical coordination and horizontal coordination. Vertical coordination involves different administrative levels, ranging from the ministry to the units working at the border. Horizontal coordination, on the other hand, happens within services (army, navy and air force) and concerns individual border crossings, as well as those between border management agencies in the country. Both forms of coordination require a clear division of responsibilities, active communication and regulated flow of information.

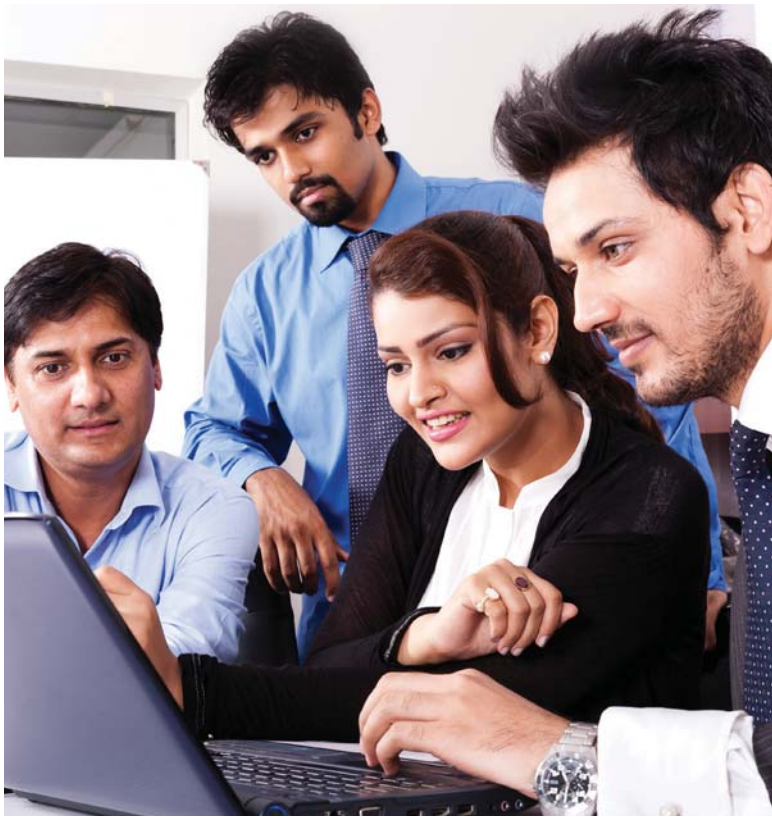
Coordination between services involves armed forces, ministries and other stakeholders responsible and competent to provide border management services. This is characterised by daily operational contacts at border crossings (both at formal and informal levels) and extends to the formulation, adoption and implementation of an accorded middle-range and long-term strategy for border management. Coordination is required to pave the way for an optimal solution for practical matters, such as harmonisation of politics and practices when necessary, development and funding of new infrastructure and IT services, and the development of common training for the existing and new personnel.

The general mechanisms followed for coordination between services at borders and inside a country are as follows:

- Coordinated processing at border crossings, which comprises proper coordination in the operation of border services, including properly defined competencies and procedures
- Integration of information systems responsible for border security with information from police and customs services

International coordination is another important facet which plays an important role in defining the processes to be followed to ensure effective and efficient border management. This can be can be divided onto three levels:

- Local cooperation of border services on both sides of the border
- Bilateral cooperation among neighbouring countries
- Multinational cooperation aimed at issues relating to border management



2.2.1. Department of border management

The Department (D/o) of Border Management was formed under the Ministry of Home Affairs (MHA) in January 2004, following recommendations from the Group of Ministers (GoM) on border security. This department has been entrusted with the responsibility of all matters associated with land borders and costal borders, with the exception of LOC in the Jammu and Kashmir sector. The roles and responsibilities of the D/o Border Management include fencing and floodlighting, surveillance and patrolling, security infrastructure development, intelligence report analysis, and development of Integrated Check Posts (ICPs).

Some of the initiatives successfully undertaken for border management are as follows:

Focus area	Details of work under the initiative
Roads	Construction of roads along the Indo-Bangladesh, Indo-Pakistan, Indo-Myanmar, Indo-China, Indo-Nepal and Indo-Bhutan borders
Fencing	Construction of fencing along the Indo-Bangladesh, Indo-Pakistan and Indo-Myanmar borders
Floodlighting	Construction of floodlighting along the Indo-Bangladesh, Indo-Pakistan and Indo-Myanmar borders
Border Outposts (BOPs)	Construction of 383 BOPs on the Indo-Bangladesh border and 126 BOPs on the Indo-Pakistan border for BSF
ICPs	Development of ICPs and setting up of the Land Ports Authority of India for their management and administration
Other security initiatives	Installation of high-tech surveillance equipment on the international border, implementation of coastal security schemes

2.2.2. Approach taken by the Government of India

The approach, as employed by the government towards border management, is categorised into four essential processes:

1. Guarding the borders
2. Regulation of the borders
3. Development of border areas
4. Constitution of bilateral institutional mechanisms for resolving disputes and ironing out conflicts with neighbours

2.2.2.1. Guarding the borders

Guarding of the Indian borders is undertaken by the various border guarding forces. The responsibility for the India-Pakistan and India-Bangladesh borders lies with BSF, AR for the India-Myanmar border, ITBP) for the India-China border, and SSB for the India-Nepal and India-Bhutan borders. In addition to this, the Central board of Excise and Customs has over 8000 officials on Border Security Check.

To manage the borders effectively, surveillance is carried out in the form of regular patrols by the border guarding personnel. In addition, several electronic surveillance equipment such as night vision devices, handheld thermal imagers, battlefield surveillance radars, direction finders, unattended ground sensors and high-powered telescopes are used by the border guarding forces as force multipliers for greater surveillance.

2.2.2.2. Regulation of the borders

Effective regulation of the borders involves facilitation of legitimate trade and travel and simultaneous prevention of illegal migration, smuggling, and infiltration of insurgents and terrorists. Building of barriers to prevent illegal ingress and egress of people and goods is an effective means of regulation that is employed at the borders.

Another method employed by the government to regulate the borders is the preparation of a national register and issuance of Multi-purpose National Identity Cards (MNICs). This would help to prevent illegal migration and facilitate the detection of those already staying in India.

The government also undertook the construction of ICPs in order to provide better facilities for the legal movement of people and goods across the border.

2.2.2.2.1. ICP

ICPs were introduced to reduce hassles in the cross-border movement of goods and people for promoting trade and commerce. The first ICP was inaugurated on 13 April 2012 in Attari. Additional ICPs in 13 locations on the Indo-Pakistan, Indo-Nepal, Indo-Bangladesh and Indo-Myanmar borders were approved by the Cabinet Committee on Security (CCS) for construction in two phases: 7 in Phase 1 and 6 in Phase 2.

The Government of India felt the need to set up ICPs because the existing systems were inadequate and did not sanitise cross-border trade and commerce completely. ICPs bring all the regulatory agencies, such as security, immigration and customs, along with the support agencies, which otherwise worked as separate entities, under one roof, thus interdicting any sort of unauthorised movement of goods and people posing a threat to the security of the nation.

The government had initially agreed to incur an expenditure of 635 crore INR to set up these 13 ICPs as listed below. The budget was finalised for 4 ICPs, while the project cost for 9 is yet to be decided.

Sr. no.	Location	State	Border	Estimated cost in crore INR	Phase
1	Petrapole	WB	India-Bangladesh	172	Phase I
2	Moreh	Manipur	India-Myanmar	136	Phase I
3	Raxaul	Bihar	India-Nepal	120	Phase I
4	Attari (Wagah)	Punjab	India-Pakistan	150	Phase I
5	Dawki	Meghalaya	India-Bangladesh	50*	Phase I
6	Akhaura	Tripura	India-Bangladesh	60*	Phase I
7	Jogbani	Bihar	India-Nepal	34*	Phase I
8	Hili	WB	India-Bangladesh	78*	Phase II
9	Chandrabangha	WB	India-Bangladesh	64*	Phase II
10	Sutarkhandi	Assam	India-Bangladesh	16*	Phase II
11	Kawarpuchiah	Mizoram	India-Bangladesh	27*	Phase II
12	Sunauli	Uttar Pradesh	India-Nepal	34*	Phase II
13	Rupaidiha	Uttar Pradesh	India-Nepal	29*	Phase II

Source: http://mdoner.gov.in/node/1483



ICPs have been instrumental in boosting the trade volume across borders. The Attari ICP, which became operational from 13 April 2014, witnessed a whopping 105.13% rise in trade volume in the following year. This volume further increased to 5443.73 crore in FY 2013–14 and clocked 2,742 crore by December 2015 for FY 2015–16.[1]

The infrastructural facilities under ICPs that are favouring trade and commerce are passenger terminal building, cargo inspection sheds, quarantine laboratories, warehouses, cold storage, etc., coupled with services like Internet facility, security systems such as closed-circuit television (CCTV)/public address (PA) system, scanners and cafeteria. Thus, the ICPs have been serving as a one-stop solution for trade and commerce with all modern facilities and security.

2.2.2.3. Development of border areas

Difficult terrain and a lack of proper roads, educational institutions and hospitals keep the border areas inaccessible and underdeveloped. The resulting lack of economic opportunities makes the border population more susceptible to illegal activities such as drugs and smuggling.

As a solution to tackle these issues, the government initiated the Border Area Development Program (BADP) in 1987, in order to facilitate the provision of the required socioeconomic infrastructure and adequate security, and to eliminate a sense of alienation among the population living at the border. BADP schemes include the development of community-based infrastructure such as forestry, pasture land, fishery ponds, parks, community centres, markets and mobile dispensaries. BADP also takes up security-related schemes.

The implementation of BADP is monitored by the D/o Border Management under the Ministry of Home Affairs.

2.2.2.4. Bilateral institutional mechanisms

Effective border management requires the facilitation of bilateral dialogue on matters of mutual concern, and thus, the Government of India has constituted a system of institutionalised interaction through the meetings of home secretaries, area commanders of border guarding forces and the joint working group on border management.

National level meetings (NLMs) and sectoral level meetings (SLMs) are organised under the Home Secretary and Joint Secretary of the Ministry of Home Affairs respectively. The primary agenda of these meetings is to ensure and maintain peace and tranquillity all along the border. To attain this objective, the two sides have agreed to 'prevent inadvertent violations of each other's territories by their security forces' and also 'monitor and curb effectively all illegal and negative activities such as tans-border movement of insurgents, narco-traffickers and others involved in nefarious activities'. Additionally, border liaison meetings (BLMs) take place between local area army commanders at designated places every six months.

