

DEFENCE AND SECURITY ALERT

SAARC COUNTRIES: US\$ 20

REST OF THE WORLD: US\$ 25

September 2015

INDIA: ₹ 120

VOLUME 6 ISSUE 12

The First and The Only ISO 9001:2008 Certified Defence and Security Magazine in India



THE ONLY MAGAZINE AVAILABLE ON THE INTRANETS OF IAF, CISF AND BSF



NATIONAL SECURITY



SECURING SMART CITIES

DSATM MISSION

*The power of a King lies in his mighty arms ...
Security of the citizens at peacetime is very important
because State is the only saviour of the men and women
who get affected only because of the negligence of the State.*

— Chanakya



DSA is as much yours, as it is ours!

Even as details are yet to be worked and there's a work in progress, the announcement of an agreement with the NSCN (IM) is the best news that has come from the national security sphere. For a long time there has not been any positive news of this type. And in terms of importance there has not been any news of this level since the short-lived and hurriedly aborted, ceasefire with the Hizbul Mujahideen. That was in the last decade and when it has taken so long to produce good news the scale of the national security drought can be well understood.

Interlocutors worked on the NSCN (IM) agreement over a long period of time and are now in the process of thrashing out the details. Just as the talks proceeded away from the media glare, so should the negotiations over details. There is a lesson in how this agreement has worked out and it holds good for other eagerly awaited talks as well. It will make good political sense and have a crucial national security impact as well, to once again pick up the threads of the ceasefire with the Hizbul Mujahideen. It is important and will send a political message of far reaching impact.

National security is, after all, also about sending political messages. Politics and security are ultimately interlinked. And so for good politics it is vital to have an amiable security environment. The recently aborted NSA level talks with Pakistan are a case in point. Far too much media attention and posturing through sound bites, made the talks unworkable from the beginning. That is a pity. It is important to have good neighbourly relations, of course, but that can only come from an element of sincerity. It would be good if Pakistan were to maintain a consistency in their intentions and it would be good if India were to maintain silence in terms of statements. There is a lesson in the Prime Minister's tactics.

It takes every kind of tactic, ultimately, to tackle the biggest national security challenge facing India. In fact there are two 'biggest' challenges facing India, but it is difficult to discern which one is a graver threat. It is impossible to downgrade one to second most important and because they are of such contrasting natures they need equal treatment. One is entirely internal and the other involves international responsibilities of an equally significant nature.

The continuing menace of Naxal violence, or in bureaucratized Left Wing Extremism, eats at the core of Indian statehood. It doesn't challenge the idea of India, or its territorial unity, or even its relations with other countries. What it does is to question the very basis of parliamentary democracy and the functioning of governing structures. It challenges and questions the edifice of governance and the worrisome fact is that it has takers. So many takers that they've got the manpower to hit at security forces for year upon year. Since they don't make the headlines at a regular level, only because the numbers are not spectacular, national attention is spared. But when the annual figures are computed the casualty figures are indeed spectacular and warrant great attention and coordination of strategy.

Strategy of an entirely different type is required to tackle the other equally important national security threat. And that is the continuing spread of the Islamic State menace in India. Because it hasn't hit India with its gore and violence, yet, the country at large hasn't taken it with the seriousness it deserves. But it continues to spread its tentacles, recruit motivated volunteers and nutcases. The very essence of IS is a grave threat to India, on account of its ideology, its contrived and contorted vision on offer. The IS is the biggest global terror threat and India is not immune either. Currently it may be making news because of its activities in Iraq and Syria. But it has the capacity to inflict damage to a larger number of countries, India included. Greater international coordination and participation, is required to take out the threat it poses.

In India's case even more so since the very basis of IS recruitment undermines the core national ethos and cultural harmony. IS feeds on disharmony and when that happens the first casualty is certain to be urban peace. When the future of Indian planning revolves around smart cities, securing them will have to get priority. Tackling the IS threat is fundamental to securing India's future smart cities.

Manvendra Singh

Chairman Shyam Sunder
Publisher and CEO Pawan Agrawal
President Urvashi J Agrawal
Director Shishir Bhushan

Editor-in-chief Manvendra Singh
Corporate consultant KJ Singh

Corporate communication
 Mamta Jain
 Natasha

Sales
 Anup Kumar Sinha

Creative
 Sashisekhar Mishra

Representative (Europe and Americas)

Jo S Birring

Representative (J&K)

Salil Sharma

Correspondent (Europe)

Dominika Cosic

Production

Dilshad and Dabeer

Webmaster

Sundar Rawat

IT operations

Pradeep Ahalawat

Photographer

Subhash

Circulation and distribution

Ashok Gupta

E-mail: (first name)@dsalert.org

info: info@dsalert.org

articles: articles@dsalert.org

subscription: subscription@dsalert.org

online edition: online@dsalert.org

advertisement: advt@dsalert.org

Editorial and corporate office

Prabhat Prakashan Tower

4/19 Asaf Ali Road

New Delhi-110002 (India)

+91-011-23243999, 23287999, 9958382999

info@dsalert.org | www.dsalert.org

Disclaimer

All rights reserved. Reproduction and translation in any language in whole or in part by any means without permission from Defence and Security Alert is prohibited. Opinions expressed are those of the individual writers and do not necessarily reflect those of the publisher and/or editors. All disputes are subject to jurisdiction of Delhi Courts.

Defence and Security Alert is printed, published and owned by Pawan Agrawal and printed at Graphic World, 1686, Kucha Dakhini Rai, Darya Ganj, New Delhi-110002 and published at 4/19 Asaf Ali Road, New Delhi (India). Editor: Manvendra Singh



INTEGRITY IN NATIONAL SECURITY

In the absence of a documented National Security Doctrine, we the citizens tend to interpret the elephant of SECURITY according to our own diverse perceptions. Worse still, we either ignore or fail to recognise the threats posed by external enemies and internal turbulence. Without prevarication, the national objective since Independence has always been a desire for peaceful

coexistence with our neighbours and a cohesive amicability in the diversity of India with the noble intention of fostering growth and development while strengthening our rightful place among the comity of nations.

We have a plethora of Security institutions under the command of Central and State governments to deal with external threats and internal disturbances respectively. They are growing by the day, albeit haphazardly and erratically, in post *ipso facto* recognition of a growing and present danger. But the vexatious questions continue to hang on our heads like the proverbial sword ... Are the Indian borders impregnable and inviolable? Are the citizens safe? Are our women and children safe?

The threats and challenges confronting India have intimidatingly multiplied in the past two decades. This has not happened overnight! Negligence at the Centre and State government levels has been paramount. Be it the politicians in power or the bureaucrats who formulate and execute the Security policy. National Security has never been taken seriously and earnestly, resulting in the alarmingly precarious situations of Naxal prone States, the daily assaults in Jammu and Kashmir and the unacceptable circumstances of Northeastern States. These threats have started percolating to the adjoining States too; which is depressingly frightening.

It is the responsibility of the Nation State to educate its citizens about Security and how to manage it. It should involve the citizens, especially the women of the country to create awareness and propagate the importance of National Security among their families and workplaces and inspire men and young minds against being victims of any security threat. I believe that along with the government and security Agencies, each individual can also play an important role in National Security by being AWARE and ALERT.

Why is it that most of the times each individual thinks only about his/her security?

Is it not possible to convert this 'I' into 'WE'?!!

It does not suffice to say: "All is well by the grace of God". I think we need to be more realistic and pragmatic in our approach to National Security. It is high time that we stop cribbing and grumbling for the challenges of a peaceful existence and start educating ourselves on how we can identify common threats and start working to counter them.

With this edition, **DSA** completes six years of its existence! Team **DSA** is committed to the momentous objective of creating awareness and empowering our citizens along with policy and decision-makers to be more aware and alert about the security of our nation. This edition highlights the many facets of National Security and analyses important aspects and policies for Securing Smart Cities, which is the dream project of our Prime Minister. Our quest to publish thought provoking content and hard hitting facts on topics of defence and security continues unabated. We solicit your comments and critique.

Jai Hind!



Pawan Agrawal

ANNOUNCES OCTOBER 2015 ISSUE

A NEW DAWN FOR INDIAN DEFENCE AND SECURITY

EXPANSION, RESTRUCTURING AND MODERNISATION

CONTENTS

ARTICLES

SEPTEMBER
2015



Sneak Peek	3
Inimical Neighbours Prem Shanker Jha	6
Changing Dimensions Of Social Security V Balachandran	10
Border Security Force Role And Challenges	14
Future Cop Humane - Tech-savvy - Lethal Prakash Singh IPS (Retd)	16
Know The Chief CISF	19
Central Industrial Security Force Role And Challenges	20
Naga Insurgency At Crossroads Col Shailendra Arya	22
Each City Is Different Brig (Dr) BK Khanna (Retd) Nina Khanna	27
Counterfeit Currency And Money Laundering BV Kumar IRS (Retd)	31

Central Reserve Police Force Role And Challenges	34
Security Challenges Of Smart Cities Satyajit Mohanty IPS	37
Aviation Security Sharda Prasad IPS (Retd)	42
Indo Tibetan Border Police Role And Challenges	45
Global Best Practices Smart And Secure Cities KPM Das	48
Cyber Security Of Digital India Dr Muktesh Chander IPS	52
Indian Coast Guard Coastal Security	56
National Disaster Response Force Role And Challenges	59
Vulnerabilities Galore Cecil Victor	62
Sashastra Seema Bal Role And Challenges	64
Get Connected	67



INIMICAL NEIGHBOURS

Pakistan can now be relied upon to continue stoking the disaffection in Kashmir in the confident belief that the Kashmir police and Indian state's disproportionate response will continue pushing the state closer to a new uprising. India will not relinquish control of Kashmir and, under the Doval doctrine of 'offensive defence' will be increasingly tempted to launch conventional military strikes across the LoC or international border.

In retrospect it is easy to see why former foreign minister, Yashwant Sinha, one of the architects of the Islamabad declaration of 2004 that began the long rapprochement with Pakistan that ended in the Delhi framework agreement between Dr Manmohan Singh and President Pervez Musharraf in 2005, condemned the forthcoming meeting between Ajit Doval and Sartaj Aziz, the national security advisers to Prime ministers Modi and Nawaz Sharif as a huge mistake.

This is Islamabad's revenge for Modi's abrupt, last minute cancellation of the Foreign Secretaries' meeting when it did not agree to cancel the Pakistan High Commissioners' meeting with the Hurriyat leaders before he left for Islamabad, for India's '10 for 1' disproportionate response to Pakistani firing across the Line of Control and the numerous belligerent statements made then by BJP ministers in the central government.

Pakistan has flung the gauntlet in India's face because it believes it has nothing to lose from doing so. What is not as easy to understand is how

Prime Minister Narendra Modi did not foresee that Pakistan would use the occasion to avenge itself for the insults New Delhi heaped upon it last year. Did the Foreign office not anticipate this, or was this a product of his overweening belief in his powers of persuasion? In either case it demonstrates that India does not have the faintest inkling of how sharply the balance of power in the region has shifted in favour of Pakistan in the past two years.

Pakistan On Rising Curve

In a nutshell Pakistan has gone from being an international pariah to a valued ally of the major powers once more. As recently as three years ago its foreign debt was close to unmanageable, its relationship with the US was severely strained. In the previous year Washington was using a cut-off in aid and payments to force it to stay in the Afghan War, pushing its economy to the brink of collapse and its relations with Hamid Karzai's government in Afghanistan were openly hostile.

Worst of all, it had enraged its key ally, China, by allowing Uighur terrorists to operate from its soil and was itself being overwhelmed by the terrorists whom it had helped to create. That was when Prime Minister Manmohan Singh's invitation to Prime Minister Yusuf Raza Gilani to attend the cricket world cup semi-final in Mohali, restarted the dialogue that had been broken by the Mumbai terrorist attack and Pakistan turned to India for help.

Today Pakistan's position is almost unimaginably different. With the American withdrawal from Afghanistan substantially over, the principal source of tension between it and the US has all but vanished. Instead the US now has a strong vested interest in showing that its 13-year incursion into Afghanistan has done some good. This will only happen if the Taliban can be dissuaded from launching another civil war and eventually be brought to the conference table. Pakistan is its best bet for both because it harbours two of the key groups of players that can make this happen – the Haqqani Taliban and the Quetta Shura.

Afghanistan's new President, Ashraf Ghani, acknowledged this when he visited Pakistan five months before visiting India, hard on the heels of his visit to China. During that visit he went not to the President's palace in Islamabad first but to the military headquarters in Rawalpindi to initiate an agreement in which Afghanistan will deny sanctuary to the Tehrik-e-Taliban and Pakistan in return will deny it to the Haqqani Taliban. Ghani has followed this up with an agreement to let Pakistan train the Afghan National Army. Clearly both moves have the US' blessing, because it too has committed itself to giving Pakistan US\$1.5 billion a year in economic and military aid provided the Pentagon certifies, every few months, that it is doing enough to curb the Haqqani Taliban.

Pakistan's foreign exchange shortage has also been dramatically reduced by the European Union which has increased its trade preference to Pakistan from GSTP – under which 20 per cent of imports from Pakistan enter duty free – to GSTP plus, which increases it to 100 per cent. This has increased Pakistan's exports to the EU by more than a billion dollars in 2014 and promises to increase them still more.

But all of this has been dwarfed by China's US\$ 46 billion commitment to build 17,000 MW of power plants, mostly nuclear and a bullet train-cum-super highway in the Karakoram to Gwadar economic corridor. Not only will the investment transform Pakistan's economy, but the transit fees it will earn from Chinese goods flowing down the corridor to the Indian Ocean will make it self-sufficient in foreign exchange for all time to come.

Rationale For Entente Cordiale Gone

The economic weakness and political isolation that had made Pakistan briefly reach out to India in 2011-14, has therefore vanished. Pakistan's establishment believes

that it no longer needs India for anything for it has supplanted India in Afghanistan; it has duty-free access to the EU, a market that dwarfs India and will soon be an essential transit link in a north-south trade that will not only give China a vital stake in ensuring its security, but also enable it to extract foreign exchange revenues from transit fees that will make what it might have earned from India's trade with Central Asia look like 'peanuts'.

The plain truth is that when this corridor is ready it is India and not Pakistan that will be isolated from the global economy to the west, as its poor relations with Bangladesh and China and have isolated it from the east. So Pakistan does not need to make any concessions to India on terrorism and Kashmir. Instead,

most, if not all, of the policy makers in that country must secretly be thanking Modi for making it so easy to resile from Gen Musharraf's acceptance of the inviolability of the Line of Control.

Pakistan also had no need to discuss either Kashmir or terrorism because everything in Kashmir Valley is moving Pakistan's way. In recent weeks it has become apparent that a new wave of violent militancy is developing in Kashmir. This burst into view when what was obviously a recruiting photograph appeared on Facebook at the end of June, of 11 young, armed militants in army uniforms in an apple orchard, somewhere in south Kashmir.

Dangers For India

The new movement is still small: Government estimates put its cadre strength at 86 at June-end. But this is by deliberate choice. The new militants are a different breed from those of the 1990s. They are far better educated, Internet savvy and use Viber and other encrypted Voice Over Internet Protocols to communicate with each other and with Pakistan. Their numbers are small because they only recruit boys who are willing to die for their cause. New recruits have to either snatch a rifle from a security force member, or kill a government official in order to be accepted.