India has constituted multiple such institutional mechanisms with Myanmar, Bangladesh, Pakistan, Nepal and Bhutan. Such bilateral mechanisms ensure that both the sides are adequately sensitised towards the respective security concerns and hence aid in better formulation of strategies for border management.

[1] *MHA' Annual Report*



2.3. Technology

The Government of India is focussing extensively on leveraging the power of technology to improve the efficiency and effectiveness of border operations. The world is moving towards technologically advanced military and defence systems and India has been equipping its military with sophisticated weaponry to help combat actual and perceived dangers to the nation.

Technology interventions near the border areas in India are broadly classified into two categories:

1. **Mobilisation and ordinance supply chain** (including equipment, weapons, vehicles and ammunition)
2. **Surveillance and communication** (including the use of technology that comprises information, logistics, reconnaissance, command and control centres, and surveillance in the border areas)

2.3.1. Mobilisation and ordinance supply chain

The conventional use of technology in the context of border management pertains to the use of high-technology weapon systems including small arms, ammunition, combat vehicles and advanced communication. These investments ensure that we have the right triggers for mobilisation and activating the ordinance supply chain, so that our state of readiness is synergised with an emerging situation on the borders.

2.3.1.1. Weapons and equipment

The armed stakeholders in border management are in the process of upgrading their weapons and equipment. The Indian Army is also upgrading its small arms such as pistols, carbines and light machine guns (LMGs), and looking forward to deploying some futuristic weapons in the border areas that are currently under development. One such example is the Future Infantry Soldier as a System (F-INSAS), which is under development by the Indian Army and is expected to connect the commander on the ground with the command and control system through a round-the-clock situational awareness update in inhospitable terrain.

Another technology being developed and waiting to be incorporated is Boomerang Warrior-X. It is a device worn in the vest which is able to pinpoint sniper positions from the enemy side up to about 1,000 yards. Besides these, the army is considering the use of explosive detection kits (EDK), suitcase SATCOM terminals, and other portable technologies to be used near the borders with China and Bangladesh.

Some other weapons being used the agencies are smart tracking sniper, army digital sniper, Sten machine carbine, INSAS assault rifle, INSAG LMG, etc.

Modernisation of the central armed police forces has also been a focus area for the government. In Modernisation Plan-II, the following weapons and equipment have been introduced:[2]

a) Weapons such as under-barrel grenade launchers (UBGLs), multi-grenade launchers (MGLs), anti-material rifles, less lethal weapons, gun shot detection systems and replacement of existing carbines and pistols with modern pistols, sub-machine guns and assault rifles

b) Equipment such as ground penetrating radar systems, unmanned aerial vehicles (UAVs), target acquisition binoculars, corner shots, handheld thermal imagers (HHTIs)/thermal sights/night vision devices (NVDs), unattended ground sensors, advanced medical equipment

c) Mine-protected vehicles, bullet-resistant vehicles/ boats, etc.

d) Communication equipment, including jammers and interceptors



[2] http://mha.nic.in/AnnualReports 2015-16

2.3.1.2. Vehicles

Border management agencies have been deploying advanced technologies in the vehicles being used around the border areas and improving the functionality of their armoured vehicles. Vehicles used by the security personnel are multipurpose, designed to help movement in tough terrains like deserts, no man's land and mountainous regions. Vehicles used for transportation around the borders are equipped with tracking systems, bulletproof armour and defence weapons.

2.3.2. Surveillance and communication

Strategic gains out of modern offensive systems, high-tech artillery and troop deployment can only be realised effectively when augmented with essential research and intelligence-based activities. In many ways, soldiers near the border areas fight a persistent battle of secrecy with the military personnel across the border. Amid such latent military intentions, information about the opposition and spying shape the basic military moves. Non-offensive technologies like advanced communication systems and surveillance enable the border guard forces to pre-empt and handle such situations in the most effective manner possible. Some of the measures taken by the Government of India include advanced surveillance systems, command and control centres, maritime border security and drones.

In this regard, the Defence Research and Development Organization (DRDO) has been supplementing India's border management techniques through extensive research and development. Special focus has been laid on technology in areas such as information, communication, command and control, Air Defence Control and Reporting System (ADC&RS), and battlefield management system.

2.3.2.1. Communication

Inhospitable terrain and the mountainous topography in the border areas in India make it very challenging to establish extensive communication networks through the laying of cables. The Center for Artificial Intelligence and Robotics (CAIR) under DRDO is helping to improve the technology in this regard. Important innovations such as the radio trunk system (RTS) and radio local system (RLS) have significantly improved military communication in the border areas.

Other technologies by DRDO include the wireless message transfer unit (WMTU) that allows mobile commanders access to communication networks, in addition to being used to transmit information via images from one place to another. Futuristic technologies like the Tactical Communication System (TCS) for the army are also being developed by DRDO. Cellular radios, wireless local loop (WLL), mobile satellite systems, etc., are being used by the agencies. Some of the communication systems being exploited by the Indian Army are the Army Radio Engineered Network (AREN), Army Static Switched Communication Network (ASCON), Troposcatter Communication Systems, SATCOM, etc.

2.3.2.2. Surveillance

Border surveillance is one of the most important parts of an integrated border management system. The Indian border extends to a length of around 15,106 km, spanning six countries with varied geographical profiling. The extreme weather conditions prevalent at the locations make the surveillance of our borders a challenging task for the armed forces. Thus, it is imperative that a technology-based state-of-the-art surveillance system be employed by the armed forces to ensure an effective surveillance, intrusion detection and identification system.



The surveillance of any border area, due to its vastness, relies heavily on the area of interest (AOI). This AOI requires round-the-clock deployment security personnel and equipment, which ensures a constant and effective vigil on the concerned area.

The Indian government has initiated multiple steps to ensure secure and non-porous borders for our country. The border areas are currently protected by fencing, floodlighting, sensors and manual patrolling. Long-range reconnaissance and observation systems (LORROSs) deployed at strategic areas have proven quite useful in the detection, identification and recognition of infiltrators.

The government has also set up a comprehensive integrated border management system for 24-hour vigilance along 2,900 km of the western border to lock down any sort of illegal intrusion. Along the Indo-Bangladesh border, vulnerability mapping and strengthening of BOPs which are identified as being prone to illegal migration/cross-border crimes have been carried out. This is being done by deploying additional manpower, special surveillance equipment, vehicles and other infrastructure support.

Moreover, steps such as deploying observation posts all along the international borders of the country, with riverine sections being patrolled using water crafts/ speed boats/floating BOPs, aerial recce at defined time intervals along the borders, procurement of state-of-the-art surveillance equipment, including day and NVDs, have been undertaken to act as force multipliers.[3]

Use of drones for surveillance and security purposes has been one of the emerging technological trends across the world for border security management system. Some of the neighbouring nations have been using drones for border surveillance. India is quick paced to develop its own drone fleet that could be used at both the aerial and ground level. The government has also realised the need for advanced UAVs that could be used to target up to a range of 10 km and can be easily integrated with the weaponry system.

Indian military has long operated Israeli Searcher and Heron drones for C4ISTAR roles and possesses anti-radiation suicide drones. It lacks missile firing drones such as the Predator in its inventory. In the near future, we may acquire the Rustom-I medium altitude long endurance (MALE) UAV. According to DRDO, it has integrated a locally developed anti-tank missile called HELINA with Rustom-I, which indicates the potential anti-armour role. Taxi trials have been completed, with flight trials expected to commence. It could certainly be used in strikes on remote terrorist camps or on small vessels on the high seas. According to a report from Centre for Asian Strategic Studies (CASS), India, the army has placed a requirement of around 1,600 mini UAVs for induction by 2017.

Furthermore, the indigenously developed drone is now being equipped with a high-accuracy satellite-based augmentation system (SBAS) and dedicated military communication satellites are being put in place, thus making the drone fleet operate as completely armed. Besides the process of weaponing, the fleet has already commenced. There is an equal dedication towards the introduction of stealthy unmanned combat aerial vehicles for India (UCAV).

However, with the Directorate General of Civil Aviation (DGCA) proposing measures to restrict the drone flight airspace, India is yet to reform and take major steps to improve its collision avoidance techniques as well as increase the satellite bandwidth.

Other than this, a need has also been identified for third-generation NVDs for better sighting at night. The requirement of around 30,000 NVDs has been raised with the Ministry of Defence. The NVDs will include battlefield surveillance radars (BFSRs), thermal sensors, high-powered sensors, NVDs and night binoculars which can help track every suspicious movement.[4]

Another important step the Indian government has taken towards securing one of the borders is a comprehensive project of locking the border by using an advanced technology system aligned with the layered defence approach to fulfil D4R2 (deter, detect, discriminate, delay, response, recover).



[3] http://mha1.nic.in/par2013/par2014-pdfs/ls-021214/1544.pdf
[4] http://cassindia.com/inner_page.php?task=research&&id=53

The project envisaged by the Government of India encompasses a five-layer advanced security system along the western border. This would include low-light CCTV cameras, thermal imaging, NVDs, surveillance radars, laser beams and underground monitoring sensors. The following table describes the system proposed in each layer:

Layer	Description
Layer I	Low-light CCTV cameras will be installed throughout the length of the border. To increase the effectiveness of these CCTV cameras, an intrusion detector alarm system has to be installed.
Layer II	Thermal imaging and NVDs will form the second layer in the security architecture frame. These will provide a view at night and will help check any sort of intrusion. The range will be up to 2 to 3 km.
Layer III	Surveillance radars will be the third layer that will be used for long-range observation. These tracks will be capable of tracking any suspicious movement up to 40 km. One of the unique features of these radars is that they will cover both sides of the border. This will help in detecting miscreants who support infiltration from Indian soil.
Layer IV	Laser beams will check infiltration from those areas that are physically difficult to monitor. Rivers such as Sutlej and Vyas flow from India to Pakistan and there are many small tributaries that have led to riverine gaps of around 2 to 3 km. There are around 130 such gaps along the western border. Elephant grasses on either side of these rivers further make monitoring difficult and facilitate infiltration. These laser beams will have two points—a receiver and transmitter; an alarm will be raised if anyone crosses these points. This will help control and secure all riverine gaps which are otherwise difficult to protect.
Layer V	Underground sensors will form the fifth layer that checks any underground intrusion. These sensors will detect vibration and heat from the human body and raise an alarm with the security personnel for their action.

During any incident, the security and surveillance mechanisms are required both at the place of the incident and the command and control centre. The place of the incident will typically be the field area of operation, where the systems described in the layers above will be deployed, while the command centre set up for the monitoring and management of these devices will act as the position for informed decision-making. Both technology and armed force personnel working in tandem ensure effective and efficient security at the borders. The proposed system for security and surveillance will typically assist the armed forces in carrying out the following activities during an incident:

At field location

- Threat detection
- Classification of threat, i.e. armed/unarmed, number of threats, vehicle borne, etc.
- Identification of friend and foe
- Availability of time and resources for incident response

At the command centre

- Decision making
- Options available for response
- Information-based timely response
- Post-incident analysis
- Forecasting-based incident pattern analysis
- Identification of vulnerabilities

A high number of infiltration incidents continue to be reported across our borders, and so it becomes imperative to modernise our surveillance and security systems.