Despite the growing frequency of rifle snatching and assassination in the valley in the past four years New Delhi has continued to insist that militancy has been crushed in Kashmir and that the present resurgence is confined to a tiny minority being



Prem Shankar Jha

The writer has been Editor of *The Economic Times*, *The Financial Express* and *The Hindustan Times*. He was the Information Adviser to VP Singh, former prime minister of India. He has authored many books and has been visiting Professor of the Indian Institute of Management, Kolkata; visiting Fellow of Nuffield College, Oxford; visiting Fellow of the Centre for International Studies, Harvard University and is the first holder of the Chair on India's economy at Sciences-Po, in Paris.

Pakistan has gone from being an international pariah to a valued ally of the major powers



orchestrated by Pakistan to keep the Kashmir issue alive. But this myth was finally exploded when it learned that Naved, the Pakistani terrorist captured alive at Udhampur on August 5 after he and a companion ambushed an army vehicle, had spent two months in south Kashmir without anyone having reported their presence to the authorities. This could not have happened without widespread, even if tacit, support for them among the people they came into contact with.

That support exists among the youth. Evidence gathered over the past four years by journalists writing for Kashmiri and national newspapers points towards one and only one, cause. This is unrelenting tyranny and oppression by a police force that no one is holding responsible for its actions.

Under the pretext of gathering information police regularly terrorise stone pelters and former militants long after they have finished serving their time in jail. For these young people life has become an uncertain hell and peace elusive. They and their families live in a constant state of anxiety for they never know when there will be a knock on the door, a peremptory summons to the police station, prolonged 'third degree' interrogation and a violent beating.

Kashmiri Helplessness

This total lack of accountability of their government to them is a constant reminder to Kashmiris of their powerlessness. It explains why more and more of the new batch of militants are well educated and come from good families. For they belong to precisely the strata of society, accustomed to self-respect, who are unable to bear the humiliation.

New Delhi has been indirectly responsible for its return. When, despite the return of curfew raj, police firing and wholesale arrests after the Amarnath land scam in 2008, 52 per cent of the valley turned out to vote in the December elections, the UPA government bugled to the world that the militancy in Kashmir that had led to the 1989 insurgency had died out. What is worse, it began to believe its own propaganda. The immediate result of this was a profound change of perception in Delhi. Kashmir was no longer a political problem to be solved as had been the Naga, the Garo-Khasi, the Mizo, the Khalistan and the ULFA problems, through dialogue, negotiation and compromise, but through a sole reliance on the coercive apparatus of the state. Delhi, in short, stopped talking to the Hurriyat and handed over the entire 'mopping up operations' to its intelligence Agencies and the Kashmir police. Counter-insurgency became a simple law and order problem to be left to the state government, the 'Agencies' and the police.

The belief that militancy had been defeated also made it unnecessary to humanise crowd control. That is what led to the deaths of more than a hundred stone pelters in 2010 and the police reign of terror that has given birth to the new militancy. But Delhi did not stop there and deliberately chose to rub their total political disempowerment into

the faces of Kashmiri ethno-nationalists (who are overwhelmingly young), by hanging Afzal Guru, when it could have so easily left him in jail for life. The pointless vindictiveness of this act, has combined with relentless police terror, to convince more and more Kashmiri youth that their only way to political empowerment is through the gun.

The Modi Faux Pas

The Modi government inherited this situation but, for ideological reasons, has bought into the myth even more ardently than the UPA. This has worsened the situation in Kashmir in four ways: First, by abruptly terminating the dialogue of Hurriyat with Pakistan's High Commissioner it discredited the credentials of the moderate separatist groups and especially the Hurriyat (M), as peacemakers between Pakistan and India. What little Modi left undone was completed by Former R&AW chief AS Dulat's revelation that India had been paying many Hurriyat leaders to keep their parties functioning.

Second, Modi first inveigled Mufti to form a coalition government with the BJP and then watched silently while the hawks in his party forced his government to go back upon every single promise it had made to the PDP in their Agenda for Alliance. This destroyed the political part of Mufti Sayeed's programme to restart the political process by first applying a healing touch in Kashmir and then re-engaging Pakistan via the Hurriyat (M) in a resumed search for peace.

Not content with that he has allowed his government to destroy Mufti's economic programme as well by withholding funds from Kashmir. In fact, whether intentionally or not, he has become party to a crude form of blackmail by first going to Srinagar and promising the Kashmiris ₹ 70,000 crore of grants and loans and then releasing only ₹ 4,000 crore as a ways and means advance in the first six months of Mufti's government.

By staying in office and hoping for the best Mufti is daily reinforcing the fear planted in the Kashmiris when he assumed power, that he has become a willing accomplice in opening the way to the 'saffronisation of the valley'. This is completing the discrediting of not only the PDP but all mainstream democratic politics as well.

Joy For Pakistan

To the newly confident Pakistan, all this has come as a gift from the Almighty. The possibility that a coalition of a Hindu and a Muslim political party could work harmoniously in Jammu and Kashmir had threatened to undermine not only its claim to Kashmir, but also the *raison d'etre* of Pakistan itself. This had made it imperative to ensure that it failed. New Delhi has made its task all too easy.

Lastly, and most tragically, the overtly communal agenda of the now RSS-controlled BJP in the rest of India, has begun to undermine the faith of 190 million Indian Muslims in their future. They

were able to cope with crude attacks upon them like 'Love-Jihad' and 'Ghar wapsi' because these were rejected by the Hindu masses among whom they lived. But they have no defence against the insidious abuse of the law, the police and the judicial process by the central and BJP-ruled state governments to victimise not only Muslims, but staunch defenders of secularism and civic liberties who have stood up on their behalf. Today they are taking note of every discriminatory or vindictive application from the hanging of Yakub Memon, to the alleged attempt by the National Intelligence Agency to make its lawyers to 'go soft' on the accused in the Malegaon, Ajmer and Samjhauta Express bomb blasts; to the systematic victimisation of Teesta Setalvad and her husband, Javed Anand and a string of other less publicised abuses and beginning to fear that they no longer enjoy the protection of the state.

This perception is percolating into the youth of Kashmir as well. Recent protests in the valley have ceased to target India and are targeting the RSS. The fear of resurgent Hindu communalism has finally begun to bring about the merger of radical separatists and radical ie Salafi Islamists that the older generation of Kashmiris and the Shia community in particular, have been warning against for the last decade.

Vanishing Kashmiriyat

In June a grass roots worker of the PDP, who hails from the most disaffected area in south Kashmir, explained exactly what is happening: "you must not forget that 65 per cent of the population is below 35. They are strangers to peace. They have not known the Pandits and have therefore never experienced Kashmiri syncretism. For them Kashmir is a Muslim country and, increasingly, the only Islam they respect is Salafi Islam. They see Salafis winning battle after battle, gaining territory, pushing back the West.

"They see that the Salafi mosques in Kashmir are far richer, their imams far more politically literate, their books far more current. By contrast the sufi ziyarats are poor, their imams know little of world affairs and there is nothing to read. So they go to pray and congregate at the salafi mosques. Today Sufi-Reshi Islam is dying, for it survives only in the older generation of Kashmiris".

The danger in this drift, of a conflict with Pakistan that could easily turn nuclear should be apparent to all. Pakistan can now be relied upon to continue stoking the disaffection in Kashmir in the confident belief that the Kashmir police and Indian state's disproportionate response will continue pushing the state closer to a new uprising. India will not relinquish control of Kashmir and, under the Doval doctrine of 'offensive defence' will be increasingly tempted to launch conventional military strikes across the LoC or international border. The answer Pakistan has prepared for this contingency, according to Gen Khalid Siddiqi, its recently retired head of nuclear forces, is the battlefield mini-nuke and its newest extremely short range, quick reponse missile, the *Nasr*. From there, as Siddiqi does not seem to understand, the escalation to an all-out nuclear attack on each other will be instantaneous. Fom then in four to five minutes both India and Pakistan and this writer and all his readers, will be history. **DA**

The escalation to an all-out nuclear attack on each other will be instantaneous





CHANGING DIMENSIONS OF SOCIAL SECURITY

World famous Swiss-French architect Le Corbusier had planned the layout of Chandigarh on invitation from Jawaharlal Nehru. The quality of life of its inhabitants was the prime concern for Nehru at that time. It is the same for the ‘smart city’ proponents too. To this end Le Corbusier made self-sufficient neighbourhood units placed along the curvilinear roads with cluster type housing, markets and centrally located open spaces. This ensured that inhabitants did not have to drive long for work, schooling or for shopping. There were no slums, power cuts or water shortage in that city when this writer first visited in 1960. Presently all these urban problems are endemic there because of poor city administration and large influx of outside population. There is almost 100 per cent possibility that the same fate may befall on the new ‘smart cities’ too.

P rime Minister Modi’s announcement in June 2014 had given an impression that the Central Government would build one hundred totally new ‘smart cities’. He said: “If we have to generate employment and change for the better, we plan to build 100 smart cities”. The PM was speaking at a function to release a book *Getting India*

Back on Track – An Action Agenda for Reform edited by Bibek Debroy, Ashley Tellis and Reece Trevor published by Carnegie Endowment for International Peace. He said: “Cities in the past were built on river-banks. They are now built along highways. But in future, they will be built based on availability of optical fibre networks and next-generation infrastructure”.

In due course this impression changed. In September 2014 it was announced that eight cities with more than four million people were identified and they would have a satellite smart city. ₹ 1000 crore were allotted for each city which would be selected according to its population. 45 cities with one to four million people would be upgraded to a smart city. 17 capital cities also qualified, irrespective of their population. There would be at least 10 other smart cities with tourist and religious significance. Frankly nothing was clear from this announcement.

Union Urban Development Ministry later identified several basic elements of the proposed smart cities: High quality utility services like water and power, a robust transport system with emphasis on public transport, employment opportunities, facilities for entertainment, safety and security of inhabitants, state-of-the-art health centres and with latest technology for energy efficiency, water conservation and garbage disposal including recycling.

European And Chinese Experiences

A European Union study (March 2014) on 15 Smart cities in China and an equal number in Europe begins with an explanation on what is meant by a ‘smart city’. This information is especially necessary in India where there is a mistaken impression that such a city would be elitist like the newly developed high end pleasure resorts like ‘Ambi Valley’ or ‘Lavasa’ which are exclusively used by more educated and technically savvy people. The Study said that there was no standard definition of what constituted a ‘Smart City’. A common denominator is that the city would push ‘the quality of resource management and service provision to the limit possible’. Also smart city projects are part of a general concept of city modernisation. It cautions against too much emphasis on the benefits of Information and Communication Technology (ICT) since ‘smart city projects should never be seen in isolation, but as one element in a city’s (or a region’s) continuous effort to find the next best way of operations’. It is not merely a showpiece of technology projects alone. In short, faced with the continued urbanisation and increased population density, the lead aim should be the ‘quality of life’ and how far technology can assist in achieving this aim.

Retrofitting Existing Cities

The study also dealt with the problems of developing existing cities into ‘smart cities’ or in some cases building them afresh:

- Existing cities with historically grown infrastructure and administration systems would require a more moderate step-by-step approach to modernisation. The analysis revealed that 3 of the 15 cities examined in China were new areas while almost all of the European cities were ‘add-ons’ to the old cities like Amsterdam, Barcelona, Frankfurt, Lyon, Bristol etc.
- Most smart city projects are actually addressing the implementation of individual solutions to

individual problems identified in a community rather than comprehensive overhauls of the way cities are managed.

- Large-scale integrated city resource management is a task almost exclusively limited to newly developed Greenfield projects.

- It was found that adding new services like parking guidance systems, introduction of electric buses or bike-sharing schemes to an already existing city with its own way of working would not interfere too much with the existing city management procedures. But upgrading a vital part of the infrastructure to the next generation technology like smart metering for water or electricity use would be a very complex task. This would mean something akin to an open-heart surgery on a city’s infrastructure, with the task of upgrading the system without disrupting the present essential services or their billing system.

- Adding smart cities to these old cities should take account of their ageing infrastructure, their operations and also long established city management procedures.

The study also pinpointed the following ‘Services challenges’ while building and running smart cities:

- Traffic systems which use data from sensors should proactively reroute traffic to avoid congestion and maximise road utilisation.
- Better grid technology to enable end users to be more efficient with their energy uses and which allows utility companies to proactively identify and repair energy or water leakage.
- Public safety and security systems to measure real-time movement of public to alert police or transport networks.
- Better health solutions which remotely monitor chronically ill patients so they could remain longer at home and reduce the pressure on limited resources of public hospitals.
- Better learning solutions such as virtual classrooms and new learning environments which would improve student outcomes, increase efficiency, enhance safety and security.

Management Challenges

This in turn would involve the following management challenges:

- EU cities have adopted a more open approach to city governance by a system of government, private sector and the public coming together in partnership which would empower the citizens to be more involved



V Balachandran

The writer is a former Special Secretary of the Cabinet Secretariat. He was also a part of the high level committee appointed by the Maharashtra government to enquire into Mumbai 26/11 terror attacks. He is a prolific writer on intelligence, terrorism and insurgency issues and has also given lectures on these subjects at several institutions in India and abroad.



in the development of their city's modernisation and smart city plans. On the other hand, the Chinese model is a 'Top Down' administration representing their own style of governance.

- Most smart cities have set up 'Integrated Management Structures' for close coordination between all the different departments involved in the development and management of such cities. This has helped faster and more accountable decision-making. On the other hand the Chinese have set up formal leadership structures with senior officials (eg Mayors, Vice Mayors etc) responsible for the overall delivery of the smart city programme.
- Many pilot smart cities have already developed and published Key Performance Indicators (KPIs) to meet international standards.
- Most European cities have implemented open data infrastructure projects, which enable businesses and citizens free access to city data. The Chinese are developing such a system.

Observations on the progress achieved and what more could be done.

- **Engagement with stakeholders:** Most cities had enlisted the cooperation of citizen task groups, industry, technologists, academia, research institutes, social innovators, environmental groups, entrepreneurs and urban designers. However, they had failed to engage with other important stakeholders such as retailers, financial institutions and investors. A smart city initiative created without the involvement of these key stakeholders may result in not receiving sufficient support and investment for the project.
- **Cross-culture dialogue:** Problems arise when city leaders simultaneously talk to small-scale, informal communities as well as to large-scale, formal institutions as their cultures are different, they use different languages and they are often focused on very different objectives.
- **Excluding segments based on socio-economic factors:** Most city projects engage with citizens via mobile applications (apps) that require access to smart devices. This policy excludes low income individuals, less educated groups, the elderly and others in need who do not have such devices or who do not know how to use them. Hence offline provision has to be made for city services.
- **Financing a smart city project remains a major problem:** Most of these cities use a mixture of government and private (corporate) funding. The Chinese projects in Tianjin, Chengdu and Qianhai have received foreign funding. This in turn will force the smart city managers to communicate the progress of such projects and day-to-day management issues to these investors. This however may dilute the autonomy of city managers and result in demands from investors that right business models should be put in place to ensure they are able to generate sufficient return on their investments. Also rating

Agencies might insist on doing their own assessments on the city finances. A number of Chinese local government financing vehicles (LGFVs) were downgraded resulting in problems for some smart cities. A corruption-free administration would be insisted upon.