2.3.2.3. Integrated command and control systems

A technologically high-end command and control system for military equipment is a must for maintaining an edge over the opposition in undefined or long porous border areas. The objective of the command and control centre is to direct information and data collected from various sources and agencies at one centralised location for immediate action. Similar information captured by different agencies may lead to multiple interpretation, with multiple teams being deployed for the same action. Hence, it is important to have all information sets at one place so that a common entity picture can be derived and necessary action can be initiated.

The vital elements that constitute a command and control centre are follows:

- An efficient communication system integrated with voice and video features
- Data visualisation tools for presenting inferences from the information received

Once a single source of truth has been established, the border agencies can initiate the necessary action, and the right teams and required assets can be deployed at the first instance, thereby saving effort and time.

An integrated command and control centre enables centralised monitoring of the border perimeter, checkpoints, buildings and compounds at all times. The major components of an integrated command and control centre include software applications, geographical information system (GIS) integration, input devices such as surveillance cameras and various types of sensors, a dashboard, mobile stations and high availability modules. Seamless integration of these modules provides real-time intrusion detection and situational awareness to the command centre. This helps in quick response and can also help in the deployment of an intervention team before a perimeter breach takes place. An integrated command and control centre is applicable to both land and sea-based threats. Software applications used for border surveillance are a crucial component of a command and control centre. They specialise in the detection of threats and intruders, event response mechanisms, coordination of interception units and 24x7x365 uninterrupted operations.

Additionally, advanced command and control systems can aid in various pre-emptive and reactive ways. The Artillery Combat Command and Control System (ACCCS) has been developed by DRDO to operate field artillery automatically. ACCCS aids in the trajectory calculation of artillery and also in the establishment of covert communication channels.

Effective border security management must include a strong and credible air defence system. Hence, the DRDO has developed ADC&RS). The primary aim of the system is to detect all aerial targets and neutralise the threat well away from the vulnerable area/vulnerable point (VA/VP) through the effective integration of all air defence weapon systems. Through CAIR, DRDO has also worked on the Command Control Communication and Intelligence (C3I) System consisting of networked computers that help in providing real-time situation awareness of critical areas concerned with security.



Chapter

3 Challenges

Different sectors of our border pose different sets of challenges and complexities. This section attempts to outline some of the major challenges that have been identified across various land border areas.

3.1.1. Indo-Pak border challenges

The Indo-Pakistan border was created in 1947 based on the Radcliffe Line, covering a length of 3,323 km along the states of Jammu and Kashmir, Gujarat, Punjab and Rajasthan. This is one of the most active borders and faces key challenges like infiltration and smuggling. This border has also witnessed several clashes with Pakistan, with the major ones being in 1947, 1965, 1971 and 1999.

Although several attempts have been made since independence to settle the border issues through negotiations and discussions, like the Indus Waters Treaty. However, critical issues like the Pakistan-occupied Kashmir, Sir Creek dispute, cross-border terrorism and ceasefire violations have remained the key challenges plaguing this part of the Indian border and our armed forces.

The harsh and varied climatic conditions along this 3,323-km of border compound the challenges faced by our armed forces in securing these areas. An increase in ceasefire violations and infiltration attempts have been observed during the pre-winter season, when vigilance becomes extremely tough due to snowfall along the mountainous terrain.

Other factors like the political instability and crisis in Pakistan also lead to an upsurge in cross-border infiltration and threats due to terrorism, creating tension along the border areas.

Cross-border terrorism stands out as one of the major reasons of disaccord between India and Pakistan. As a control measure, India started fencing its border in the 1990s and successfully completed fencing Jammu and Kashmir, Punjab, Rajasthan and Gujarat by 2011. Fencing and floodlighting, together with electrification, have been successful in checking all sorts of infiltration to a great extent. A stretch of 1,952 km of border length was floodlighted and a stretch of around 1,958 km of border was fenced by 31 Dec 2014.[5]

State-wise details of fencing along the Indo-Pak border

Name of state	Total length of border	Total length of border to be fenced	Length of border fenced thus far	Remaining length of border proposed to be fenced
Punjab	553	461	462.45*	–
Rajasthan	1037	1,056.63	1,048.27*	–
Jammu International Border	210	186	186.00	–
Gujarat	508	340	261.78	78.22
Total	2,308	2,043.63	1,958.50	78.22

[5] *MHA Annual Report, 2014-15. Retrieved from mha.nic.in/annualreports*

State-wise details of floodlighting along the Indo-Pak border

Name of state	Total length of border	Total length of border to be floodlighted	Length of border floodlighted thus far	Remaining length of border proposed to be floodlighted
Punjab	553	460.72	460.72	–
Rajasthan	1,037	1,022.80	1,022.80	–
Jammu International Border	210	186	176.40	–
Gujarat	508	340	293.00	47.00
Total	2,308	2,009.52	1,952.92	47.00

Source: MHA Annual Report, 2014-15

3.1.2. Indo-China border challenges

The India-China border, known as the McMahon Line, is spread over a distance of 3,488 km. Originally the Indo-Tibetan border (before the occupation of Tibet by China in 1950), this border remains disputed along its entire length and is one of the key points of friction between the two countries over the past years. Although confidence-building measures such as the appointment of special envoys and formation of joint working groups have been initiated time and again, incidents along the border have been reported in the past. All this makes it imperative for the Indian armed forces to maintain constant vigil along the LoAC (Indo-China border).

3.1.3. Indo-Bangladesh border challenges

India shares 4,096 km with Bangladesh. This is the fifth longest international border in the world. The length covers different geographical terrains such as open area, plain, a river and jungles. The states of West Bengal, Assam, Meghalaya, Tripura and Mizoram adjoin Bangladesh on three sides. Since the partition in 1947, the primary challenge on this side of the border has been the influx of illegal immigrants. Over the years, due to the porosity of the border, a large number of illegal immigrants have continued to enter India, especially the adjoining states, leading to serious burdens on state resources, infrastructure and contributing to vast changes in the demographics of the state.

The large settlements of illegal immigrants have also been the cause of social unrest and underlying tensions in the northeastern states. The local population is overwhelmed by the presence of outsiders and the resulting impact on their way of life. This social unrest is a cause of concern for the Government of India, as it poses a serious threat to the internal security of the country. Illegal immigration, including both refugees and economic migrants, has been a persistent burning issue for the state and central governments in India.

Another major challenge with this part of the Indian border is the smuggling of arms, ammunition and drugs, which has increased the number of anti-national elements illegally entering through this porous border.

With the porosity of the border being identified as the main problem, the Government of India has taken initiatives such as the construction and repairing of the fence along the border. To protect the border from infiltration, smuggling and any other sort of cross-border terrorism, however, more efforts are needed is required in the region.

To address the above-mentioned challenges, 383 additional BOPs have been sanctioned to be constructed along the India-Bangladesh border, which already has 802 BOPs. Land custom stations have been built along the border in the states of West Bengal, Meghalaya, Assam, Tripura and Mizoram. As per the MHA Annual report of 2016–16, out of 383 sanctioned BOPs, 65 have been completed and 78 are in progress.

Name of state	Number of BOPs		
	Approved	Already existing	To be established
West Bengal	633	410	223
Meghalaya	125	108	17
Assam	91	85	06
Tripura	245	181	64
Total	1185	802	383

(Source: MHA Annual Report 2015-16)

State-wise details of fencing along the India-Bangladesh Border

Name of state	Phase I		Phase II		Total (Phase I + Phase II)	
	Sanctioned	Completed	Sanctioned	Completed	Sanctioned	Completed
(1)	(2)	(3)	(4)	(5)	(6)	(7)
West Bengal	507.00	507.00	913.33	734.73	1,420.33	1,241.73
Assam	152.31	149.29	77.57	74.6	229.88	223.89
Meghalaya	198.06	198.06	263.2	150.99	461.26	349.05
Tripura	–	–	865.99	752.78	865.99	752.78
Mizoram	–	–	348.68	146.93	348.68	146.93
Total	857.37	854.35	2468.77	1,860.67	3,326.1	2,710.02

State-wise details of floodlighting along the India-Bangladesh border

Name of State	Sanctioned	Completed	Balance
West Bengal	1,134.13	956.69	177.44
Assam	208.74	217.44	0
Meghalaya	443.00	156.6	286.4
Tripura	718.47	660.8	57.67
Mizoram	335.66	51.11	284.55
Total	2,840.90	2,042.64	806.06

Source: MHA Annual Report 2015-16; status as on 31 Dec 2015

3.1.4. Indo-Nepal border challenges

The India-Nepal border is an open border that covers a length of 1,751 km. Being an open border, it has provided a platform for strong bilateral relations. It has also been the cause of illegal activities such as smuggling of drugs, stolen vehicles, and arms and ammunition into the country. Lately, anti-social elements and terrorist organisations are also using this open border for a least resistance passage into India, thus posing a serious security threat to the states along the border and the internal security of the country as a whole.

The open border with Nepal has been exploited by terror groups. Thirty-one battalions of SSB have been deployed to check all such activities at the India-Nepal open border. Moreover, there have been discussions at various levels to set up platforms for dealing with issues of mutual concern.

3.1.5. Indo-Myanmar border challenges

India shares a porous border with Myanmar that spans across Arunachal Pradesh (520 km), Nagaland (215 km), Manipur (398 km) and Mizoram (510 km). Fencing is very thinly done and has been a concern for the United Nations Drug Control Program (UNDCP) and International Narcotics Control Board (INCB), as it has been witness to drug trafficking. There is a Free Movement Regime up to a distance of 16 km along the border.

Though the border between India and Myanmar is properly demarcated, its porous nature of border is a great threat to border security. More than 30,000 people live along the Indo-Myanmar border within a radius of 10 km; they can cross the border at any time without any visa restrictions. The open border and cross-ethnic ties among the tribal community help insurgents escape from the hands of the border security forces. These insurgents are extensively involved in drug trafficking, especially in areas such as Moreh in Manipur and Golden Triangle covering Northern Thailand, Laos and Myanmar. Although the government is taking steps to ensure better border management and robust fencing, these activities have been suffering due to protests from the local tribal community and the hilly and inhospitable terrain, which makes movement and development of the area difficult.

The Government of India has allocated a fund of around 30.96 crore INR to fence the area between pillar number 79 and pillar number 81, which covers a length of around 10 km. There were huge protests from the local tribal community and the work has been halted after construction of 4.02 km of fencing. Approval from the Ministry of External Affairs is awaited to resume the work.

3.1.6. Indo-Bhutan border challenges

Like the Indo-Nepal border, the Indo-Bhutan border is an open border and is properly demarcated. The demarcation conflict lies along the tri-junction where China comes into the picture. The India-Bhutan border is 699 km long and proper demarcation was completed in the year 2006. Smuggling is one of the major concerns along this border. Steps have been taken by governments on both sides of the border to ensure bilateral cooperation. Additionally, the Indian government has also approved a budget of 1,259 crore INR for the construction of 313-km long border roads along the Indo-Bhutan border.

The Government of India and Government of Bhutan have agreed for bilateral cooperation on the issue of border security. Insurgent camps established in the southern districts of Bhutan were successfully eliminated by the Royal Bhutan Army forces between 2003 and 2004. This military operation is widely known as ‘Operation All Clear’



Chapter 4

Way forward: Smart border management

Smart border management aims to modernise our country's existing border management by improving the quality and efficiency of border-crossing processes. It further aims to help India and neighbouring countries to deal with increasing traveller flows, without necessarily increasing the number of border guards and patrol forces. The fundamental objective of smart border management is to promote mobility between India and other countries in a secure environment while contributing to the fight against terrorism, drug trade, smuggling, illegal activities and other serious crimes.

Thus, in this context, smart border management is a stronger, more efficient and transformational solution towards border management that lays emphasis on improved controls for border security, smarter information systems for intelligence gathering, and preventing and acting upon any threats in a more planned and sophisticated manner using the latest technological advances.

4.1. Trends

In the last several years, we have tried to delve into and explore areas that mandate a greater need for advanced security for our country's borders. Various trends today are prompting the need for a better and smarter border management framework.

This section details these trends and tries to identify their impact and disruptive effects, if any, on border management and the global security environment.

4.1.1. Demographic and social change

India is the second most populated country in the world. With advances in healthcare and increase in average life expectancy, this growth is escalating. Explosive population growth in India contributes to everything from shifts in economic power to resource scarcity to changes in societal norms. As the population grows, the demand for effective border management increases.

Today, more people can afford to travel to other countries. In 2015 alone, the world's airlines carried over more than 3 billion passengers. These trends suggests the need to put better security controls in place in order to effectively monitor and gauge the vast numbers of people and goods moving in and out of the country. At the same time, tighter entry-exit controls are needed to contain illegal migration and trafficking.

4.1.2. Shift in global economic power

The focus on national growth is increasing at a fast pace. Shifts in global economic power have resulted in significant changes in the patterns of demand from border agencies as economic growth drives the burgeoning population classes in our country and increases export production. The movement of goods and services in open market conditions has also grown exponentially. As a result, our government is faced with challenges such as smuggling of illicit goods, human trafficking and smuggling of drugs.

4.1.3. Accelerating urbanisation

According to 1901 Census, less than 12% of India's population lived in cities. Currently, that proportion has risen to 31% as per the 2011 census and, by 2030, the UN projects that 40% of the country's population will reside in urban areas. Urbanisation and globalisation are driving increasing volumes of travellers, both legitimate and illegitimate, to cross borders. This imposes greater pressure on the various agencies involved in border management to create and maintain border-crossing infrastructure and ensure secure transport hubs. There is a need to effectively regulate the travel flows in partnership with transport operators to offshore controls and enable the use of technology solutions for identity management, movement tracking and automated decision making.

4.1.4. Resource scarcity

Even though the exchange of people and goods has increased exponentially over the last several years, the border management resources, including patrol forces, border guards and security personnel to man border checkpoints, have remained limited. Scarcity of resources is a national economic concern. There is a greater need to deploy systems that are automated and 'smart', thus reducing the dependency on manual controls currently required by our border management agencies.

4.1.5. Technological breakthroughs

With every new advancement in technology and research and development capability, the productive potential of enterprises has increased. These advancements are also increasing the sources of threats to their disruption and destruction. New automation techniques, analytics and communication devices are creating new vulnerabilities that pose challenges for law enforcement, security and defence organisations. The new technologies that have

emerged in the field of surveillance and security, such as the combination of infrared and thermal cameras, surveillance drones, Internet, smart handheld devices, data analytics, artificial intelligence, and cloud computing, have become increasingly essential to border management agencies. It is imperative that the border management agencies develop and embrace these new innovations and, at the same time, put more focus on capacity building and change management.

4.1.6. Terrorism

Over the years, terrorism has risen to new proportions. Terrorists, radical religious or ethnic sects, and rogue tribes possess the power to illegally get their hands on the latest weaponry. And the disturbing trends of unconventional weapons proliferation, including weapons of mass destruction (nuclear, chemical and biological), hint that these groups can carry out catastrophic attacks. There have been numerous instances in the past when terrorists from our neighbouring countries have managed to infiltrate our porous borders and wreak havoc on the lives of innocents. Lack of effective border management thus allows these agents to harm citizens, gain access to critical national infrastructure and disrupt the nation's vital lifelines.

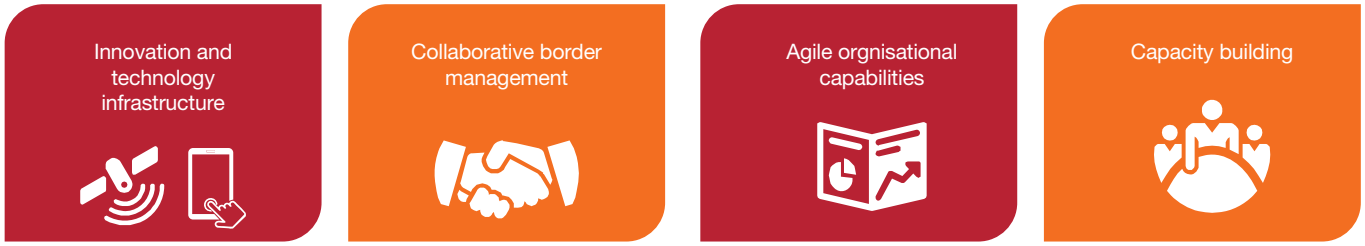
4.2. PwC's Smart Border Management framework[6]

Considering the implications of the above trends, a smart border management programme for Indian Borders is the need of the hour. Smart border management will create a balance between lawful and illegal migration, combat transnational criminal and other national security threats, and enhance the sovereignty of India and neighbouring countries.

Our expertise has highlighted the need to integrate resilient security with a modern and effective approach to border management. We therefore suggest that border management agencies adopt a proactive and resilient approach comprising four key elements: innovation and technology infrastructure, collaborative border management, capacity building and agile organisation.

As the figure below depicts, these four elements are interdependent, and require robust performance indicators to ensure effectiveness, vigilance, and continuous improvement.

PwC's Smart Border Management framework



6 *https://www.pwc.com/m1/en/publications/documents/the-future-of-border-management.pdf*

4.2.1. Innovation and technology infrastructure

The nations of the world have been busy equipping themselves with the latest and deadliest weapons in a bid to ensure their security. This attitude has created significant challenges in border management. These technologies are also being misused and exploited by terrorists. Attacks such as the 26/11 attack, the Pathankot Airport attack and regional bombings have elevated the need for better management of borders.

There is no fixed definition of a smart border. It can vary from country to country depending on the level of technological advancement. Different layers of smartness can be added to border management. The Smart Border Management framework suggests the following technology infrastructure for Indian borders:

- Smart identity management
- Smart inspection system
- Monitoring and surveillance system

4.2.1.1. Smart identity management

Border security management resources cannot grow in volume at the same pace as that of the travelling population. The combined forces of burgeoning cross-border traffic, severe infrastructure constraints, and, ironically, added delays that result from stepped-up efforts to detect and intercept illicit activities at the border are making the border more difficult to police. Passenger processing, security checks, etc., must be quick and secure enough to prevent any sort of inconvenience to legitimate travellers. Hence, border management agencies have to proactively identify any potential breach of security that might pose a security risk to the nation.

The use of biometrics (photographs, fingerprints, face, iris, etc.) for identification is one of the smart ways of identity management. It is smart because these means of identification always remain with the individual and cannot be changed or forged easily. It also reduces processing time considerably. Biometrics can be used to accessing the social and financial health of an individual, such as criminal record and tax liabilities.

The following are key aspects of the different biometric technologies available for smart identity management:

1. Photographs are popular basic biometrics due to their simplicity. However, they are not considered sufficiently reliable, e.g. for international travel purposes, as individuals may bear resemblance to one another, making it impossible to distinguish them under operational conditions.
2. Fingerprints are the oldest and most widely adopted biometric technology used in smart identity management. As a result, this is the most mature of all biometric technologies.
3. Face recognition uses the structure and spatial geometry of landmarks such as the nose, eyes, lips and jawline. It can be performed on 2-D and 3-D images. This technology has improved significantly over the last decades.
4. Iris recognition uses the pattern that is formed by the muscle tissue and cell structure in the iris region of the eye. The iris image is captured using infrared illumination and a camera. It has attracted a lot of attention in the last decade.
5. Hand geometry recognition uses the contours of the hand, the length and thickness of the fingers and the spatial distance between other landmarks of the hand. It is heavily recommended in physical access control applications.
6. Voice recognition uses characteristics such as the pitch, intonation and vocal speed of an individual's voice. It has seen low adoption in the commercial sector.
7. Vascular pattern recognition uses vein patterns. Veins carry deoxygenated blood back to the heart, and research indicates that the pattern formed by the vascular network is relatively unique and permanent.
8. Dynamic signature verification uses velocity, direction, number of strokes, time of each stroke and pressure applied by the user during the signing process.
9. DNA was originally been used in forensic sciences, but is now pursued as a biometric technology. However, there are still issues to be addressed such as invasive data capture, processing time (hours rather than seconds) and price.

The utilisation of the above biometric technologies as stand-alone methods or in combination with incorporate multiple layers of security is suggested in smart identity management. For example, fingerprints can be used to check the registration of a traveller in the system, while facial recognition can be used for quick, reliable and automatic verification at subsequent entries.

Individual ID and family ID will help track the individual easily and will check fraud in the ID creation process. Every individual ID can be linked to the family ID to trace the identity details of a traveller backwards. This data can be derived from passport, Aadhaar card, Voter ID, immigration database, etc., and the database created from these sources can be the reference data to be used by border security management agencies. This big data can be used by analytical tools to create a list of suspicious profiles, identify high-risk zones. In addition, it can used for resource profiling and deployment for screening any sort of intrusion.

A frequent traveller programme can identify low-risk travellers and help them with easy access facilities like self-service kiosks at the airport. This can save a considerable amount of time and effort for both travellers and security personnel. Travellers should be entitled to avail of this facility only after a proper background and history check.