The Indian Plans

Reports released on August 1 indicated that several state capitals like Lucknow, Mumbai and Raipur 'have made it to the smart city list' while Patna, Kolkata and Bengaluru have not been included among the 100 future 'Smart Cities'. Union Urban Development officials said that a number of factors like better capability for implementing projects and generating their own resources were considered for this selection. It was said that in the first phase, 20 cities would be selected and in the next two years 40 cities would be chosen. All these will receive ₹ 500 crore as central funding over the next 5 years.

Security Challenges

It is not that we had not built such 'smart cities' earlier. The only difference is that we did not call them so. World famous Swiss-French architect Le Corbusier had planned the layout of Chandigarh on invitation from Jawaharlal Nehru. The quality of life of its inhabitants was the prime concern for Nehru at that time. It is the same for the 'smart city' proponents too. To this end Le Corbusier made self-sufficient neighbourhood units placed along the curvilinear roads with cluster type housing, markets and centrally located open spaces. This ensured that inhabitants did not have to drive long for work, schooling or for shopping. There were no slums, power cuts or water shortage in that city when this writer first visited in 1960. Presently all these urban problems are endemic there because of poor city administration and large influx of outside population. There is almost 100 per cent possibility that the same fate may befall on the new smart cities too. Thus developmental security problems would loom large as our smart cities are being developed:


- The same security problems now faced by mother cities like Mumbai, Delhi or Lucknow would bedevil the new smart cities since these are 'Brownfield' projects and not 'Greenfield' or 'start up' plans where one could have planned better security arrangements from the beginning. These problems are unregulated urban sprawl, migration, crime, inadequate transport, traffic congestion, inadequate water supply, mounting garbage, corruption and a host of urban problems which are not adequately solved now.
- Being 'add-on' of major cities, these new clusters would suffer from the same lack of security for the common man and senior citizens since the police have to look after the high personages in government, politics, business or film world on priority. The common man will receive the lowest priority.

- Most municipalities in major Indian cities are unmanageable entities often riddled with corruption and partisan politics with no links with common people. Municipalities like Mumbai have no real administrative autonomy since the Municipal Commissioner is more answerable to the State government than to the Mayor. As an example one may cite the sudden change over of the Marine Drive street lighting. Early this year the BJP government decided to replace the yellow street lights (which had earned the road its name 'Queen's Necklace') with LED white lighting on the ground that the power consumption would be low. No prior consultation with the public or municipal council was done. The ruling Shiv Sena party in the corporation and the Heritage Committee were not consulted. There were public complaints that the LED lights were not adequate for traffic safety as there were dark patches. Even the High Court wanted the old yellow lights to be brought back. However even in August this has not been done by the Municipal Commissioner.
- The building, roads and water supply departments in most municipalities are notoriously corrupt. Employees often extort money from new building projects or even from repair contractors. False muster rolls of contractual employees are prepared to steal government money. All these routinely affect the infrastructure of the city, making the citizens face more danger and hardship. Since the 'smart cities' will be under the same management, there will be no change in their quality of lives, despite that being the prime aim of these new projects.
- Since the smart cities are add-on projects the same shortage of policemen will continue to affect their security. Since the police are under State government, they have to follow the narrow political priorities fixed by the State government. During the earlier Congress-NCP government in Maharashtra state the then Home Minister had made a priority of 'Moral Policing' to watch ladies' dance bars. All police stations had to leave other policing work and patrol during the night to check dance bars. Similarly the present BJP government has made beef imports and sale as their priority necessitating overwhelming efforts by the police in detecting such cases.
- The new smart cities will need heavy investment, which is not possible to be raised even by most state governments, leave alone the municipalities. The Central assistance of ₹ 500 crore over 5 years will not be enough to develop the 'add-on' portion of the city to satisfy the global bench-mark for being called a 'Smart City'. Hence they have to go for heavy corporate or multinational investment. This in turn will necessitate sharing the management responsibility or rights of inspections with them which will not be to the liking of the local political classes. Political agitation over this issue cannot be ruled out.

- Hedged by the financial constraints and to satisfy the corporate or foreign investors, there may even be a possibility that the local governments /corporations might agree to the new areas designated as 'smart city' as an exclusive area like the colonial 'Civil Lines' where ordinary people would not be admitted. This will lead to serious political agitations.
- In India the police have to tackle the end results arising out of faulty town, road or highway planning, increase in unauthorised colonies, faulty emergency relief measures and a host of other infrastructural deficiencies.

Case Studies

A couple of years ago the Eastern Freeway over the Mumbai Port Trust land was constructed. It certainly reduced the driving distance from South Mumbai to North Mumbai. But this narrow freeway is a security nightmare for major road accidents or possible hostage situations since there is no corridor or emergency exit routes for life saving or for mounting counter terrorist or rescue operations. When this was pointed out to these bodies who constructed it, an arrogant reply was received that they were not legally bound to consult the police. However when the crunch comes, everything is left to the police. During 26/11 the police had to take over the responsibility of even failed civic services in Mumbai. Ambulance services failed while fire engines ran out of water. Police vehicles had to be used to ferry the injured to hospitals and also as escorts for fire engines trying to replenish their water. The same situation might happen if the police are not consulted during the planning and construction of smart cities.

Finally a case study done by foreign and Indian media on 'Dholera' 'smart city' in Gujarat is not encouraging. 'Dholera' was to be a massive Greenfield 'smart city' project and a global manufacturing and trading hub. The case study also reflects some problems mentioned in the EU-China study. A *Business Standard* (Feb 9, 2013) report said that Hindustan Construction Company (HCC) had to forfeit its deposit for not being able to complete some parts of the 'Dholera' project. A very discouraging report in *The Guardian* of UK titled 'India's Smart City Craze - big, green and doomed from the start?' (17 April 2014) said that the area was prone to seasonal flooding. It said: "Indeed, the proposals for 'Dholera' have sparked several protests. A grassroots movement for land rights called Jameen Adhikar Andolan Gujarat (JAAG) has been at the forefront: organising peaceful demonstrations against 'Dholera' and other 'smart cities' with farmers, activists and opposition leaders across the region." It also said that some of the major investors have backed out. The same thing was reported in a CNN report dated July 18, 2014. It is only hoped that this will not be the fate of our 100 'smart cities'. 



ROLE AND CHALLENGES

Raised on 01 December 1965, the Border Security Force is one of the most versatile forces capable of functioning in diverse terrain and climate both in times of war and peace. The world's largest border guarding force, BSF has been entrusted with the responsibility of guarding almost 2,300 km of the Indo-Pak Border on the west and the entire 4,096 km of the Indo-Bangladesh border on the eastern side. BSF is also tasked and committed to tackle the menace of transborder smuggling of narcotics, contraband and weapons besides checking of infiltration of terrorists and influx of migrants on the border at all times. Further, BSF has also been assigned the task of anti-Naxal operations, maintaining peace and law and order during agitations, elections and pilgrimages like the annual *Amarnath Yatra* etc.

In performance of their multi-faceted duties under hostile and tough conditions the officers and men of the BSF have faced all challenges head-on and have gallantly made supreme sacrifices to maintain peace in the country and to uphold the sanctity of the nation's borders. The force is in a constant endeavour to evolve and

face the ever changing hues of myriad challenges in the assigned tasks.

Border guarding is the primary mandate of the BSF. Secure borders always are a prerequisite to safe and secure hinterland. The India-Pakistan border stretches over a length of 3,074 km running along the states of Gujarat, Rajasthan, Punjab and J&K. The border has distinct geographical and physical features depending on the state it passes through. The snow laden mountains, vast salt and sand deserts, the meandering rivulets with overgrowth of elephant grass at times defeat technology and men. In spite of the ever vigilant first wall of defence, the anti-national forces are at times able to creep in and wreak havoc in the country. The 4,096 km Indo-Bangladesh border running through the states of West Bengal, Assam, Meghalaya, Mizoram and Tripura has its own peculiar challenges. Several insurgent groups operating in India seek shelter in dense forest in Bangladesh. Infiltration of illegal immigrants from the east is another formidable problem. Smuggling of narcotics poses a major irritant on the western front through Punjab, Rajasthan

and Gujarat borders. The quantum of narcotics smuggling is relatively low through the Rajasthan and Gujarat borders but is a major cause of worry on the Punjab border. Fake currency also at times enters the country through some parts of the borders that are porous.

When the BSF was set up in 1965, it was assigned two major roles, one pertaining to peacetime and the other during war. In peacetime, the BSF is required to 'police' the border. In the event of the transborder situation hotting up, leading to a war, the Army would move to the border and the BSF would assist the Army. Peacetime duties performed by the BSF, independent of the Army and other Agencies, gives it a major responsibility and opportunity to ensure national security. This is so because transborder activities prompted and inspired by some of our neighbours to disintegrate India, seriously jeopardise national security. Apart from this and what often seems to escape notice is the responsibility given to the BSF to safeguard the security of the border population. The BSF plays this role without intruding into the responsibility of the State Administration of the area concerned. It is in the light of these considerations that the BSF was also assigned special responsibilities in regard to assisting the State authorities in dealing with internal security situations in border areas.

The canvas on the border and areas close by is fragile. Along with the responsibilities involving vigilant and constant watch on movement of individuals across the borders illegal immigration of individuals or groups, the BSF also safeguards agricultural operations in the border areas. To discharge the duties effectively, the BSF has to remain sensitive to human rights of people and constitutional mandate of the states.

Augmentation of the strength of the border guarding force, the creation of border infrastructure coupled with technological supplements have paid rich dividends in improving the security of our borders. BSF has always kept pace with developments in the fields of information technology. The national security challenges always pose a serious threat to the sovereign stability of the country. Borders are vibrant with activities most of which are inimical to the interests of the country. Incidents on the borders have national and international ramifications and have to be handled professionally and with maturity. The bordermen are being provided with the latest in equipment and personal armour. The organisation today has a futuristic look, strategy and approach to deal with issues at hand. Threat perceptions are constantly analysed. The force today stands tall at the borders. **DSA**

FUTURE COP

HUMANE – TECH-SAVVY – LETHAL

The internal security of the country faces great challenges from terrorists, both domestic as well as transnational. These terrorists are not only interested in perpetuating individual incidents – their objective and target is to destroy India as a whole. That is why they have been targeting institutions and cities which symbolise the strength and diversity of the country. They target Delhi because it is the political capital of the country; they create mayhem in Mumbai because that is the commercial centre of the country; they perpetrate incidents in Bangalore because that is the IT hub of the country; they cause explosions in Ayodhya and Varanasi with a view to sharpening the communal divide.

The country is facing multiple challenges on different fronts. The Maoists have spread their network over vast areas of Central India. The secessionist elements in Jammu and Kashmir continue to pose a threat to the integrity of the country. In the northeast, there are several insurgent groups disturbing law and order in the different states of the region. Illegal migrations from Bangladesh have upset the demographic balance in several states. Organised criminal syndicates of drug traffickers, arms smugglers, counterfeit currency

carriers etc, also pose serious threats to the security and economy of the country.

The police needs to be overhauled and reorganised to deal with the plethora of problems confronting the country. Unfortunately, we are still saddled with the colonial legacy. There have been several attempts at reform. The National Police Commission submitted a comprehensive report in eight volumes during the period 1979 to 1981. Soli Sorabjee drafted a Model Police Act. The Supreme Court gave elaborate directions to the state governments and the central

government for police reforms on Sep 22, 2006. Seventeen states passed legislation purportedly in compliance of the Court's directions, but actually to circumvent their implementation. The remaining states passed executive orders but these are also not in keeping with the letter and spirit of Court's directions. The central government defaulted in passing the Model Police Act and has generally been cool to the idea of police reforms.

Control By Vested Interests

The Prime Minister recently came up with the concept of SMART Police. He implied a police which should be Strict and sensitive, Modern and mobile, Alert and accountable, Reliable and responsible, Techno-savvy and trained. It is an unexceptionable concept. But his advisers should have told him that the police just cannot be sensitive unless it is insulated from extraneous influences, that it can be mobile and modern in terms of transport and technology but would never be able to win the confidence of the people unless it is accountable to them rather than to the political masters, as is the arrangement today. The net result is that neither the Court's directions nor the Prime Minister's call for a SMART Police have led to any changes on the ground. On the contrary, the vested interests which want the *status quo* to continue have even taken regressive measures in certain states. In Uttar Pradesh, the executive has been appointing Directors General of Police for short terms ranging from one month to six months, making a mockery of the high institution of Police Chief.

The police has to be reorganised, restructured and rejuvenated to be able to deal with the numerous challenges on the law and order front the country is confronted with. People would have to raise their voice for the change. There will have to be a popular demand to replace the present Rulers' Police with a People's Police. The future cop will have to be versatile – in particular, he must be humane, he must be tech-savvy and he must be lethal.

Being humane and lethal at the same time may, on the face of it, appear contradictory, but at the ground level these traits could co-exist. The police will have to be humane towards the law abiding citizens and lethal while dealing with terrorists and other anti-national elements of different shades.

Humane

One of the major complaints against the police is that its personnel are rude, impolite, abusive, high-handed and that they are harsh even while dealing with the average citizens. As far back as 1902, the Fraser Commission made the following observations:

"The police force is far from efficient; it is defective in training and organisation; it is inadequately supervised; it is generally regarded as corrupt and oppressive; and it has utterly failed to secure the confidence and cordial cooperation of the people."

It is distressing that these comments are valid even today. The Human Rights Watch made the following observations in a Report, India: Broken System, published in 2009:

"A dangerous anachronism, the police have largely failed to evolve from the ruler-supportive, repressive forces they were designed to be under Britain's colonial rule. While sixty years later much of India is in the process of rapid modernisation, the police continue to use their old methods. Instead of policing through public consent and participation, the police use abuse and threats as a primary crime investigation and law enforcement tactic."

The National Police Commission was of the view that "a healthy police-public relationship on a continuing day-to-day basis is vital to secure the desired measure of public involvement and cooperation in police work to make it meaningful and acceptable to society". The image of the future cop will, therefore, have to change from being oppressive to being humane. The police must acquire a people-friendly image. This would require a tremendous amount of in-house effort. The senior police officers will, on the one hand, have to set an example and, at the same time, educate and train their subordinate ranks to behave with the people in a humane, compassionate and understanding manner. The police may have genuine problem in recording a report immediately, but they could always be sympathetic to the complainant and give him/her a patient hearing meanwhile. They may or may not be able to work out a case, but they could always give the impression of having done their best to work it out. These changes would go a long way in winning the confidence of the people.

The police would have to be particularly careful to uphold the human rights of scheduled castes/tribes, women and minorities and the poor people of all denominations.

Tech-savvy

Events are moving very fast and the law breaker is equipped with the latest gadgets and the most modern equipment. That being the scenario, police will have to catch-up with them in technology. The future cop will have to be tech-savvy; he must be computer-literate and conversant with the different forms of cyber-crime. It is a great pity that in most of the states, the police station looks like a law enforcement unit of Aurangzeb's time. The munshi (clerk) sits on the floor with a desk in front of him and uses carbon to make multiple copies of a document. He should be able to print the complaints on a desktop and use a printer for getting as many copies as he needs. Computerisation in police has been slow compared



Prakash Singh IPS (Retd)

The writer, a recipient of Padma Shree, was formerly Director General of BSF and also DGP Uttar Pradesh and DGP Assam. He was also Member, National Security Advisory Board.



to the progress made in some other departments like the Railways or the Income Tax.