4.2.1.2. Smart inspection system

A smart inspection system uses a smart identity management system that ensures that only legitimate people are allowed to engage in cross-border management. Further, these people should not be carrying items that are not permissible according to the law of the land—for instance, weapons and drugs. This calls for s smart system that de-risks the border from the entry of any such hazardous material. The most advanced scanning technologies need to be installed at entry points; these devices should be quick and accurate. Non-invasive inspection techniques such as explosive vapour detectors, full-body scanners, metal detectors and handheld substance detectors can be used for the detection of concealed weapons, drugs, illicit radiological material, etc., while saving time and manpower.

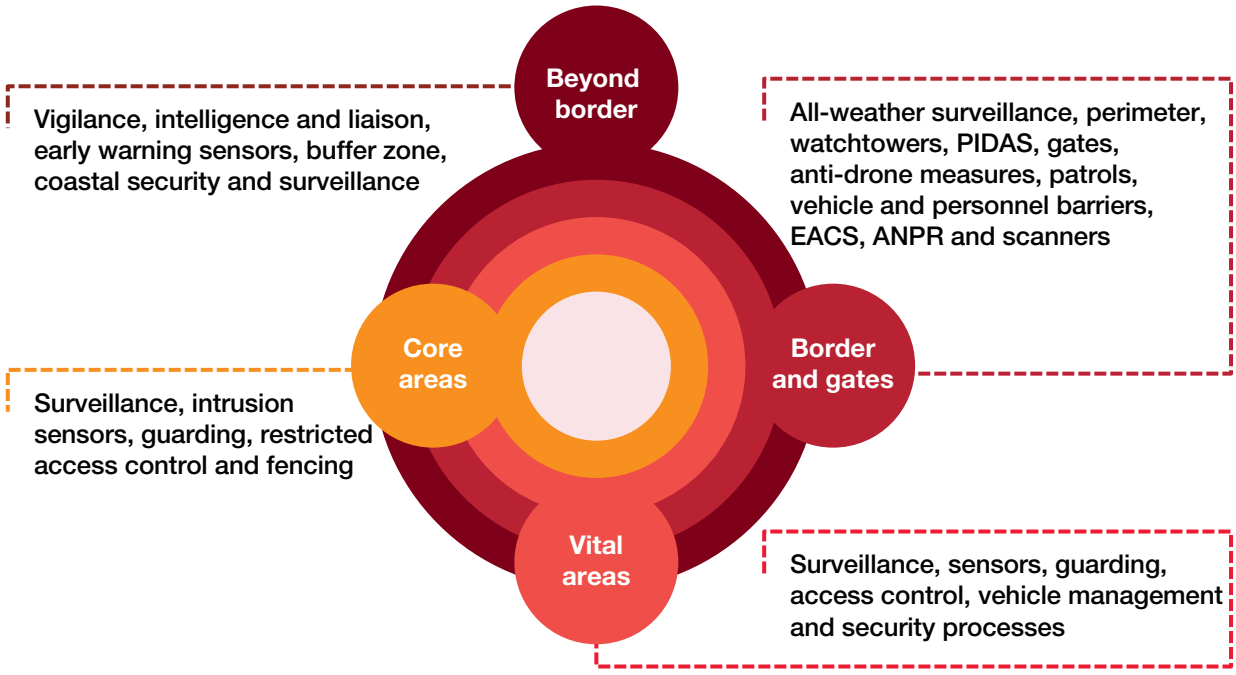
Verifying legitimate cross-border vehicle or people flows is also sometimes difficult. Aggregate border-crossing numbers are sometimes misleading, since the same vehicle and a driver pass through the border and are recorded as different entities. Mostly, vehicles involved in illegal practices have sufficient incentive to repeat the act owing to lack of border controls. After undergoing a pre-screening application and inspection process, vehicles can be equipped with an electronic transponder and the driver can be provided with an ATM-style identity card with encoded handprint or retina information to verify their identity.

ePassports and eGates are being used by some countries to automate the inspection process and increase the effectiveness of cross-border movement inspection systems. An ePassport contains the same information as that present on the hard-bound copy; however, it eliminates the risk of forgery that is associated with normal passports. An ePassport can be customised as per security requirements. The eGate facility was first installed in Singapore and is one of the most advanced immigration biometric technologies that uses documents like passports and travel documents for authorisation and hence minimises the risk of illegal immigration.

4.2.1.3. Security and surveillance system

Monitoring and surveillance systems act as force multipliers to the armed forces personnel who have been deployed at our border areas to guard against any intrusion or threats. These systems enable 24x7 operations and effective and efficient surveillance of the AOI at the border areas. These systems typically comprise a sensor layer, which is arranged strategically to allow a layered defence mechanism; a network backbone, which allows data transmission in real time from the field locations to the relevant stakeholders; and a command centre where all decision makers and stakeholders can monitor and analyse the incident and initiate the response mechanism for incident management and control based on pre-defined standard operating procedures (SOPs).

A typical layer defence concept that can be utilised to organise security and surveillance systems is presented below. The outermost layer comprises all systems and mechanisms used for early detection of incidents/ infiltrators beyond our borders. This layer typically consists of systems like early warning sensors, radars and thermal imaging cameras with analytics, and mechanisms like vigilance and intelligence gathering from reliable sources. The second layer comprises intrusion detection systems, watchtowers, surveillance cameras and laser curtains, which are typically deployed at border areas along the border fence. The third and the fourth layers of the diagram depict the systems which may be used to protect vital installations and core areas of operations using surveillance systems, intrusion sensors and access control.



The objective of security and surveillance systems deployed at each layer is D4R2 (deter, detect, discriminate, delay, respond and recover). That is, based on the functions they perform, the deployed systems will deter any act of forced intrusion/criminal activity by anti-national forces, detect the presence of any unauthorised personnel, and delay the intrusions until the response mechanism is activated and the situation is brought in control. Furthermore, once threat mitigation/incident management is achieved, a recovery mechanism can be initiated for the system and applications to perform post-incident analysis, pattern analysis and vulnerability mapping.

4.2.2. Collaborative border management

In this era of globalisation, economic growth is not only defined by parameters such as internal growth and stability but also on the degree of connectedness with the global community in terms of trade, policymaking and technology. Collaborative border management is basically aimed at improving trade, commerce and security by enhanced coordination between border agencies. In the current structure of border management, goods and people have to comply with innumerable compliances and measures which leads to wastage of time and effort. Goods are made to wait longer at border areas which either leads to wastage or impacts the price of the product.

Borders have evolved with the passage of time and they do not remain just a mere physical border. ICP at Attari did trade of 2,742 crore between April to December in FY 2015–16. Borders have become gateways of trade and commerce and due consideration has to be given on this aspect as well. Collaborative border management (CBM) brings together security agencies and industries to work on designing the processes that would allow easy passage for legitimate people and cargo and at the same time, protect the border areas from any sort of national threat from neighbouring countries. Categorisation into different risk buckets will help in easy identification of suspicious elements trying to cross the border. An overwhelming majority of vehicles, people and cargo that move across the Indian borders operate along predictable patterns. If we empower our border agencies with the means to analyse and keep track of these flows, they will have the ability to detect unnatural or awkward behaviours. This can only happen if a seamless exchange of information takes place between various stakeholders, and border management agencies are provided access to timely intelligence about real or suspected threats.

Technology integration can add multiple layers of smartness in the enterprise that CBM targets to set up. However, cost benefit analysis should be done since this would require investment in developing the infrastructure and integrating the technology.

The Smart Border Management framework recommends the adoption of the following principles of CBM for both domestic stakeholders or security agencies and neighbouring countries for smarter border management.

4.2.2.1. Cross-border cooperation (CBC)

The core principle of cross-border cooperation (CBC) is the information sharing and collaborative approach between neighbouring countries for border security for issues such as human trafficking, arms or drugs smuggling, terrorist threats, etc. The main robustness of such an approach lies in the fact that it maintains the jurisdiction of the two nations as both continue to control their own security policies. It is recommended to share the national databases of citizens, criminals, watch list, etc. for purposes of migration and border management. Access to such database shall be provided only to designated authorities of the neighbouring countries for the purposes of prevention, detection and investigation of terrorist offences and of other serious criminal offences. The establishment of joint BOPs, joint cross-border patrols, providing access to border roads to neighbouring countries for patrolling in case of limited road infrastructure, sharing of crucial intelligence information for border security, etc. will be incorporated as an integral part of CBC. This will help in building trust and communication between the neighbouring border control agencies and develop spontaneous information exchange about areas such as goods movement, suspects and vehicle across common borders.

4.2.2.2. Public private partnership (PPP)

Adoption of the public private partnership (PPP) model will support border management to counter border infrastructure problems. The encouragement of private investment will not only save the government resources but also allow the best practices, innovation, knowledge to be inherited for designing of border infrastructure which will be commerce-friendly without threatening the country's security and sovereignty. The various agencies involved in border management can encourage the private sector to take these steps in a number of ways, for example, establishment of a PPP model similar to the Customs-Trade Partnership against Terrorism (C-TPAT) model which is joint government-business partnership by the US Customs and Border Protection (CBP) to help and support the supply chain and increase border security. If the Indian government and the public sector undertake these changes, the private sector must also change its attitude about engaging in self-policing and sharing anything but the minimum amounts of relevant data with government agencies to help contain the border situation.



Collaborative border management

4.2.2.3. In-country collaboration (ICC)

In-country collaboration (ICC) will include participation of all country stakeholders which will comprise of forces at district borders, community policing, citizens residing in border areas, etc. The following collaborative strategies may be considered for smart border management.

1. Community policing

Community policing focusses on dynamic, transparent and a collaborative partnership between the citizen, government agencies, business community, media and other stakeholders for quick identification of problems and their efficient and effective resolution. Citizens become equal stakeholders in the resolution of these issues and hence this enforces transparency and accountability in the issue resolution mechanism. The existing system of policing was more confined to get hold of criminals by collecting evidences against them for the prosecution process. There was limited or no involvement of the citizen in the entire process which led to resurgence of the same problem or crime. Community policing does focus on getting hold of criminals and it is one of the important aspects, but what it does more is the involvement of the police, citizens, businessmen as well as government agencies in identifying the problems of society and provides a permanent solution to the issues. Some of the activities that comes under the scope of community policing and the ones which have been implemented at the India-Nepal border include rolling out measures for minimising violence and crime rates, emergency and disaster management, social awareness campaigns, community services, volunteer mobilisation, etc.