Police specialisation in cyber-crime is a must in the present context. Criminals are exploiting the speed, convenience and anonymity of the Internet to commit a range of criminal activities across the international borders. These crimes broadly fall into three categories: attacks against computer hardware and software like malware and network intrusion; financial crime and corruption such as online fraud and phishing; and abuse in the form of 'sexploitation', especially crimes against children. New trends in cyber-crime are emerging all the time, with costs to the global economy running into billions of dollars. According to a recent study by the ASSOCHAM-Mahindra, the number of cyber-crimes in India may touch the humungous figure of 300,000 in 2015, almost double the level of last year causing havoc in the financial space, security establishment and social fabric. What is particularly disturbing is that some of these crimes have originated from foreign countries including China, Pakistan, Bangladesh and Algeria. According to the National Crime Records Bureau (NCRB), in 2013, 681 cyber-crime-related cases were registered in Maharashtra, which meant a 44.6 per cent rise compared to 2012. Andhra Pradesh with 635 cases registered in 2013 witnessed a 48 per cent rise while Karnataka with 513 cases registered in 2013 saw a 24.5 per cent rise compared to 2012.

All state capitals must have well equipped cyber cells manned by well trained staff, some of which could be inducted from the open market in view of the high level of specialisation called for.

Lethal

The internal security of the country faces great challenges from terrorists, both domestic as well as transnational. These terrorists are not only interested in perpetuating individual incidents – their objective and target is to destroy India as a whole. That is why they have been targeting institutions and cities which symbolise the strength and diversity of the country. They target Delhi because it is the political capital of the country; they create mayhem in Mumbai because that is the commercial centre of the country; they perpetrate incidents in Bangalore because that is the IT hub of the country; they cause explosions in Ayodhya and Varanasi with a view to sharpening the communal divide. Hafeez Mohd Sayeed, the chief of Lashkar-e-Toiba, does not mince his words. In one of his speeches delivered in Lahore, he openly said that they will "not rest until the whole of India is dissolved into Pakistan." Recently, on December 5, 2014, he said that the only way to deal with India was "to adopt the course of Ghaznavi and Ghauri". He also boasted that the Pakistan Government and the Army support his plan for jihad in Jammu and Kashmir. Within the country, Indian Mujahideen has spread its network in different states. SIMI is

also active. Besides, Al Qaeda has set up a unit in India. The Islamic State, which seeks to establish a Caliphate, is also spreading its wings in India. Flags of ISIS are routinely displayed in Srinagar.

The Maoist insurgency also poses a serious threat to the internal security of the country. The northeast has multiple insurgent groups.

The police would have to enhance its capabilities and acquire a lethal punch to deal with these separatist and secessionist elements in different parts of the country, particularly in J&K, the northeast and in Central India. Unfortunately, in a large number of incidents, policemen are at the receiving end. In a dreadful incident in Dantewada (Chhattisgarh), the Maoists were able to kill 75 CRPF personnel in one attack. The Government of India has already advised the states affected by Maoist insurgency to raise units on the pattern of Andhra Greyhounds. Other states are also raising specially trained police forces. Thus, Maharashtra has Force One. Actually, the states need to build the capabilities of their police forces as a whole. They should have good transport, reliable communications and adequate forensic support – apart from modern weapons for the specialised units.

Internal Security Doctrine

The Central Armed Police Forces would also need to upgrade their skills in counter-insurgency and acquire the latest weapons which would be effective against terrorists and insurgents. There has been a gradual deterioration in their potential during the last ten years, partly because of lack of clarity on the part of government in the degree of firmness and aggressiveness to be displayed by the security forces. Government should give a clear mandate to the police and paramilitary personnel that while human rights have to be observed, while innocents must not be harassed, no quarter should be given to those who have taken up arms against the state and are waging war against it. The anti-national elements have to be neutralised and for that the forces on the ground must have lethal capabilities.

It is a great pity that our response to the various challenges confronting the country has been rather supine. We have the armed forces to vanquish the various separatist and secessionist elements and yet we have been mollycoddling them. We need to define our internal security doctrine and thereafter implement that with the required degree of firmness. The police will have to be reformed and reorganised to be able to combat the threats. It will have to be people-friendly, techno-savvy and must acquire the punch to neutralise the anti-social and the anti-national elements. As Aurobindo said, "what India needs especially at this moment are the aggressive virtues, the spirit of soaring idealism, bold creation, fearless resistance, courageous attack". **DA**

The anti-national elements have to be neutralised and for that the forces on the ground must have lethal capabilities

SURENDER SINGH IPS

DIRECTOR GENERAL

CENTRAL INDUSTRIAL SECURITY FORCE



Surender Singh, IPS assumed the charge of Director General, Central Industrial Security Force on 01.05.2015. He is the 25th Director General of CISF

He joined Indian Police Service in 1980 at the age of 24 years and was allotted West Bengal cadre. During his distinguished career spanning 35 years, he has held many important and sensitive positions in the state of West Bengal and on central deputation to Government of India. During the period of 1981 to 1987, he served in various capacities in the Districts of Midnapur, West Dinajpur in West Bengal and Commandant of an Armed Police Battalion in Rajasthan.

In the year 1987, he joined the Intelligence Bureau on central deputation. He served in the Intelligence Bureau in Kohima (Nagaland) and Arunachal Pradesh. He has manned various important desks at IB Headquarters and looked after many sensitive responsibilities like issues related to North Eastern States, Left Wing Extremism

etc. He has also served as First Secretary in the Indian High Commission in Dhaka (Bangladesh). On 31 July 2014, he was promoted to the rank of Special Director in IB (in the rank of Spl DG) and continued to look after various important assignments.

He has attended many prestigious courses/training including Police Command Course (1994), West Yorkshire Police Training School, Wakefield (UK), National Defence College Course (2003) at NDC, New Delhi and India Major Case Management Course (2006) at Washington (USA).

He has been decorated with the Police Medal for Meritorious Service in 2001 and President's Police Medal for Distinguished Service in 2007. **DA**



ROLE AND CHALLENGES

Central Industrial Security Force (CISF) was raised in the year 1969 to protect and safeguard the Public Sector Undertakings. Over a period of time, the CISF has emerged as a specialised force shouldering pivotal responsibility in securing some of the most critical infrastructure of the country in the public/joint/private sector establishments in a befitting manner.

At present CISF is providing security cover to 317 different establishments with 1,45,000 sanctioned strength. CISF is the only Central Armed Police Force, which has a separate Fire Wing providing fire-safety cover to 91 installations.

Today, CISF provides security cover to nuclear installations, space establishments, 59 major airports, seaports, core areas of power, steel, coal, oil etc including security to Delhi Metro, Government Buildings, Heritage Monuments like Taj Mahal and Red Fort. The Special Security Group of CISF provides security to various category Protectees/VIPs. It is evident that this

force has seen exponential growth, both in terms of its strength and responsibilities. CISF has earned the reputation of being a multi-skilled and tech-savvy Central Armed Police Force which is ready to accept any challenge at any given time. The contribution of CISF in internal security of the country and in conduct of free and fair elections has always been praised and recognised. Its dedication, professional competence, adaptability and the use of cutting edge technology have been the hallmark of the force.

CISF is deployed in almost all parts of the country to protect and safeguard the vulnerable and critical infrastructures, sensitive establishments in core sectors which are contributing immensely in our national development. Each establishment is different from others in view of locational vulnerability, threats of various kinds and tough terrain etc. For example seaports, few atomic energy establishments and other installations are located at sea coast. These are exposed to the water fronts and face threat from seaside. Accordingly, CISF

guards the water fronts in our area of responsibility and carry out patrolling by the boats equipped with required weapons and gadgets.

Today, CISF has the largest public interface dealing with lakhs of people throughout the country daily. This is also a challenge before us to deal with the general public with due courtesy and politeness coupled with firmness on security matters. On an average 28 lakh commuters travel in Delhi Metro and 5.1 lakh passengers move through the airports. About 33-34 lakh passengers are travelling daily in the secured environment provided by CISF. The women personnel of the force are also deployed at the places where there is an interface with women passengers/employees etc. CISF women personnel undergo Pre-Commando course soon after the completion of Basic Training and thereafter they are imparted specialised training in martial art which makes them fit and confident to neutralise any opponent in odd hours. In this manner, CISF women personnel instil the sense of security amongst women passengers and employees of establishments.

The diversified role of CISF enriches the capability and adaptability of the force personnel to take on any challenge in any adverse circumstances. Two unique features of the CISF set it apart from other Central Armed Police Forces:

- Firstly, it is cost-reimbursement Force. The entire expenditure of the force is borne by organisations where the force is deployed.
- Secondly, CISF units are organised on a need basis and not on the battalion pattern. This has imbued the CISF with an adaptability that is manifest in its professional response to the demands of the time and it has evolved as a highly professional and tech-savvy Central Armed Police Force.

There are enormous threats and challenges in today's world. The transnational terrorism, Naxalism and anti-national outfits pose a serious threat to the national security besides conventional internal and external threats viz theft/pilferage, white collar crime, sabotage, espionage, subversion etc. This makes the task of CISF more diversified and challenging which requires high order of professionalism and multi-skilled capability. On account of these challenges the mandate of CISF has broadened. CISF is no longer a PSU centric force as responsibility of security in the field of VIP security, Government Building security, Heritage Monuments, Airports, Delhi Metro and sensitive installations etc have also added. Constant technical modernisation, upgradation of gadgets and weaponry, extensive use of dog squads and BDDS, well equipped QRTs, manual and CCTV surveillance, specialised training to the force personnel has enabled the force to stand forth and protect the installations of immense importance in a more secured manner. Operational plans

are constantly and periodically reviewed for different sectors like airports, seaports, atomic energy, space establishments etc. CISF has transformed into a highly professional, premier multi-skilled and tech-savvy security agency to handle and neutralise any kind of challenge in the area of responsibility.

Cyber security will be the daunting challenge in future. CISF as a premier and specialised force, has sensitised the need of protection and security of all digitised data either on flow of networking or stored on server. CISF has charted out its schedule to carry out the Cyber Security Audit of all hardware and networking to ensure fail proof safeguarding of digitised data. Initially, the Cyber Audit of all IT related equipment and functions has been carried out at Central stage. Use of technology as a force multiplier has always been the forte of CISF and constant endeavours are regular process for improvement and upgradation of the technology.

CISF has the potential to expand more in areas of consultancy services in the field of fire, security and cyber security, expansion of fire wing, security of Indian Embassies located abroad and many more left out areas of critical infrastructure of the country contributing immensely in national development.

In view of the present security scenario across the world and future requirements of the force, new methodologies have been adopted in CISF to sharpen the multi-tasking ability of its personnel which is the core capability of the force. These are – One Minute Drill on 10-15 different situations for quick and decisive action in a very short time, Soft Skill Training, Martial Art Training (Pekiti Tirsia kali for Women and Krav Maga for Men), Joint exercises with NSG/other CAPFs and special forces of the state, quality mock drills, capacity building of BDDS teams, workshops, standardisation of electronic gadgets and equipment, new HR policy, new induction norms, qualitative improvement in consultancy services, set-up of cyber security cell etc.

Modernisation process for this tech-savvy force gained momentum soon after the identification and standardisation of equipment/gadgetry with required QRs in different operational sectors with special thrust on proper maintenance facility. **The special focus has been given on optimal use of multi-skilled manpower and sophisticated/modern gadgets with the integration of entire security matrix for the fail proof security.**

CISF has a people friendly approach committed to serve the citizens of our country in letter and spirit. CISF personnel are polite and courteous but firm on security while dealing with the general public. CISF is known as the force of the future for providing protection and security in all fields of economic activity. **DSA**



NAGA INSURGENCY

The Indian Army should not dilute its counter-insurgency operations and the intelligence set-up in the Northeast. At the same time, a political solution needs to be found to the underlying socio-economic causes, good governance insisted upon, infrastructure development speeded up and the political process with the Naga groups be expedited. The funds earmarked by New Delhi must trickle down to the misty hills. Often they do not leave Delhi or Guwahati. A strong political initiative, supplemented with a renewed push by the Army and the Assam Rifles can neutralise NSCN (K). Army can also get ample intelligence inputs from its rival factions, mainly NSCN (IM), which likes to fancy itself as sole representative of Naga people.

The gunfire is again raging in the misty Northeast. The recent abrogation of 14 years old ceasefire by Nationalist Socialist Council of Nagaland-Khaplang (NSCN-K) which had been largely missed by the national media until the deadly ambush on Army on June 4, 2015 has significant security, political and economic ramifications for the Northeast.

But then in a major development, the Centre signed a peace accord with the NSCN (IM) on August 03, 2015, marking a positive turn for India's longest running insurgency. The agreement was signed by chief Indian interlocutor RN Ravi with T Muviah, the general secretary of the powerful and the largest insurgent group – NSCN (IM). Interestingly, the agreement was signed at the Prime Minister's residence and was witnessed by PM Narendra Modi, Home Minister Rajnath Singh and the NSA Ajit Doval. Nineteen top Naga leaders from different Naga organisations and civil society groups were also present. It has been clarified that this pact is a 'framework' for working out a permanent solution to the Naga problem and the exact terms will be finalised over the next three months. The terms of settlement with NSCN (IM) are likely to include greater autonomy for Nagas living in Manipur, Arunachal Pradesh and Assam, disarming of cadres and cultural integration of Nagas across states.

It is likely that the failing health of NSCN (IM)'s chairman Isak Chisi Swu and the urgent need to get NSCN (IM) on board in flushing out NSCN (K) to Myanmar prompted this accord. The reactions have been mixed – the Naga society in general has cautiously welcomed it, the Naga National Council (NNC), now a former shadow of itself and only a fringe player, claimed itself to be guardian of Nagaland, while NSCN (KK), currently observing a ceasefire, stated that it has nothing to do with this peace accord. These reactions were predictable. What is certain is that as the contours of the accord are shaped, the positions on either side of the divide shall harden and NSCN (IM), now backed by accord and a newly-found



legality, shall endeavour to implement it across the Naga inhabited areas and propel itself from the largest player to the sole and legitimate representative of the Nagas. In this process, it shall encounter symbolic opposition from NNC, political manoeuvring with pie-sharing attempts by NSCN (KK) and NSCN (R) and significant armed opposition from NSCN (K).

The recrudescence of violence and the attack on the Army convoy appeared set to jeopardise the tenuous Naga peace process and put a question mark on the ambitious connectivity plans via North East to South East Asia. It threatened the outcome of the 18 months deadline set by the Modi government in

AT CROSSROADS

November 2014 to fast-track a solution to the long-standing Nagaland issue.

Khaplang Group On Offensive

The abrogation of ceasefire was accompanied by attacks on security forces by NSCN (K). On March 21, 2015 a Gorkha Rifles convoy was ambushed in Tamenglong district of Manipur but no casualties were reported. The first major attack took place on April 3, 2015 on the soldiers of 4 Rajput Battalion while they were moving on the Khonsa-Longding road in Arunachal Pradesh's Tirap district bordering Nagaland, leading to the loss of life of three Army personnel. Another attack followed on May 4, 2015

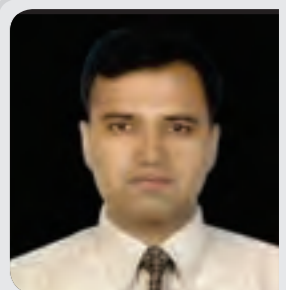
and improvised explosive devices were used. The attack was carried out by NSCN (K) with support of a Meitei insurgent group – the Kanglei Yawol Kanna Lup (KYKL).

Though there has been cooperation in context of arms smuggling, training and logistical support between these two groups, this incident marks the first time there has been a coming together of Naga and Meitei insurgent groups to attack the Indian Army. It may be noted that the Naga and Meitei insurgent groups have competing territorial claims with Nagas claiming large parts of Manipur as 'Greater Nagalim' and the Meiteis insisting on territorial integrity of the existing Manipur. The NSCN (K) is nevertheless supported by CorCom, short for Coordination Committee, an umbrella organisation of six insurgent groups of Manipur created in 2011, reportedly with Chinese encouragement, after a meeting at Ruili in China's Yunnan province.

Apart from sending Naga Hills and the adjoining areas of Arunachal Pradesh and Manipur into another spiral of violence, renewed inter-faction killings and a sad reversal of peace process; these new developments also have the potential to stall the ambitious plans of connectivity via Myanmar that the PM announced on his visit to the Northeast last year. This once again brings the Naga insurgency to crossroads of peace and conflict. The oldest insurgency of India has been there many times earlier and has mostly taken the path of violence. Will this time be different?

NSCN (K) – Back To The Bush

The present deterioration in security situation can be attributed to the continued neglect of Northeast, inability to diplomatically engage with Myanmar to disallow its soil for anti-India activity and the breakdown of ceasefire with NSCN (K). It may be noted that while the ceasefire agreement between the Centre and NSCN (K) was signed in 2001, the two sides are yet to start political dialogue, leading to political frustration in NSCN (K). The NSCN (K) also perceives Centre as favouring its arch-rival NSCN (IM) and was being sidelined. Consequently, on March 27, 2015, NSCN (K) chairman SS Khaplang abrogated the ceasefire saying, "The 14 years of ceasefire between NSCN (K) and New Delhi has become a mockery and futile exercise."



Col Shailender Arya

The writer is an alumnus of RIMC, Dehradun and NDA, Khadakwasla. He has served as GSO 2 of a mountain artillery brigade on the Line of Control, a company commander with Assam Rifles in Nagaland and as a Staff Officer with the United Nations. He is an MSc in Weapon Technology from Poona University and an MSc in Defence and Strategic Studies from Madras University. He has served as a GSO 1 (Operations) of a newly raised AR Sector HQ in a counter-insurgency environment in South Manipur and is now commanding his unit on the Line of Control in J&K.



In April 2012, NSCN (K) had signed another ceasefire with the Myanmar government. It was opposed by all other Naga groups particularly by NSCN (IM) and the NSCN (KK), who said that the NSCN (K) could not function like a transborder group and be allowed to sign ceasefires with two sovereign governments. But the political success with Myanmar allowed SS Khaplang to think that he could outmanoeuvre both the Indian government and NSCN (IM). His strategy was simple – delay political talks with the Indian government and wait for the ongoing New Delhi-NSCN (IM) talks to fail. Being a Burmese Naga, he as such did not have any stake in a political settlement with India.

The agreement with Myanmar government at Hkamti on April 9, 2012 was a success for NSCN (K). It was drafted and signed by two Indian Nagas and Kilonsers (ministers) Wangtin Naga and P Tikhak – both later expelled by SS Khaplang. Shangwang Shangyung Khaplang is a Hemi Burmese Naga and has many shades; he is considered a fatherly figure (called baba) by Naga villagers in Myanmar and in border districts of Nagaland, the NSCN (IM) considers him rather rustic while in the insurgent circles he is considered to be a wily fighter – not technology or media savvy but excellent in the jungle. Incidentally, the 75 years old and ailing Khaplang had been shifted from his base in Tago, located along the China-Myanmar border, to Yangon for medical treatment in the early part of this year.

While NSCN (K) has largely adhered to its ceasefire agreement with Myanmar, it had been violating the ceasefire with India both in letter and spirit. In 2001, it had agreed not to assist any insurgent groups to set up base camps in Myanmar. However, in NSCN (K) dominated areas such as Lahe, Leshi and Nanyun in Sagaing administrative region of Myanmar, the United Liberation Front of Asom (ULFA – Paresh Baruah faction) and the National Democratic Front of Bodoland (NDFB – Songbijit faction) have set up camps to carry out attacks in Assam. Northeastern insurgent groups also have access to training and regrouping camps in Myanmar's Naga Self-Administered Zone, where NSCN (K) has been granted autonomy by the Myanmar government.

This protection of other insurgent groups in Myanmar by NSCN (K) comes with a price – 'protection money' paid to NSCN (K) with its amount varying upon the size of the camp, cadre strength and degree of indulgence in smuggling activities. Recently, the Prime Minister's high-level Task Force on the Northeast also reported that the Khaplang group has been raising funds by providing training and logistics to insurgent groups like ULFA, NDFB, People's Revolutionary Party of Kangleipak and the Kangleipak Communist Party.

Wangtin Naga and P Tikhak, leaders of a new organisation called NSCN (R), have stated that it was at ULFA leader Paresh Baruah's instance that SS Khaplang expelled them from the organisation as kilonsers (ministers) and abrogated the ceasefire deal with New Delhi. According to Tikhak, after being expelled from Bangladesh, Paresh Baruah came to Myanmar and took refuge with

SS Khaplang. They also did not rule out Chinese intervention ie under Chinese influence, Baruah was instrumental in convincing Khaplang to abrogate the ceasefire with India.

The NSCN (K) in any case was not a party to the political process in India and would have been a loser on successful conclusion of negotiations between New Delhi and NSCN (IM). With ceasefire abrogation and sensational attacks on security forces, NSCN (K) hopes to play a spoiler, rally all the anti-talk factions of Northeast and earn money by providing them training, arms and safe sanctuary in the areas under its influence in Myanmar. It can also continue to run its Indian extortion empire with credible threats of violence.

New Alignments

A new anti-India and anti-talk umbrella group has recently emerged in Northeast. This new conglomerate of four militant outfits of Northeast – NSCN (K), ULFA (I), NDFB (S) and Kamatapur Liberation Organisation has been named United Liberation Front of West South East Asia (UNLFW) and was formed in Myanmar in April 2015. The meeting was held in the Sagaing region of Myanmar and was facilitated by Chinese intelligence personnel. This new platform is headed by SS Khaplang, the chairman of NSCN (K).

The NSCN, which was formed in January 30, 1980, was split into the NSCN (Isak-Muivah) and NSCN (Khaplang) in 1988. The NSCN (K) first split in 2010 into a faction led by Khole and Kitovi Zhimomi and this faction was called NSCN (KK). N Kitovi Zhimomi was the then General Secretary and Khole Konyak was the commander-in-chief; both were expelled on the grounds of 'anti-party activities' by SS Khaplang. NSCN (K) has now split again, leading to the formation of another splinter group named NSCN (Reformation) formed by the expelled senior India-based leaders of NSCN (K), Y Wangtin Naga and P Tikhak.

The trigger for expulsion was these two functionaries attending the Ceasefire Supervisory Board meeting at Chumukedima on March 28, 2015 and expressing their desire to extend the ceasefire. Wangtin Naga is a Konyak Naga from Nagaland while P Tikhak is a Tangsa Naga from Arunachal Pradesh. The new outfit NSCN (R) now aims to represent the Indian side of the Nagas as distinct from those living in Myanmar. The Centre has engaged the new breakaway faction NSCN (R) in ceasefire. The agreement was signed by Shambhu Singh, Joint Secretary, MHA and Wangtin Konyak and P Tikhak, co-conveners, on behalf of NSCN (R) in April 2015. In April 2015, the Centre also extended the ceasefire with NSCN (KK) for a period of another one year.

Growing Chinese Influence

The re-emergence of Chinese support for the Northeast insurgents after 25 years of non-interference is a disturbing development. China, apparently alarmed by growing closeness of Myanmar to US and India, is reasserting its influence in this region. Apart from helping Indian insurgents, China has also actively started assisting the United Wa State Army in the hills

of Shan state in Myanmar with sophisticated weaponry that include armoured personnel vehicles. There had also been reports of arms sales by China to NSCN (IM) in return for intelligence on Indian Army. Possibly, by exercising greater influence in Nagaland, China could be aiming to secure a bargaining chip in the deadlocked border negotiation talks between India and China.

According to Wasbir Hussain of the Institute of Peace and Conflict Studies, China holds the key to the availability of weapons and ammunition among the terror groups in Northeast India that is actually keeping insurgency alive in this far-eastern frontier. The first signs of a growing Chinese influence came in 2009 when in April 2009, Isak Chisi Swu, the NSCN (IM) president visited China (the 'I' in IM is for Isak). Soon Paresh Baruah visited China in 2010 and the reports suggest he led a group of 80 ULFA cadres which received training and weapons in Yunnan province. Even today, Baruah is said to be ensconced in Ruili and Kunming, both in Yunnan province of China and in touch with the Chinese PLA officials.

From 2010 onwards there were reports of Chinese nationals facilitating arms procurement by the insurgent groups. In the charge-sheet filed by the National Investigating Agency on March 26, 2011 against Anthony Shimray, chief arms procurer of NSCN (IM), it is stated that Shimray accompanied by a NDFB representative visited the Norinco (China North Industries Corporation) headquarters in Beijing to procure arms. In 2011 and 2012, two major conclaves of Northeastern insurgent leaders were organised by the Chinese at Taga in Western Myanmar, in an area where NSCN (K) has significant influence. The growing Chinese influence is now clearer by the reports of presence of Chinese ex-soldiers and intelligence operatives during the formation of UNLFW in Myanmar.

Possible Solutions

The Indian Army has hit back by cross-border raids on two camps including a camp in the Ponyu area where the NSCN (K)'s 3rd Brigade was based. In end-June 2015, Khumlo Abi Anal, a regional commander of NSCN (K) was also arrested from Chandel district of Manipur. The seizure of military initiative by India and senseless violence by NSCN (K) provides a window of opportunity for India to capitalise on the popular anti-violence sentiment in Nagaland, push NSCN (K) out of the country to Myanmar and sign a meaningful peace agreement with the dominant Naga insurgent group – NSCN (IM), which will then, in absence of NSCN (K), have the capability to implement it over the entire Naga inhabited areas.

The Myanmar Factor

Simultaneously, there is a need to engage Myanmar to expel Indian insurgents operating from its soil. Myanmar has become particularly important as the safe sanctuaries in Bhutan and Bangladesh are no longer available to the insurgents. The Indian insurgents are

not supported by the Myanmar government. It is a 1,640 kilometers long and porous border with shared ethnicity across borders and the poor administrative grip over these regions by Naypyidaw which has led to this situation. Further, most of Myanmar border areas including opposite India are themselves in grip of insurgency with varied ethnic groups mainly Kachins, Karens, Wa, Shan and Chins fighting against a Burman dominated military government. In these complex circumstances, the Indian insurgents obtain sanctuaries in the border areas of Myanmar by paying the poorly paid lower rung of the Myanmar Army (Tatmadaw). A greater incentive in terms of aid and equipment to the Myanmar Army by India shall win them over – both from Indian insurgents as well as from the growing Chinese influence.

Presently, the heavily committed Myanmar Army sees more merit in befriending Nagas rather than combating them. Post the ceasefire agreement with NSCN (K) in April 2012, NSCN (K) has refused to be drawn into any alliance of insurgent groups in Myanmar against the Myanmar Army in spite of the Kachin Independence Army approaching NSCN (K) several times for a coalition. NSCN (K) has also accepted some demands of the Myanmar Army like allowing Naga children to be taught Myanmar in some villages. In addition, the Myanmar Generals are conscious of the rich mineral deposits in the Naga region – these can only be exploited in an ambience of peace and understanding with the NSCN (K). Gold mining takes place quite close to Khaplang's headquarters in Taga where the rebels and the Myanmar Army have stakes.

The Indian Army should not dilute its counter-insurgency operations and the intelligence set-up in the Northeast. At the same time, a political solution needs to be found to the underlying socio-economic causes, good governance insisted upon, infrastructure development speeded up and the political process with the Naga groups be expedited. The funds earmarked by New Delhi must trickle down to the misty hills. Often they do not leave Delhi or Guwahati. A strong political initiative, supplemented with a renewed push by the Army and the Assam Rifles should neutralise NSCN (K). Army shall also get ample intelligence inputs from its rival factions, mainly NSCN (IM), which likes to fancy itself as sole representative of Naga people.

Politically, the NSCN (IM) and the two other recently created factions – NSCN (KK) and NSCN (R) could push NSCN (K) to the sidelines and eventually to Myanmar, rendering it inconsequential in India. According to Chinwang Konyak, the adviser of the Eastern Naga Peoples' Organisation (ENPO), "This is a blessing in disguise as the Khaplang group will be left in Myanmar. Let them deal with the Myanmar government. It is better to part ways with them peacefully." ENPO is a civil organisation with representatives from ethnic groups of Nagaland, Arunachal Pradesh and Myanmar.

While the vacuum after the exit of NSCN (K) shall be filled by other Naga groups, the drifting peace

The Indian Army should not dilute its counter-insurgency operations

process with NSCN (IM) must be taken to its logical conclusion. The gap between what they want – ‘independence (earlier) to special federal relationship (now)’ to what New Delhi can offer ‘greater autonomy or special status’ – is gradually decreasing. The Naga groups must not perceive that the government is not serious and is adopting delaying tactics, somehow hoping that the current Naga leadership shall fade away and a *status quo* type of diffused solution found. After over 70 rounds of talks since 1997, frustration with this interminable peace process is evitable and is growing every day.

The peace talks with NSCN (IM) should also include other stakeholders – the elected state government, the traditional Naga tribal bodies like Naga Hoho and the other factions – NSCN (KK) and NSCN (R). As regards the complex question of ‘Greater Nagalim’, the Prime Minister’s Task Force, led by RN Ravi, chairman of the Joint Intelligence Committee and the PM’s envoy for peace talks with Nagaland insurgents, is likely to recommend a deal that would give Naga tribes living inside Manipur special rights, without changing the existing state boundaries. It already has backing of NSCN (IM) on this plan. This Task Force is also likely to recommend that Army should guard the Indo-Myanmar border.

Future Prospects

The eventual exit of NSCN (K) dominated by Myanmarese Nagas reflects the first ever territorial alignment of the Naga tribes in consonance with the international border between India and Myanmar rather than on a common Naga identity – the root cause of the vexed ‘Greater Nagaland’ demand which includes parts of Myanmar. As the demand for integration of all Naga inhabited areas gives way to the demand for greater political autonomy and cultural unity for the Nagas, a solution must now be found to the simmering Naga insurgency. Presently, there is an exceptional situation wherein there is an elected state government but not a party to the peace talks, the extortion empire of NSCN (IM) is flourishing amidst an uneasy ceasefire and the Nagas themselves are getting increasingly fed up with the inter-faction clashes and illegal ‘taxes’ imposed by insurgent groups.