Human trafficking is one of the major areas of concern in border areas. Community policing can increase the vigilance of citizens across different layers in society. It is not possible for the police alone to keep an eye on the entire border stretch, and hence, involving the citizen can help in identifying suspicious activities within their respective localities. Rehabilitation of victims can also be facilitated by the process of community policing so that they resume normalcy in their day-to-day activities.

Robust community policing needs to be a key component of a smart border strategy. Community policing is a 'collaboration between the police and the community that identifies and solves problems' in a proactive and resilient manner. It will help in deterrence of various types of crimes at the border which in turn will help the department's challenge of policing the border in a more manageable manner.

2. State-level participation

It is suggested that the agencies involved in border management should consider the following initiatives at the state and district levels for smart border management:

- Establishment of a marketing strategy which will involve communications to all district borders about the smart border management programme and nationwide implementation with creation of a national centre for best practices and lessons learned.
- Establishment of a strategy for the formation of the state defence forces which will develop team effort at the border by increasing manpower resources. This should also incorporate the provisioning of funds for establishment of system and standards for state defence forces to increase border safety.
- Awareness programmes shall be organised in collaboration with border states as well as districts to guide and protect citizens residing in border areas with legal guide pamphlets, guidelines, etc.

4.2.3. Capacity building

Over the years, there has been a paradigm shift in the way terrorists carry out their attacks at national borders. Latest technologies and sophisticated weapons are being used to execute these attacks. And, this is the reason why capacity building has assumed such a high priority in smart border management. Community police forces have to be empowered with efficient use of latest technologies for investigating crimes, proactively collect information on potential threats, tracking the criminals and neutralising them before they cause any harm to the nation, disaster management, emergency situations, bomb disposals, etc. The success of technology advancements in ICT implementation for security totally depends on the readiness of our forces to understand and then implement them.

Capacity building and change management forms an integral part of smart border management since it will develop the capability of defence forces to maintain one's own safety, minimise liability, ensure that the forces understand and fulfil their missions of national security. The agencies involved in border management shall ensure that all existing and new recruited security personnel shall receive adequate and frequent trainings, provide funds for the construction of new classrooms, living space, firing ranges, physical fitness facilities, and training areas at the

border police academies. The agencies involved in border management need to establish faster and more innovative training avenues and strategies for capacity building and change management without sacrificing the quality of training. An example of such a solution would be to conduct computer-based training programmes at border academies that will decrease the training costs and enable sharing of knowledgeable best practices and learnings across various defence forces. The border management agencies may also collaborate with local computer institutions to utilise their existing infrastructure for remote training campuses.

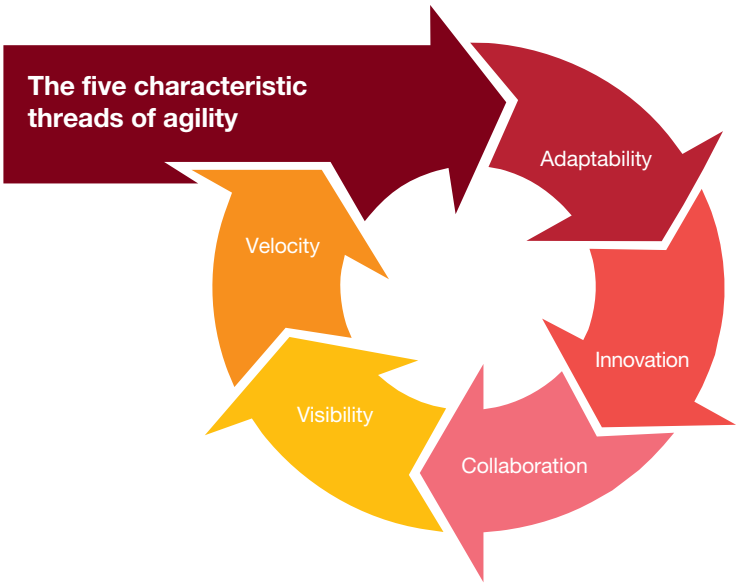
4.2.4. Agile organisational capabilities

In recent years, the border management policy and practice have often worked reactively, since governments struggled to respond to events, emerging threats, and the growing demand for services. These demands will increase with a surge in the number of travellers and more goods will be traded which will result in diversified range of increased national threats. The Smart Border Management framework recommends that the government departments and various stakeholders involved in border management adopt an agile and flexible approach to provide effective and resilient security against these threats.

The concept of agility is especially relevant to border management agencies owing to the high-risk and fluid portfolio of threats that they manage. Agility is defined as perpetual awareness and the ability to be decisive and take action in an expedient and well-coordinated manner. Different terms can apply to the same concept, but what is important is the underlying idea. An agile border management organisation retains its core tenets while empowering units to evolve in response to the environment. Agility at an organisational level is the strategic mix of standardisation and flexibility, targeted at those organisational pressure points where they are not only needed today, but will most likely be needed tomorrow. This model provides a consistent vision and structure while allowing for operating flexibility.

We believe that there are five characteristics of an agile organisation. We identify these characteristics as 'threads' because of how they should weave their way through the key processes of an organisation in a complimentary fashion. In agile organisations, threads function to produce highly effective actions that anticipate and mitigate a broad range of tactical and strategic challenges.

Five characteristic threads of agility



Chapter

5 Case studies

5.1. African Union border[7]

5.1.1. Introduction

African countries were facing daunting tasks of managing their borders to: secure their territorial sovereignty; manage their borders as bridges rather than barriers for cross-border cooperation and regional integration; prevent illegal entries and exiting of people and goods while allowing easy movement of goods and people; allow relatives to visit their kin while keeping away criminals (such as drug and human traffickers, terrorists, etc.); and facilitate tourists to easily cross while keeping out terrorists.

Challenges faced by African states to manage their borders were compounded by globalisation that was tearing down traditional borders through advancement in technology and transformation of international relations. Currently, crimes and transactions of huge amounts of illegal goods are conducted through cyberspace. The Internet has not only made it more difficult to manage borders and combat cross-border crimes, but has also effectively dismantled borders by allowing imports without going through customs.

The main sources of insecurity at the African border were as follows:

- Lack of political desire and engagement of resources for effective border management
- Lack of cooperation between in-country stakeholders and inter-country stakeholders
- Insufficient availability of manpower and skillset for deployment on the borders
- Inadequate intelligence communication between agencies and countries
- Lack of security infrastructure at borders
- Lack of facilities (accommodation, offices, etc.) for border patrol and control personnel
- Inadequate communication channels and infrastructure for border management
- Lack of road and transport infrastructure along borders for border patrols
- Poorly demarcated borders; illegal border-crossing points

These issues coupled with an increase in volumes of cross-border trading and movements of people from their countries of origin had put enormous pressure on border control systems. These realities had led African countries to put in place effective border management systems to: minimise border tensions; increase joint enforcement and surveillance efforts; decrease organised crime activities by syndicates and traffickers in borderlands; generate common understanding of border insecurities and approaches to addressing them; secure flow of goods and people in the spirit of regional and continental integration; integrate and develop marginalised border areas through provision of essential infrastructure and promotion of a sense of security; well-being among the border population; enhance communication and information exchange between neighbouring countries; maintain borders in ways that do not obstruct cross-border trading and legal movements of people; and enable borders to be sources of mutual trust and harmony between neighbours.

5.1.2. Solution and key features

The African Union (AU) had launched the African Union Border Programme (AUBP) in 2007 as a direct response to the above mentioned risks. The core building blocks of the programme were: border delimitation and demarcation; cross-border cooperation; and capacity building among AU member states. The Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH, on behalf of the German Federal Foreign Office supported the AUBP for rendering implementation assistance on the continental, regional, national and local level.

The AUBP was implemented through the following core principles of smart border management:

5.1.2.1. Delimitation and demarcation

Delimitation and demarcation of borders and reaffirmation of demarcated borders were done between AU member states as a core principle of AUBP.

5.1.2.2. Cross-border cooperation

Under the cross-border cooperation principle, joint plans and development of cross-border areas and wider infrastructural facilities such as transportation, communication, etc. were taken up by AUBP.

[7] https://www.researchgate.net/

5.1.2.3. Capacity building

GIZ project advised AUBP unit for elaboration and implementation of strategic plans in the areas of human resources and organisational development. This included training and research activities, development of infrastructure and specialised institutions in the support of smart border management and regional-level integration activities between AU member states.

5.1.3. Impact and achievements

With the implementation of the core principles of the border management programme, few of the achievements of AU are as follows:

- Demarcation of 413 km of the Burkina Faso-Mali border
- Delimitation of the maritime boundary between the Comoros, Seychelles and Tanzania
- Reaffirmation of 330 km of the Mozambique -Zambia border
- Reaffirmation of 805 km stretch between Zambia and Malawi
- Ongoing reaffirmation exercises between Mozambique-Tanzania, Malawi-Mozambique, Mali-Senegal
- Establishment of the African Union Boundary Information System (AUBIS) which is a central database containing information on AU member states boundaries
- Collaboration with the Government of the Federal Republic of Germany especially through the Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH, as well as other multilateral organisations, such as the United Nations (UN), the European Union (EU), the Organization of American States (OAS), etc.
- Adoption of the Convention on the Cross-Border Cooperation in Niamey, Niger, in 2012
- Publication of the AUBP book series of practical guides on African boundary delimitation and demarcation, the implementation of cross-border infrastructure projects, creation and operation of boundary commissions, border dispute settlement, as well as a collection of all AU documents, resolutions and declarations pertaining to African borders

African Union

Learnings in the context of Indian borders

Cross-border cooperation:
Information-sharing and collaborative border management initiatives like joint border outpost (BOP) and joint cross-border patrolling between neighbouring countries can be adopted.

Capacity building:
Capability development of border forces and other stakeholders, innovative training avenues and infrastructure can be matured.

5.2. European Union border[8]

5.2.1. Introduction

European Union (EU)'s border management has witnessed considerable developments over the past decade which laid down the rules on the policy on external border crossings. The first step towards a common external border management policy was taken on 14 June 1985 when five of the then 10 member states of the European Economic Community had signed the Schengen Agreement. The Schengen area, the borderless zone, currently comprises 26 European countries. The following five categories of rules were incorporated into EU legal order by the Amsterdam Treaty:

- The Schengen Borders Code (SBC) was considered as the central pillar for external border management which specified the rules on external border crossings and conditions governing the temporary reintroduction of internal border checks.
- EU had funded few of the member states who were not having external borders and were not affected by border traffic flows.
- Centralised databases were established for migration and border management: the Schengen Information System (SIS), Visa Information System (VIS), and Eurodac which was the European fingerprint database for identifying asylum-seekers and ensuring proper implementation of the Dublin Regulation.
- A set of policies were designed in order to prevent and penalise unauthorised entry, transit and residence.
- Establishment of the European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union - FRONTEX.