The Northeast deserves attention and development. The lack of opportunities is fuelling alienation and insurgencies. Unimplemented accords, ceasefire abrogation or new factions always incite violence. There was widespread violence in aftermath of 1975 Shillong Accord, the NSCN split in 1988 was accompanied by massacres and the gun-battles raged when NSCN (KK) was created in 2010. Today, the drifting peace process and increased factionalisation of Naga groups could lead to renewed conflict unless the ‘mother insurgency’ of Northeast is addressed – both politically and militarily. From this crossroad of peace and conflict, the correct turn for the Naga insurgency is critical for the entire Northeast and India. **DA**



EACH CITY IS DIFFERENT

There is a myth among certain decision-makers that similar model of Smart Cities in Western countries can be applied to cities in India too. But the fact is that no two cities are similar and hence innovation plays a big role in developing each Smart City. Besides Indian cities have inadequate infrastructure *vis-a-vis* population, unplanned colonies, poor general awareness about impact of natural and man-made disasters and inadequate preparedness by first responders.

As the global population continues to grow at a steady pace, more and more people are moving to cities every single day. Experts predict that 75 per cent of the world population will live in urban areas by 2050 – which means we are adding the equivalent of seven New Delhi cities to planet earth every year. Urbanisation accompanies economic development. Countries are urbanised as they move from agrarian economies to industrial and service sectors. Urban areas generally provide agglomerations that industrial and service sectors require. Approximately 80 per cent of the global gross domestic product (GDP) is attributed to cities. On negative side, cities consume 60 per cent of world’s energy and US\$ 100 billion was spent on Information and Communications Technology (ICT) in the year 2014. As per the High Powered Committee Report on infrastructure, submitted to Union Urban Development Ministry in 2011, urban explosion is taking place in India too with number of cities/towns growing up from

5,161 in 2001 to 7,935 in 2011. Urban population is expected to increase from about 350 million in 2011 to 600 million in 2031, from 50 metropolitan cities in 2011 to 87 by 2031.

Need For Smart Cities In India

The alarming growth of urban population has raised concerns over support system these cities can offer. Cities are stretched to the limit, struggling to provide basic urban services, viz cities have started experiencing socio-economic challenges of resource scarcity, unemployment and inadequate housing. Traffic congestion and pollution continue to increase as overcrowding has become endemic. There is a



Brig (Dr) BK Khanna SM, VSM (Retd)

The writer is former Founder Senior Consultant (Training and Capacity Development) with National Disaster Management Authority (NDMA), Government of India.



Nina Khanna

The co-writer is Research Scholar in Manav Rachna International University, Faridabad.

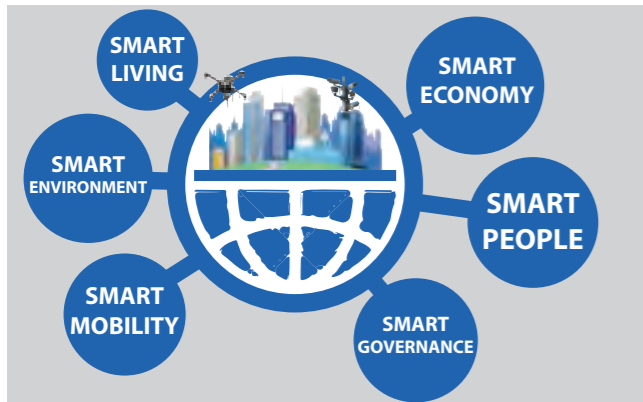




growing demand for innovative strategies across the economy for Government to provide smart governance to its citizens, by addressing local challenges affecting the citizens in their daily lives for the purpose of 'building trust in society and solving complex problems'. With an urban population of 31 per cent, India is at a point of transition where the pace of urbanisation is likely to speed up. It is for this reason that India needs to plan its urban areas well and earlier it is done, better it would be in the long run. Moreover, it also offers an opportunity to create a conducive environment for creation of employment opportunities and economic activities while improving quality of life. It allows an opportunity to learn from good practices and mistakes made elsewhere in the world while developing smart cities. It is in this context that the Government of India decided to develop 100 Smart Cities in the country. Accordingly, in Budget Speech of July, 2014, the Finance Minister stated, "As the fruits of development reach an increasingly large number of people, pace of migration from rural areas to cities is increasing. A neo middle class is emerging which has aspiration of better living standards. Unless, new cities are developed to accommodate burgeoning number of people, the existing cities would soon become unlivable. The Prime Minister has a vision of developing 'one hundred Smart Cities', as satellite towns of larger cities and by modernising existing mid-sized cities."

Smart City Concept

The Smart City concept can be looked at as a framework for implementing a vision of modern urbanisation which envisages achievement of four goals – social equitability, economic viability, safe and secure environment and environmental sustainability. Social equitability is based on principle of inclusion; there is no discrimination in access to benefits across population segments. Economically viable solutions are those that are financially self-sustaining. Safe and secure environment makes the citizens feel safe from all types of perceived threats and disasters. Environmental sustainability ensures preservation of environment for future generations. Smart City is one that has got digital technology embedded across all city functions, is equipped with basic infrastructure to give a decent quality of life and clean and liveable environment to live smarter. Besides Smart City information and communication



technologies provide better quality and performance thus engage more effectively with its citizens. Smart City ingredients are given below:

What Is A Smart City?

Smart City as per Business Directory is, "A developed urban area that creates sustainable economic development and high quality of life by excelling in multiple key areas, economy, mobility, environment, people, living and government. Excelling in these key areas can be done through strong



human capital, social capital and/or ICT infrastructure." Sectors that have been developing Smart City technology include Government services, transport and traffic management, energy, health care, water and waste management. Smart city applications are developed with a goal of improving the management of urban flow and allowing for real time responses to challenges. A Smart City therefore will be more prepared to respond to challenges than one with a simple transactional relationship with its citizens.

Securing Smart Cities

Concept of a Smart City is very topical and many organisations around the world are working on intelligent solutions to make urban areas energy efficient, comfortable, environmentally friendly and safe. Far fewer are thinking of cyber security of Smart Cities. The more IT is involved in creation and operation of a Smart City, greater is the potential risk. If not addressed early on, cost and complexity of creating a Smart City could make it far more difficult to address security problems further down the line. Securing Smart City involves solving cyber problems at every stage of a Smart City development from planning through to actual implementation of smart technology. Smart City projects cannot just be smart but they need to be safe. "Cyber security of a modern smart city is not something that one can solve on his own. The concept involves so many different technologies communicating with each other in so many ways, that only way to predict and eliminate all possible security issues is through collaboration between experts around the world. This is what securing Smart City is all for," said Caesar Cerrude, CTO for 10Active.

Some Examples

There are a number of good practices in Smart Cities around the world. It is not possible to list all of them. One example of how building management can be calibrated to work in response to local micro-climates and maintain occupant comfort is found in the California Academy of Sciences in San Francisco, which takes advantage of natural air currents in surrounding Golden Gate Park to regulate the indoor temperature. Windows and skylights are designed to open and close automatically, controlled by an automated ventilation system. As heat rises through the building during the day, skylights will open to allow hot air out from top of the building, while louvers below draw in cool air at lower floors. This provides an energy efficient and cooling flow of air during hot weather that can operate independently without the need for conventional energy intensive air conditioning systems and chemical coolants. Similarly, while developing Smart Cities in Germany, France, Canada, Netherlands, Austria, UK and USA, smart metering infrastructure, transport management and accident avoidance, e-governance, smart street lighting, CCTV cameras, central control room and quick response teams etc have been adopted.

Requisites For Smart Indian City

After taking into consideration the good practices world over for building resilience, following requisites have been identified for Securing Smart Cities in India against natural and man-made disasters:

- Advanced information gathering system for providing early warning on perceived disasters with last mile connectivity.
- State-of-the-art Control Room with monitoring system.
- Response teams with modern arms and equipment and high level of training.
- Advance analysing data on super computers for providing cyber security and to detect crimes.
- Smart street lighting with low consumption energy technology.
- Smart Traffic Management System.
- GPRS for solid waste management.
- Online Water quality monitoring.
- GIS for property tax.
- Online building plan approvals and birth, death, marriage and caste certificates.
- Smart meters.
- Self-sustenance for at least 24 hours, before the first responders can arrive at disaster site, as they may themselves be affected by a major disaster and will take time to respond.
- Selection of safe places/houses and safe evacuation.

Major Initiatives By Government

Current Initiatives

Ministry of Urban Development has undertaken several initiatives to promote Smart City concept. These include:

- Promoting transit-oriented development.
- Land use planning.

- Street-lighting.
- Intelligent traffic management.
- Deploying technologies for e-governance.
- Ministries/departments and municipalities are also funding smart initiatives.
- In addition, compendium of best practices/smart initiatives is available in the public domain.

Future Initiatives

- Need to develop viable financial models with defined revenue stream (to make projects bankable).
- JNNURM II to act as a catalyst.
- PPP is the way forward.
- For developing 100 Smart Cities, an investment of ₹ 7 lakh crore is required over a period of 20 years with annual budget for this coming to ₹ 35,000 crore. Government has allocated 7,060 crore for the year 2014-2015 for Smart City Project.

Other Initiatives By States

- Multi-modal transport system in Lucknow, Ahmedabad, Delhi and Gurgaon.
- Panaji converted into a vehicle free city.
- Better surveillance system in Delhi, Bengaluru and Noida.

Pay Heed To USP Of City

There is a myth among certain decision-makers that similar model of Smart Cities in Western countries can be applied to cities in India too. But fact is that no two cities are similar and hence innovation plays



a big role in developing each Smart City. Besides Indian cities have inadequate infrastructure vis-a-vis population, unplanned colonies, poor general awareness about impact of natural and man-made disasters and inadequate preparedness by first responders. It may be mentioned that there are certain drivers of a Smart City value chain from quality of life to sustainability through growth, which are listed below:

Quality of Life	Growth	Sustainability
<ul style="list-style-type: none"> ● Safe ● Diverse ● Leisure ● Convenience 	<ul style="list-style-type: none"> ● Knowledge ● Innovation ● Employment ● Investment 	<ul style="list-style-type: none"> ● Carbon neutral ● Clean air and water

Market Drivers

Besides, market drivers which promote development of Smart Cities are given below:

- **Decongestion:** Provision of BRT routes, metro, cluster buses, tolls for multi-modal transport.
- **Safety:** City surveillance, availability of cyber forensic labs etc.
- **Citizen Convenience:** Aadhar linked services (UID scheme), smart grids, waste disposal.

Key Recommendations

- The process of master planning needs to be aligned with digital planning.
- Smart Cities in Indian conditions should be developed as satellite townships to existing cities/towns.
- Technology needs to be deployed to improve service delivery in sectors such as public transport, health, education, security and disaster management etc.
- Land value monetisation is a significant factor for determining financial viability of any Smart City development.
- Cost of technology deployment must decline as its usage increases.
- While planning Smart Cities, check vulnerability of area to various types of natural and man-made disasters. Buildings/infrastructure as per the seismic zone, water harvesting, power back-up and parking inside the complex should be planned. Sufficient gaps should be kept between buildings, keeping into account fall of buildings.
- Check BIS code for the seismic zone, before drawing up town plan. Take on-board Disaster Management expert, besides others.
- Smart City should have inbuilt resilience to perceived disasters.
- Set up state-of-the-art City Disaster Management Operations Centre. It should be manned in 24x7 mode, redundancy in communication and close coordination should exist between police, ambulance services, hospital and fire services. The city should have its own rescue, first aid and security teams from among the community.
- Early warning system should be put in place for warning community with last mile connectivity, through sirens, SMSs, mobiles, emails, landline telephones, through religious places and loudhailers.
- Contingency and DM Plan should be formulated by analysing hazard, risk and vulnerability, resource mapping and selecting and training disaster management teams.
- There should be self-sufficiency in fire fighting for dousing small fires. Hand-held emergency equipment like combo cutter and expander, saws, air lifting bag and inflatable lighting tower should be kept at city level.

Government of India has taken a defining step in developing 100 Smart Cities over a period of 20 years. It has also earmarked token amount to declare its commitment. For such a huge project to fructify, it needs investment from private sector as well. While India is on threshold to become a developed country, simultaneously the Smart Cities must also come up for giving it authenticity and sustainability. **DA**



COUNTERFEIT CURRENCY AND MONEY LAUNDERING

Organised criminal groups, adopt the same *modus operandi* followed by major smuggling syndicates in setting up a rigid hierarchy network to minimise the risks to their criminal enterprise with the result that the prospect of most of the enforcement Agencies in apprehending the top management is minimal. The organised criminal groups involved in currency counterfeiting insulate their leadership from direct involvement in the operations through an intricate organisational structure.

The first international legal instrument dealing with counterfeit currency is the International Convention for the Suppression of Counterfeiting Currency signed at Geneva on 20.4.1929 (CCC 1929). The most prominent and commonly known cases are 'Operation Bernhard' in World War II when Germany tried to destroy the British economy by counterfeiting huge amounts of British pounds. In another prominent case Hungary tried to destabilise the economy of France as an act of revenge after having lost huge parts of its territories in the Peace Treaty of Versailles in 1919, after World War I. The political involvement of Hungary was of such a

magnitude that the international community established the CCC, 1929. This convention is a specific legal, international and binding instrument for fighting against currency counterfeiting. The UN Convention against Transnational Organised Crime was adopted by the General Assembly on 15.11.2000 is one of the main international legally binding instruments in the fight against cross-border organised crime.



BV Kumar IRS (Retd)

The writer was Director General (Revenue Intelligence) and Director General, Narcotics Control Bureau, government of India. During the Interpol Conference held at Nice in November 1987, he was elected as President of the Drugs Committee which is one of the most important Committees of Interpol. Visiting Lecturer at National Defence College, New Delhi and National Police Academy, Hyderabad. He has co-authored a book *The Narcotic Drugs & Psychotropic Substances Laws of India* and authored *The Preventive Detention Laws of India*.





Currency counterfeiting can have a high impact on the political and economic system of a country and may destabilise the very foundations of a sovereign country. The involvement of organised crime and terrorist groups in intensive currency counterfeiting for financing their activity at low cost can pose a serious threat to national and global security.

Counterfeit And Hawala Currency

The Financial Action Task Force (FATF) in its report of June 2013, quoting the report of UNODC (2012) observed that ‘Currency counterfeiting and money laundering have the potential to destabilise the national economies and threaten global security as they are key ways in which terrorists and other criminals finance their activities and conceal their profits.’

K Subrahmanyam, in the Chapter on ‘External Security’, in India Vision 2025 (Planning Commission, 2003) wrote that the flow of fake currency into India, where cash transactions dominate at ground level and black money constitutes a significant proportion of the economy, the infusion of fake currency presents two kinds of threats. Firstly to our economy, secondly the fake currency enables the adversary to obtain the services of individuals and groups to act against our security interests at very low cost to themselves. Once such conduits are established they are used to push in drugs, explosives, weapons and trained terrorists.

In February 2014, the Finance Minister of India informed the *Rajya Sabha* that counterfeit Indian currency notes worth ₹ 107.33 crore (US\$ 17 million approximately) had been seized between January 2010 and June 2013.

Fake Notes From Pakistan

Fake Indian Currency Notes (FICNs) printed in Pakistan are smuggled into India through couriers via Bangkok, Kathmandu and Dhaka airports. According to reports of Indian Intelligence Agencies, organised crime syndicates push FICNs through China, Malaysia, the UAE, Denmark, Netherlands, Singapore and Sri Lanka.

The Research and Analysis Wing (R&AW), the Intelligence Bureau (IB) and the Directorate of Revenue Intelligence (DRI), informed Parliament’s Standing Committee on Finance that fake banknotes of mostly ₹ 500 and ₹ 1000 denominations are printed in Pakistan and circulated in India by the ISI through the underworld and terror operatives. The Committee was informed about the involvement of Pakistan in the manufacture and supply of FICNs for financing terrorist activity in India. They were further informed that several terrorists owing allegiance to groups such as Lashkar-e-Toiba (LeT), Al Badr, HuJI, Hizbul Mujahideen (HM) and the crime syndicate of Dawood Ibrahim, were found carrying fake rupee notes at the time of their arrest. Terrorists who were arrested in Delhi confirmed that the Kashmir based militant groups have been running FICNs Operations with

Pakistan’s Connivance. The attack on the Indian Institute of Science, Bangalore in December 2005 and November 2008 as well as the Mumbai terror attacks were financed by counterfeit currency and or money sent through hawala operations. This was revealed by Abdul Karim Tunda, an LeT operative who stated that Pakistan’s Intelligence agency, ISI runs the entire supply chain of FICNs and gave the names of other persons involved in these operations (*The Hindu*, August 21, 2013). He further confessed that he has been moving FICNs to fund terrorism in India through his contacts. The Indian Mujahideen (IM) also raises funds through hawala transactions and circulation of FICNs in the country. IM’s India Operations Chief Yasin Bhatkal was arrested by the STF in Kolkata in 2009 for carrying fake Indian currency notes (*The Times of India*, August 29, 2013).

High Quality Print Technology

A detailed forensic analysis by the NIA has revealed that the notes have been printed on highly sophisticated machines involving huge capital investment and the paper used to print the

counterfeit notes matches with the legal tender of Pakistan. The Parliamentary panel was informed that the volume of FICNs smuggled into India in 2010 was between ₹ 1,500 and ₹ 1,700 crore, which went up to ₹ 2,500 crore in 2012. Over the last three years the volumes would have doubled if not tripled and indications are that though the checks have been intensified at the traditional routes, the flow of counterfeit currency has not slowed down. The Indian Intelligence Agencies have found that most of the FICNs in circulation are reportedly printed in Government-controlled printing presses at Karachi, Multan, Quetta, Lahore and Peshawar in Pakistan and the ISI has a major role in these operations.

Investigations into past terrorist activities and confessions made by terrorists apprehended during such operations have confirmed the fact that state and non-state actors in Pakistan are solely responsible for printing and smuggling FICNs through various channels to foment terrorism and criminal activities in India. Further, it was revealed that large scale funding for Kashmir-centric Hizbul Mujahideen comes from FICNs cartels based in Pakistan.

Criminal Nexus

Organised criminal groups, adopt the same *modus operandi* followed by major smuggling syndicates in setting up a rigid hierarchy network to minimise the risks to their criminal enterprise with the result that the prospect of most of the enforcement Agencies in apprehending the top management is minimal. The organised criminal groups involved in currency counterfeiting insulate their leadership from direct involvement in the operations through an intricate organisational structure. They employ their trusted confidants for recruiting landing agents, transport agents and setting up safe storage places and distribution networks. The structure of these groups is characterised by rigorous internal discipline to insulate the network at each level, so that the top management is too remote and faceless for the law enforcement Agencies to identify, let alone apprehend them.

At the distributional level, the persons and places are carefully identified, so that there are maximum cash transactions where the inflow and outflow of cash is high such as theatres, retail stores, casinos, bars, exhibitions etc where the FICNs get

Studies on currency counterfeiting indicate that organised criminal groups operating transnationally are heavily involved in the business of currency counterfeiting on a global scale with strong links with other forms of criminal activity such as drug trafficking and arms smuggling. It is well-documented that huge quantities of high quality FICNs are being infused into the financial system of India by Pakistan to lower the value of the currency, trigger inflation and erode the faith of the people in their currency and if possible to destabilise the whole economy.

Legislative Backing

The Mumbai High Court (in October 2012) held that mere possession and circulation of fake currency cannot be termed as an act of terror under the provisions of the Unlawful Activities (Prevention) Act, even if it is printed in a foreign country, while granting bail to one Dhiren Ghosh arrested in 2009, by the Maharashtra Anti-terrorism Squad for alleged possession of counterfeit notes. Parliament passed the Unlawful Activities (Prevention) Amendment Act, 2012, (which came into force from 1.2.2013) making the circulation of counterfeit notes either

by individuals or a group or an association as a ‘terrorist act’. The amendment broadens the scope of the ‘terrorist act’ by incorporating threats to economic security and the monetary stability of India by way of production, smuggling or circulating high quality counterfeit currency. The law increases the period of declaration of an association as unlawful from two years to five years, criminalises high quality counterfeiting and includes within its scope offences by companies, societies or trusts and provides punishment. In January 2014, a special National Investigating Agency Court gave a life term to six convicts in a 2009 FICNs case, including Dhiren Ghosh, Nooruddin Bari, Mohammed Samad and Aizul Shaikh and convicted them under Sec 16 and 18 of the Unlawful Activities (Prevention) Act and Sec 489 of the IPC on 29th January 2014 (*PTI* January 2014).

In the International Narcotics Control Strategy Report (2011), the US Department of State observed that “India (also) faces an increasing inflow of high quality counterfeit currency, which is produced primarily in Pakistan but smuggled to India through multiple international routes. Criminal networks exchange counterfeit currency for genuine notes which not only facilitate money laundering but also represent a threat to the Indian economy.”

It must be mentioned that so far the nature, intensity and character of currency counterfeiting and its nexus in financing terrorism has not received the attention that should be given to this form of serious crime by the law enforcement Agencies and Financial Intelligence Units. Further, close Co-operation is required between these two and their counterparts in other jurisdictions to effectively combat this scourge. **USA**



Fake Indian Currency Notes printed in Pakistan are smuggled into India

Trafficking in counterfeit currency is closely and inextricably linked with money laundering



ROLE AND CHALLENGES

It has become almost clichéd to state that the challenges will last forever for Security Forces – such are the intelligence leads on the internal threats that the country is staring at. But the biggest challenge for the Forces like CRPF is to operate on such half-baked intelligence reports and tackle militancy head on when the system is indecisive about what ends have to be achieved. The intelligence machinery of the Force has to rise to a high tactical level with capability and assets available to the smallest fighting formation.

Early on 27th July morning, on the 76th Raising Day of CRPF, there was a wake-up call to inform that militants had attacked and seized Dinanagar police station in the Gurdaspur district of Punjab. The militants had killed seven persons and injured fifteen in the attack. The whole drama seized the nation's attention for the whole day through live feeds on national media. The question on everybody's mind was whether militancy in Punjab which was so alarming in 80s and 90s of the last century, was really finished? CRPF's contribution in eliminating the militancy was laudable.

Mystery Of Security In The Northeast

Only a few weeks ago, on 4th June in the Chandel district of Manipur – a place which has always been

admired for its serene beauty, the lush green hills and the colourful festivals – had blood and bullets all around its green canvas when in an ambush 18 soldiers were killed and 16 injured. This was one of the biggest losses for the Army in the last two decades. Horrified and stunned people are still thinking: Is it breach of trust or crack in the elusive peace process. Is it a single stray incident or revival of bloodshed in the region? The peace process that is being nurtured by everyone with care and caution has taken a toll. Tranquillity, which is so much part of nature in northeastern states of India, seems to be making noises again and again for wrong reasons. The primitive mindset of a few people is fuelling the fire for implementation of Inner Line Permit system in Manipur. Protests paralysed the capital city of Imphal for days and as usual a few precious lives were lost and the limbs of many severed forever. But does anybody care?

Stray Incidents Or Latest Trends

These two incidents are not stray ones. In fact, these are the new challenges to national security. The trends of emerging threats are unpredictable and sometimes the challenge pops up from the corner which has hitherto been considered contained and controlled.

The challenges for CRPF are not going to be softened either in Left Wing Extremism affected areas of Central India or in the Kashmir Valley. On the contrary, the problems seem to be erupting in Punjab and northeastern states especially in Manipur and Nagaland. At the same time the pressure on the State Police in maintaining law and order will spillover to the CRPF and it will have to play a critical role in riot control, crowd management, holding of even *Panchayat* elections besides the *Lok Sabha* and State Assembly elections. The dissatisfaction of people with governance is also being increasingly reflected in massive protests often paralysing the day-to-day affairs of the common man. These issues will become more problematic because of political absurdities of protests even by ruling parties and local governments. Further, tweets of merely a few words are quite often seen sparking volatile situations necessitating prompt actions and intervention of CRPF.

Punjab And Cross-border Terrorism

The situation in Punjab is very complicated and peculiar. The militant groups have signalled start of fresh acts of terror and Pakistan is willing to assist them as much as are the jihadi groups including Kashmiri militants. The state is also facing one of the ugliest phases of widespread drug-addition amongst youth. The economic dynamics has led not only to prosperity but also made them prone to various abuses and social vices – a very conducive situation for rise of militancy again and other anti-national subversive activities. The threat from across the border is also an issue owing to the geopolitical strategy which Pakistani Army has formulated. Under the existing scheme of things, even sabotaging the peace initiatives of their own political masters is a game plan which often results in bloodbath across the borders. This obviously increases the role of CRPF in professionally tackling it.

Half-baked Intelligence

It has become almost clichéd to state that the challenges will last forever for Security Forces – such are the intelligence leads on the internal threats that the country is staring at. But the biggest challenge for the Forces like CRPF is to operate on such half-baked intelligence reports and tackle militancy head on when the system is indecisive about what ends have to be achieved. The intelligence machinery of the Force has to rise to a high tactical level with capability and assets available to the smallest fighting formation. To appreciate security environment and embrace the changes is indispensable in the present day scenario. The collection and creation of data base and analysis should result in productive operational efforts. Building-up intelligence base in the Force is obviously a challenge in a country so diverse in thoughts, actions and expectations.

Emerging Contours

With the focus of citizens on their own rights, securing peace is becoming a challenge to governance. Good policing is integral to this process. And in most of the

states off late policing is highly dependent on the CRPF. This dependence will further increase in future as state governments want to play safe as far as police actions are concerned lest they lose their political patronages.

The CRPF being mandated for management of internal security has onerous task of anticipating, assessing and acting on all kinds of threats. Internal security has become a complex and a multi-agency function. From border-management to local eruption of violence over petty issues are becoming matters of grave concern. It is not only about protecting physically but now virtual space too needs to be monitored and protected. Cyber space to prayer houses all need to be sanitised and secure. The multitude of issues demands technological advancements and commitments. Thus, the challenges before the CRPF are to dynamically evolve to meet the stakeholder's interest and secure peace within the country. This has huge cost implications as well.

Resource Mobilisation

The CRPF would be facing the issue of resource constraints also in its modernisation attempt to secure the nation. The infrastructural augmentation of the organisation is essential for prospective planning and meeting expectations. Capacity building of the Force will remain the 'core' area which requires focus and upgradation. The relevance of Forces trained in counter-insurgency operations with adequately equipped intelligence mechanism is imperative in present context to ensure peace.

Threats To Cities

The trends in national security indicate that the CRPF has to be in counter-insurgency operational mode even while performing law and order duties at so-called peaceful locations. The incidents of Ayodhya, Akshardham and the Sarojini Nagar blasts etc all are indicators as to how challenging it has become for Forces to manage terror attacks across the nation. The very concept of assessing vulnerable spots is just not enough anymore, especially when terrorists are zeroing in on the gaps in security at many places in the country.

Kashmir Militancy

The Kashmir militancy will not subside till the attitude of promoting cross-border terrorism by the Pakistani Army does not change. The internal dynamics of various groups within the valley also needs to be addressed. The CRPF has so far been able to control the situation to a great extent which may need further reinforcement in the coming days. *Fidayeen* attacks and blasts on the rail tracks and roads have always been a threat against which preparedness cannot be eased. Rather, it may call for more involvement in terms of manpower and technology. On 27th July 2015, while carrying out attack on a police station, the militants also planted bombs on the railway tracks at five places simultaneously. Thus, securing rails and roads again are of prime concern. The nation cannot afford threats to such infrastructural lifelines if it has to be ushered into a developed nation.

Left Wing Extremism

Assessment of information available indicates that there is likelihood of spike in violence graph in



Left Wing Extremism affected areas and may result in a situation where more troops may be deployed. About ten thousand armed cadres organised on military pattern and supported by *Dalams* and *Sanghams* continue to pose dreadful challenges for Security Forces. Their tactics of use of mines and improvised explosive devices imaginatively compensates its lack of automated weaponry, though, now even the weapon profile of the Maoists has improved. The Left Wing Extremists will attempt to maintain a level of violence threshold to challenge governments' authority in demonstrative ways. With the expressed ideology of use of violence combined with the tough terrain of the area of their influence will remain a tactical challenge in coming decades.

Improved Explosive Devices

Improved Explosive Devices (IEDs) are likely to pose serious challenges to CRPF in all the theatres. The preemptive preparations and tactical planning seems to be the only plausible solution to counter it. For this, two-pronged strategy of enhancing technological capabilities and developing tactical skills are the need of the hour. The tactical evolution of Forces has to be more than the anti-social element's disruptive tricks. So in the coming days, training a huge number of force personnel is also a major challenge which stares at the Force right in its face. Training such a huge number would require trainers of calibre and adequate resources.

Security Of Vital Assets And VIPs

The CRPF besides being a Counter-insurgency Operations Force has also been assigned tasks to protect vital installations, dignitaries, critical infrastructure and a few most troubled spots like Srinagar and Jammu airports. The Force is protecting many important functionaries in states too. The threat of IEDs and ambushes are likely to increase in the future owing to lethality of mindless attacks and the fear such incidents generate among people. With unrestricted flow of information on social media, generally not authentic only complicates the situation and then responding under such circumstances becomes very strenuous. The Force has to be trained to cope with such negative and grilling situations.

Handling Public Perception

Handling public perception is emerging as a major challenge for the Security Forces. CRPF is almost always pressed into service on controversial and critical security issues. Unless and until the support of the citizens is with Force personnel, it would be difficult to maintain the trust of the system. The CRPF besides being a Force focused upon complete resolute actions against extremists ought to be imparted soft skills too, so as to connect with people and win over their trust and support. India of today requires a very agile security governance to meet developmental goals and CRPF has to gear up to meet the challenges with which the speed the security environment is changing. A multiple approach of competence building in the profession of security in terms of developing human resources, technological integration and tactical approach is necessary to protect assets of the nation and secure peace. **DA**



SECURITY CHALLENGES OF SMART CITIES

As the cities will turn Smart, improving the city services and providing better quality of living, the services are likely to be more vulnerable to attack and disruption and breach of privacy of individual citizens will be a norm rather than exception. The twin challenges of security and privacy pose another massive challenge before the city managers, that is, how to bring the perpetrators to justice when they operate in a complex, borderless cyber space as faceless entities.