5.2.2. Schengen Information System

The second-generation Schengen Information System (SIS II) is a Europe-wide large-scale joint information system for public security that enables exchange of information between national border control, police, customs and other competent authorities, ensuring that the free movement of people within the Schengen area can take place within a safe environment. Competent authorities have access to alerts on people and objects for the purposes of border checks, as well as police, customs and other checks carried out within the countries, and, to a certain extent, for the purpose of issuing visa and residence permits. At the external borders, it is mandatory to check a third country national in the SIS II before granting them access to the Schengen area.

SIS II replaced the former technical implementation of the Schengen Information System (SIS1). SIS II responded to the need of servicing an increased number of users and handles an increase number of queries.

SIS II provides the potential for additional functionalities, such as new categories of data and the use and storage of images and biometrics. It went live on 9 April 2013.

In each participating country, there is a dedicated office for handling supplementary information and bilateral or multilateral contacts with regard to the cases identified through the use of SIS II (for e.g. providing supplementary information after a hit and managing the communication necessary for further police and legal actions). These offices are called Supplementary Information Requested at National Entry (SIRENE).

Technical aspects and architecture

The SIS II architecture is characterised by the following characteristics and guiding principles:

- It is composed of a central database that is fully or partially replicated at the national level for countries that have chosen to have a national copy of the central database as part of their national architecture.
- The central system has two physical locations, one of which is used as backup system.
- SIS II allows the possibility to include fingerprints in an alert. While storage of fingerprints as images is already being used by the participating countries, the option to use it for identification has not yet been implemented.
- The retention period of data stored varies on the basis of the type of alert and the specific situation.

[8] *www.europarl.europa.eu*

5.2.3. Visa Information System

The Visa Information System (VIS) allows Schengen countries to exchange and process data and decisions relating to applications for short-stay visas to visit, or to transit through, the Schengen Area. It consists of a central IT system, national systems in all participating states and of a communication infrastructure that links this central system to national systems. VIS is accessed at Schengen consulates, at central visa authorities and at all external border crossing points (BCP) of Schengen countries.

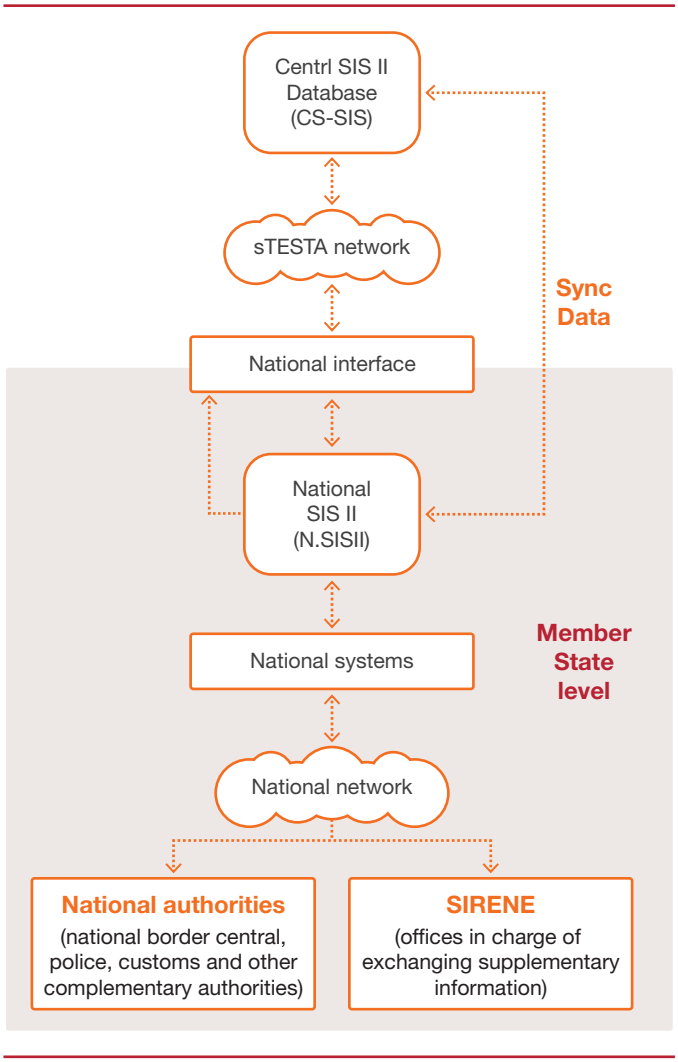
The objective of the system is to support the common visa policy and the visa application procedures, and in particular the following areas:

- To identify visa applicants and their visa history
- To check and/or identify visa holders at borders, with the support of biometric identifiers (fingerprints)
- To prevent 'visa shopping' and other types of fraud at consulates
- To assist in the fight against irregular migration
- To contribute to the prevention of threats to internal security of the member states

For each person applying for a Schengen visa, the VIS stores and retains for a maximum period of five years, both biographic and biometric information, including the following:

- Alphanumeric data (biographic information, visa information and additional information)
- A photograph of the applicant's face
- Ten flat fingerprints, which are kept valid for 59 months from the enrolment in the system, in case of subsequent applications

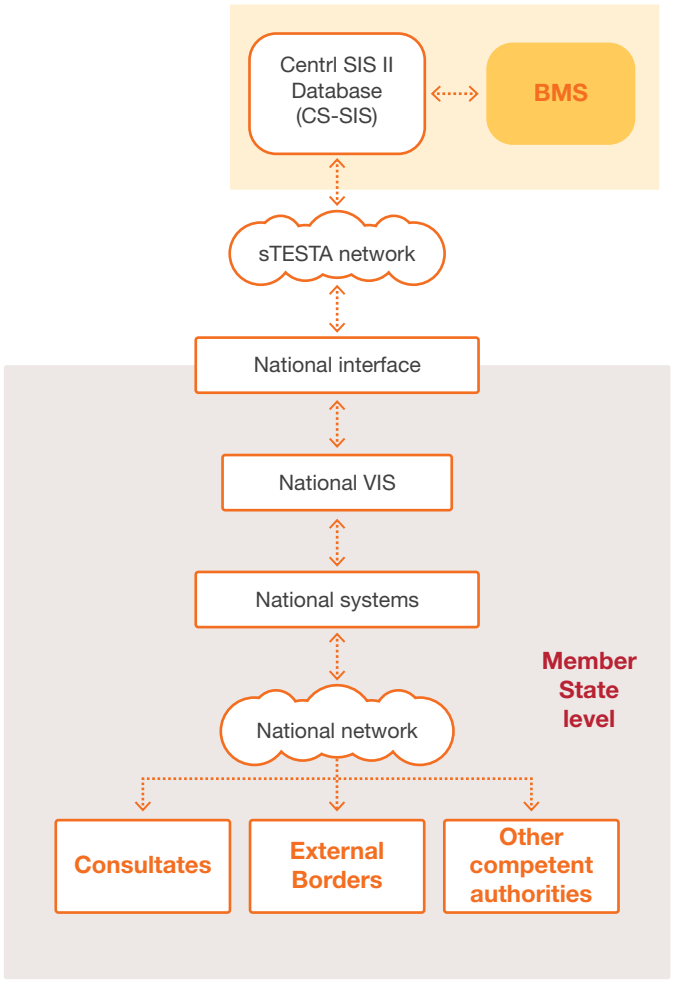
VIS started operations on 11 October 2011 and from 1 November 2011, all Schengen countries implemented mandatory checks of VIS using the visa sticker number for queries. The biometric verification at the border has also become mandatory. Each application file shall be stored in the VIS for a maximum of five years. The member state responsible shall check the data concerned and, if necessary, correct or delete them immediately. Furthermore, when an applicant has acquired a nationality from one of the member states, the application files and links relating to him or her shall be deleted without delay from VIS by the member state which created the respective application file(s) and links.



Technical aspects and architecture

The VIS architecture has the following characteristics and guiding principles:

- VIS is a central system with two physical locations, one of which is used as backup system.
- The VIS architecture includes a biometric matching system (BMS) for fingerprint matching. Member states do not connect directly to the BMS, but only through VIS.
- Ten fingerprints are enrolled, however only one to four fingerprints are necessary for verification.
- Access is provided only to designated authorities of the member states for the purposes of prevention, detection and investigation of terrorist offences and of other serious criminal offences.



5.2.4. Entry-Exit System

The Schengen Borders Code has no provisions on recording the travellers' cross-border movements into and out of the Schengen area. As a general rule, third country nationals have the right to enter for a short stay of up to 90 days within any 180 day period. Currently, the stamping of the travel document indicating the dates of entry and exit is the sole method available to border guards and immigration authorities to calculate the duration of stay of third country nationals and to verify if someone is overstaying. These stamps can be difficult to interpret, they may be unreadable or the result of counterfeiting. Similarly, it is difficult for consulates having to process visa applications to establish the lawfulness of previous visas on the basis of stamps present in the travel document. As a result, the whole procedure is considered error prone and not always systematically implemented.

As a counter measure to the problem, the European Commission and European Parliament (EP) are under the process of examining the proposal of the Entry-Exit System (EES) for recording of information on the time and place of entry and exit of third country nationals entering the Schengen area and amendments in the Schengen Borders Code since February 2013. Based on the findings of the technical study, test results of the pilot project, the technical discussions with co-legislators and stakeholders as well as a public consultation, the Commission prepared a detailed impact assessment report and followed by the amended proposal in November 2015.

The key objectives of EES are as follows:

- Contribute to the modernisation of the external border management by improving the quality and efficiency of the external border controls of the Schengen Area
- Addressing border check delays and improving the quality of border checks for third country nationals
- System based identification of over-stayers
- Reinforcing internal security and the fight against terrorism and serious crime
- Assist member states dealing with ever increasing number of travellers to the EU without having to increase the number of border guards.

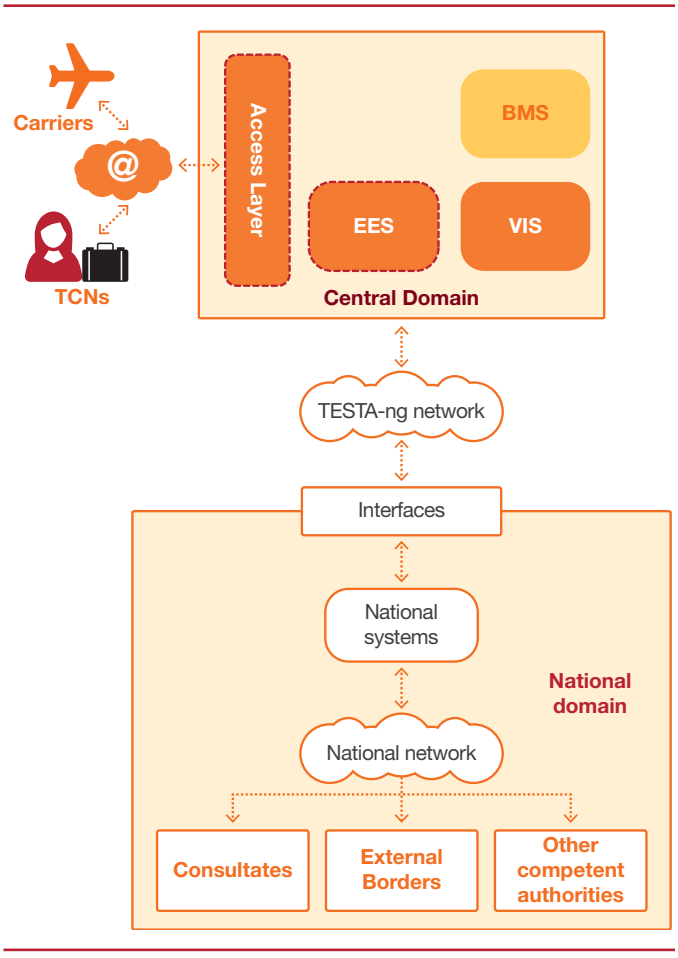
The expected outcomes of EES are as follows:

- Precise information availability to border guards during border checks, which will replace the current slow and unreliable system of manual stamping of passports and thus, providing a better monitoring of the authorised stay as well as more efficient border checks
- Travellers will be provided by precise information on the maximum length of the authorised stay
- Automated border controls for third country nationals under the surveillance of the border guards
- Identification of overstaying travellers will support controls within the territory and allow to apprehend irregular migrants more efficiently
- Identification of irregular migrants with help of stored biometrics in the EES.
- An evidence-based approach through the analysis generated by the system. In the case of visa policy for instance, EES will provide precise data on whether there is problem with overstayers of a given nationality or not, which will be an important element when deciding whether to impose or lift visa obligations on a third country in question.
- Identification of terrorists, criminals as well as of suspects and victims

Technical aspects and architecture

The guiding principles of the envisaged EES architecture are as follows:

- EES shall be a central system with connections to the national border infrastructure through a National Uniform Interface which will be identical for all member states, and will allow the use of the existing national EES. However, data from the central system cannot be copied into these existing national EES.
- Interoperability shall be ensured between the EES and VIS in order to achieve more efficiency and rapidity at border checks. To this effect, a connection will be established between the central systems of the EES and the VIS and direct access between them will be regulated for specific purposes.
- The EES shall enrol a combination of four fingerprints and the facial image as biometric identifiers which will allow accurate verifications and identifications while keeping the amount of data to a reasonable level with speeding up border controls. The four fingerprints are used at the enrolment process to check if the third country national was already registered in the system while the facial image allows for a quick and reliable (automatic) verification at subsequent entry that the individual subject to the border control is the one already registered in the EES.
- The retention time for the stored data will be five years.



European Union

Learnings in the context of Indian borders

Database sharing
Sharing of national database of citizens, criminals, watch list, etc., can be practiced.

Biometrics:
Use of biometrics (fingerprints, facial and iris recognition, etc.) for identity management can be implemented.

Interoperability:
Interoperability between immigration systems of neighbouring countries for smarter border checks can be integrated.



FICCI Security Department

FICCI has many specialised committees where key concerns of the industry are debated and discussed with the specific aim of presenting the recommendations to the government for favourable decisions.

Considering that internal security is the backbone of growth and overall development of a nation, FICCI has constituted two specialised committees to look into various aspects of security:

- The Committee on Homeland Security (HLS) is chaired by G. K. Pillai, Former Union Home Secretary, Government of India, which is working towards bridging the gap between policing and technology.
- The Committee on Private Security Industry (PSI) is chaired by Manjari Jaruhar, Former Special DG – CISF, Government of India. The committee has been advocating key policy issues confronting the industry.

Some of the focus areas:

SMART Policing: FICCI has instituted an award for best practices in SMART Policing in India, with the objective of promoting initiatives taken by the police for the safety and security of Indian citizens. This can change public perception and build a positive and progressive image of the police among people. FICCI SMART Policing Awards provide a platform to police officials across India to learn from the experiences of other states and also for possible adoption of the best practices to further enhance policing in their respective states.

Police modernisation: FICCI is working towards bridging the gap between policing and technology. We engage with various enforcement agencies and provide them with a platform to interact with industry, to articulate their requirements and to understand new technologies for security. This initiative is under our umbrella theme of 'Safe & Secure Nation'.

Road safety: United Nations has proclaimed 2011–20 as the Decade of Action on Road Safety. FICCI feels that Indian industry can play a significant role in addressing the issue of road safety and will be promoting potential private sector interventions in road safety through their core business activities.

Indian unmanned aerial vehicle (UAV) policy and regulations: FICCI has initiated formulating working groups in the areas of: (a) enabling regulations for developmental use of UAVs and prevention of rogue UAVs, (b) framework for permission and licencing for manufacturing of UAVs and (c) technological structure for detection and neutralisation of unidentified UAVs. FICCI will submit the suggestions and recommendations for Indian UAV policy and regulations to the Ministry of Home Affairs.

India Risk Survey: Every year, FICCI conducts a survey of risk as perceived by corporates, which could affect business continuity. The objective of the report is to inform and sensitise all stakeholders about the emerging risks for a developing economy like India, so that well-planned and strategic policy decisions can be made.

Security standards and guidelines: FICCI is working with the Bureau of Indian Standards (BIS) for the creation of standards and guidelines for electronic security.

Capacity-building programmes: FICCI has initiated capacity-building programmes and workshops as an attempt to increase awareness about women's safety at the workplace, forensics of fraud detection, white-collar crimes, etc.

Public procurement for internal security: FICCI is working towards advocacy for bringing well-defined procedures for the fair and transparent procurement of security products and solutions, so as to provide level playing field to the industry.

Enforcement of Private Security Agencies Regulation (PSAR) Act, 2005: A major portion of the private security industry is unorganised. FICCI is advocating the proper enforcement of the act.

Armed security for cash logistics: FICCI is advocating a well-articulated policy for the deployment of armed private security guards for the protection of cash vans which carry crores of public money every day.

Private security workers' categorisation as skilled/highly skilled workers: FICCI is working towards the appropriate categorisation of private security guards.

Minimum standards/guidelines for cash logistics companies: FICCI is advocating the establishment of standards and operating guidelines for cash logistics companies.

About FICCI

Established in 1927, FICCI is the largest and oldest apex business organisation in India. Its history is closely interwoven with India's struggle for independence, its industrialisation and its emergence as one of the most rapidly growing global economies.

A non-government, not-for-profit organisation, FICCI is the voice of India's business and industry. From influencing policy to encouraging debate and engaging with policy makers and civil society, FICCI articulates the views and concerns of industry. It serves its members from the Indian private and public corporate sectors and multinational companies, drawing its strength from diverse regional chambers of commerce and industry across states, reaching out to over 2,50,000 companies.

FICCI provides a platform for networking and consensus building within and across sectors and is the first port of call for Indian industry, policymakers and the international business community.

Contacts

Sumeet Gupta
Director
sumeet.gupta@ficci.com

Ankit Gupta
Senior Assistant Director
ankit.gupta@ficci.com

FICCI
Federation House, Tansen Marg, New
Delhi - 110 001
T: +91-11- 23487212, 23487474
www.ficci.com

www.ficci.com

© Federation of Indian Chambers of Commerce and Industry (FICCI) 2015. All rights reserved.

The information in this publication has been obtained or derived from sources believed to be reliable. Though utmost care has been taken to present accurate information, FICCI makes no representation towards the completeness or correctness of the information contained herein. This document is for information purpose only. This publication is not intended to be a substitute for professional, legal or technical advice. FICCI does not accept any liability whatsoever for any direct or consequential loss arising from any use of this document or its contents.

About PwC

At PwC, our purpose is to build trust in society and solve important problems. We're a network of firms in 157 countries with more than 208,000 people who are committed to delivering quality in assurance, advisory and tax services. Find out more and tell us what matters to you by visiting us at www.pwc.com.

In India, PwC has offices in these cities: Ahmedabad, Bengaluru, Chennai, Delhi NCR, Hyderabad, Kolkata, Mumbai and Pune. For more information about PwC India's service offerings, visit www.pwc.com/in

PwC refers to the PwC International network and/or one or more of its member firms, each of which is a separate, independent and distinct legal entity in separate lines of service. Please see www.pwc.com/structure for further details.

©2016 PwC. All rights reserved.

Contacts

Neel Ratan
India Government Leader
neel.ratan@in.pwc.com

Subhash Patil
Partner
Government and Public Sector
subhash.patil@in.pwc.com

Cdr Deepak Uppal (retd.)
Director
Government and Public Sector
deepak.uppal@in.pwc.com

Rajat Chowdhary
Associate Director
Government and Public Sector
rajat.chowdhary@in.pwc.com

Acknowledgements

Aditya Shrivastava
Associate Director
Government and Public Sector
aditya.shrivastava@in.pwc.com

Atul Gupta
Principal Consultant
Government and Public Sector
atul.gupta@in.pwc.com

Vaishalik Jain
Principal Consultant
Government and Public Sector
vaishalik.jain@in.pwc.com

Ritesh Choudhary
Senior Consultant
Government and Public Sector
ritesh.choudhary@in.pwc.com

Sanchit Nagpal
Senior Consultant
Government and Public Sector
sanchit.nagpal@in.pwc.com

Sunny Kapoor
Senior Consultant
Government and Public Sector
sunny.k@in.pwc.com

Salil Aggarwal
Consultant
Government and Public Sector
salil.aggarwal@in.pwc.com

pwc.in

Data Classification: DC0

This publication does not constitute professional advice. The information in this publication has been obtained or derived from sources believed by PricewaterhouseCoopers Private Limited (PwCPL) to be reliable but PwCPL does not represent that this information is accurate or complete. Any opinions or estimates contained in this publication represent the judgment of PwCPL at this time and are subject to change without notice. Readers of this publication are advised to seek their own professional advice before taking any course of action or decision, for which they are entirely responsible, based on the contents of this publication. PwCPL neither accepts or assumes any responsibility or liability to any reader of this publication in respect of the information contained within it or for any decisions readers may take or decide not to or fail to take.

© 2015 PricewaterhouseCoopers Private Limited. All rights reserved. In this document, "PwC" refers to PricewaterhouseCoopers Private Limited (a limited liability company in India having Corporate Identity Number or CIN: U74140WB1983PTC036093), which is a member firm of PricewaterhouseCoopers International Limited (PwCIL), each member firm of which is a separate legal entity.

PD-IMS/September2016-7184