By 2025 fiftyeight per cent of the world's population or 4.6 billion people will live in cities. Huge population will exert unprecedented pressure in the service delivery system of these urban agglomerates. It will be humanly impossible to monitor the various urban services starting from street light to traffic management, garbage collection to supply of safe drinking water etc manually. Therefore, city services are increasingly becoming based on Information and Communication Technologies (ICTs) to provide better living conditions – a concept which is generally termed as 'Smart City'. Though there are several ways to define a Smart City, the International Telecommunication Union (ITU) has

created the definition of 'Smart Sustainable City' as follows: "A Smart Sustainable City is an innovative city that first uses information and communication technologies (ICTs) and other means to improve the quality of life, efficiency of urban operation and services and competitiveness, while ensuring that it meets the needs of present and future generations with respect to economic, social and environmental aspects".



Satyajit Mohanty IPS

The writer is Additional Director General of Police, PHQ, Odisha. He holds a Master of Science and a Law degree from Utkal University, Bhubaneswar, a degree in Master of Human Rights from Pondicherry University and a Management and Public Policy degree from IIM Bangalore and Syracuse University, New York, USA. He is presently pursuing his PhD from National Law University, Odisha. He is a member of the National Police Mission and has been active in formulating sound policy proposals on community policing.





The Perceived Threats

The developments of Smart Cities have been a major global trend in the past couple of decades. Simultaneously, concerns have been raised regarding protection of data, systems and infrastructure that play critical roles in the operation of the Smart City as well as safety and livelihood of its residents. The systems used in the Smart City have sophisticated features and functionality which are often characterised by a high degree of vulnerability to hacking, manipulation and cyber-attack due to their complexity, a high degree of interconnectedness and high volume of information. If a device is hacked successfully, it may act as a pivot and bypass the existing defence mechanism. A related point is that digital lifestyle may have significant privacy costs. The analysis and integration of data has facilitated surveillance and dataveillance (tracking the trails created by activities of an individual) and increased the threat of constant breach of individual privacy.

While undoubtedly the Smart Cities have created new economic and social opportunities, simultaneously they pose challenges to security and expectation of privacy. Humans are already connected by smart phones and gadgets. Smart energy meters, security devices and smart appliances are being used in many cities. Homes, cars, public venues and other social systems are now on the path to full connectivity known as 'Internet of Things' (IoTs). They will lead to unprecedented improvement in the quality of life. Infrastructure and services of cities are changing with new interconnected systems for monitoring, control and automation. The integrated systems will aid public safety, emergency responders and disaster recovery. These benefits must be considered against the potential harm that may come from this massively interconnected world. Two of the most critical challenges of Smart City will be related to security and privacy (Elmaghraby, Losavio -2014, Journal of Advance Research, Vol V).

Connectivity Hubs

Security and privacy concerns rest on how the information within the instrumented (components, devices), interconnected (internet, cloud, server) and intelligent (analytics) environment – 'IN3' – is used. The core of the technology is the information. A full examination of any system of the Smart City may categorise information as to sources, types, collections, analytics and use. The following schematic diagrams explain how the IN3 is brought together in the commercial culture of search, recommender services and locational apps for devices that suggest services based on a person's location, characteristics and historical preferences (Elmaghraby, Losavio, ibid).

The instrumented source may have particular rights or risks associated with particular types of information, such as a person's location or actions. The collection of that information, such as on the device or on a cloud aggregator, similarly invoke issues of rights, duties and risks. From those collections analytics can build services of varied

sophistication which, in turn may be used for good or ill (Fig-1). Information source nodes are

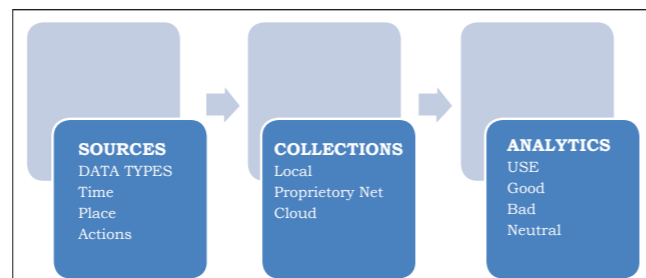


Fig-1 Data sources feed data collections feed data analysis for knowledge
 Courtesy: Elmaghraby, Losavio, Journal of Advanced Research, 2014.

the activities and services of social and civic life, people, work, home, transport and social life (Fig-2).



Fig-2 Source nodes of activities and services producing data
 Courtesy: Elmaghraby, Losavio, ibid

<<http://www.sciencedirect.com/science/article/pii/S2090123214000290#gr3>>

Protecting The Digitised Citizen

Three important challenges of Smart City are discussed in this article, security, privacy and enforcement. Security includes illegal access to information and attack involving physical disruption to services. As digital citizens are more and more instrumented with a host of electronic and telecom appliances, knowingly or unknowingly parting with personal information including real time location, the field of privacy recedes. When an attacker gets illegal access to information, hacks the system and causes physical disruption of services or when the personal information of an individual is used for fraud or blackmailing, the perpetrators must be brought to justice. Such contraventions or offences are committed in the borderless cyber space by faceless entities, making it too challenging for law enforcers to bring them to justice.

Vulnerabilities To Look For

Cesar Cerrudo, the Chief Technology Officer, IOActive Labs, US has delineated that any of the following cyber security problems could trigger a cascading and chaotic effect on the city service:

■ **Lack of Cyber Security Testing**

Often, cities are implementing new technology without testing the efficacy of cyber security. Vulnerable technology which is being used across different industries without security testing is a matter of concern.

■ **Poor or Non-existent Security**

Many vendors do not properly invest in improving security, lack skilled security manpower and have little or no experience in implementing the security features. For instance, many vendors do not object to giving full privileged access to devise or system to anyone who is on a local network because they presume that internal network is safe. However, if an attacker accesses the network, he can easily compromise the available devises and systems.

■ **Encryption Issues**

Wireless devices such as traffic and surveillance cameras, smart meters, street lights, smart pipes, sensors etc make them easy to be implemented but become easy targets of hacking, if communication is not properly encrypted. Many may implement good standard encryption but still have weak encryption key management. Once an encryption key is compromised, attackers get full access to communication. In a nutshell, when either the wireless and wired communication is not secure, an attacker can easily intercept and manipulate communication and take control of devices and network.

■ **Large and Complex Attack Surfaces**

There is huge and unknown attack surface on Smart Cities. With so much of complexity and interdependency, it is difficult to know what and how everything is exposed. A simple problem could cause a big impact due to interdependency and chain reaction.

■ **Patch Deployment Issues**

Patch deployment and system updates face many security problems. Because of complexity, patches are difficult and costly to test on non-production system. It has become common for cities to use vulnerable devices and systems because vendors are either slow to release patches or patches are not available.

■ **Insecure Legacy System**

Often new technology is being integrated with old technology that may be vulnerable. Some old technologies that lack standard may require a piece of technology in middle to communicate between old and new systems and to translate protocols. Some systems may not run on newer and more secure operating systems and therefore, the older and vulnerable operating systems remain in use. This adds to the complexity, increases the attack surface and makes adoption of newer technology slower.

■ **Simple Bugs with Huge Impact**

A simple software bug can have huge impact in a city that is running hundreds of system and devices for critical services. To illustrate an example, on 14th August, 2003 a blackout affected an estimated ten million people in Ontario and 45 million people in eight US States. The blackout was caused by software bug in the alarm system at a control room of First Energy Corporation located remotely in Ohio.

■ **Susceptibility to Denial of Service**

With so many services depending on technology in a city, attackers have many methods to abuse the Denial of Service (DoS). For instance, DoS attack could interrupt a server feeding data to a number of systems thereby having a big impact on regular city services and activities.

Cyber-attack On Cities

Technologies used by the Smart Cities and the associated cyber security problems open the door for several possible cyber-attacks. Let's discuss some of the key technologies and systems that together make up Smart City's complex attack surface.

Traffic control systems without an encryption for communication between traffic control systems, traffic lights, traffic controllers allow an attacker to directly change the traffic lights. The chaos in which thousands of busy intersections in cities flashing wrong traffic signals is beyond imagination.

Wireless street lighting systems are being deployed in many cities around the world. Most systems use wireless communication and have the encryption related problems described earlier. Attacks on smart street lighting system can have big impacts by causing street blackouts in large areas.

Sabotage

Every city has hundreds of systems to manage different services and tasks. Hacking these systems would give leverage to an attacker to cause incalculable damage in terms of lives and property. For instance, an attacker could manipulate map information with work orders being given to the contractors to dig a hole over gas or water pipes or communication cables with the intention to damage these facilities.

Smart City systems rely heavily on sensor data to make decisions and to act on such decisions. Most sensors use wireless technology which is susceptible to breach of security. Attacks that involve compromising sensors, sending fake data can directly affect the systems, since decision and action will be based on such fake data, which could have spiralling and cascading effect on the city services. The attackers could even fake an earthquake, gun shooting, large scale riot, raising alarm and causing general panic.

Public data (open data) is available to all and sundry in real time. This data can be used to select a target or schedule the timings. For example, attackers can identify exactly when a bus or train would arrive or when the traffic is at its peak and plan accordingly for maximum damage.

Mobile applications are affected by common security vulnerabilities which could allow the attackers to perform a variety of operations from simple Man in The Middle (MiTM) attacks to more complex ones. Mobile applications are an important target since users make decisions on the basis of such information. Hacking mobile apps could have direct impact on citizens' behaviours. For example, if a hacked public transport app shows delay of the scheduled transport like bus or rapid transit system, the user may prefer to commute by his own car. If similar decisions are taken by hundreds of commuters on the basis of bugged apps, the city roads would be clogged with traffic going haywire. The surveillance cameras are becoming more widely used in the cities around the world keeping virtual surveillances on the key activities of the city. A Denial of Service (DoS) attack on these devises is possible by modifying firmware or exploiting the vulnerabilities. Some of these cameras

are wireless and suffer from the problems such as no encryption or weak encryption, making them more vulnerable for attacks and manipulation.

The use of online social networking sites for feedback on municipal services is increasingly becoming common in the recent past. This platform could be abused by subversive elements for creating confusion, chaos and even abetting hate crimes.

Challenges To Privacy

Further, the legal and social concepts of a citizen's 'right to privacy' are entangled with the challenge of cyber security and the benefits of the Smart City. That legal /social concept of privacy addresses confidential aspects of life, control of one's own public profile and a life free of unwarranted interference. This applies to both state action and that of private parties. As to 'cyber privacy' the legal regime is further defined by related, analogous statutes that may prohibit unauthorised access to a computer, a network and related data, unauthorised interception of, interference with or transmission of data and unauthorised data processing and analytics of a data collection. Any of these may be authorised by statute, judicial order or the consent of a data subject. So the data processes of the Smart City may be completely permissible under the law. But the benefits of the Smart City, such as locational services, may create unexpected risks.

Locational data can detail much about a person's life they do not wish revealed. GPS systems can track destination and origination points when used and may even store the actual route taken. Access to contact lists and messages tells much that may need to be kept private for personal, professional or commercial reasons.

Increasing urbanisation is changing the operating landscape for law enforcement Agencies worldwide

Locational data can be a key security concern. Many set the GPS originating address from their homes. Access to these data details that home location. If the automobile is away from home, that home may be a better target for burglary. This privacy violation is a major security risk. Once the motivated offender has a profile and location on the victim/target at all times he or she knows when that victim/target would be most vulnerable to a physical attack (Elmaghraby, Losavio, *ibid*).

Challenges Of Enforcement

Increasing urbanisation is changing the operating landscape for law enforcement Agencies worldwide, where more than 35 cities are home to a population of more than 10 million each. Higher population and infrastructure density would lead to increased diversity and social changes, presenting new security challenges. With globalisation, criminals also have been able to operate 'in loose and fluid networks' to avoid investigations and prosecution.

The global reach of crime indicates that geographical boundaries are no longer constraints in launching attacks of scale and high impact. In the recently concluded Interpol World Conference at Singapore the police leaders and industry stakeholders across the globe expressed concern over the challenges of enforcement of cyber-crimes. Madan Oberoi, director of cyber innovation and outreach for Interpol Global Complex for Innovation <<http://www.zdnet.com/article/interpol-presence-strategic-to-singapore-cybercrime-purge/>>, noted that the borderless nature not just of the Internet, but also of the services most commonly used today as well as the globalisation of business operations posed a serious cyber security challenge for law enforcement. While the industry had grown increasingly borderless, law enforcement remained governed by local jurisdiction. To drive multi-jurisdictional cooperation and interoperability, standard operating procedures (SOPs) and processes must be established. However, even if such SOPs were in place, the question remained whether all countries or jurisdiction would have the capacity or necessary infrastructure to support such processes, he said, pointing to the disparate level of readiness between nations as another key challenge in cyber security. The Singapore Home Minister in his keynote address underscored the international cooperation between governments to tackle the borderless nature of crime, which would support quicker identification as well as mitigation of threats. The law enforcement Agencies around the world need to collaborate and leverage each other's resources and build expertise as well as introduce 'innovative policing solutions' beyond the traditional methods of investigation. The Conference highlighted the importance of closer cooperation between the government and private sector <<http://www.zdnet.com/article/singapore-reiterates-call-for-industry-collaboration-in-security/>>, pointing to information sharing, research and development, as well as capacity building and training.

As the cities will turn Smart, improving the city services and providing better quality of living, the services are likely to be more vulnerable to attack and disruption and breach of privacy of individual citizens will be a norm rather than exception. The twin challenges of security and privacy pose another massive challenge before the city managers, that is, how to bring the perpetrators to justice when they operate in a complex, borderless cyber space as faceless entities. The international bodies of governments, national governments, industry managers, cyber security experts, law enforcers and all stakeholders must come together as the challenges need solutions in shape of new national legislations, international laws, protocols, standard operating procedures, security audit norms and regulatory regimes.



ASIA 2015
KUALA LUMPUR, MALAYSIA
4th GENERAL POLICE AND SPECIAL EQUIPMENT EXHIBITION & CONFERENCE ASIA PUTRA WORLD TRADE CENTRE (PWTC)
21st - 23rd OCTOBER 2015
Opening Hours
10.00am - 5.00 pm



A show dedicated for police, special forces and internal security equipment and services

- 1 A congregational point for regional law enforcement agencies.
- 2 Platform for inter-disciplinary cooperation for information exchange.
- 3 Delegations from ASEAN and Asia Pacific countries.
- 4 A power-packed international security and law enforcement conference.

ASIA'S LARGEST POLICE & HOMELAND SECURITY EVENT
Incorporating
1st PUTRAJAYA INTERNATIONAL SECURITY DIALOGUE

BOOK YOU SPACE NOW AT:

Middle East and Asia Pacific
F & R EXHIBITION AND CONFERENCE SDN BHD
Unit 23A-3A, Level 23A, Menara 1 Mont Kiara
No 1, Jalan Kiara, 50480 Kuala Lumpur, MALAYSIA
tel + 603 - 6243 1115
fax + 603 - 6211 0101
email marketing@fr-exhibitions.com.my
website www.fr-exhibitions.com.my
www.gpecasia.com.my

Rest of the World
EXHIBITION & MARKETING WEHRSTEDT GMBH
Hagenbreite 9, 06463 Falkenstein Harz
/ OT Ermsleben, GERMANY
tel + 49 (0) 34 743 - 62 092
fax + 49 (0) 34 743 - 62 091
email info@gpec.de
website www.police-exhibition.eu
www.gpec.de



AVIATION SECURITY

IMPORTANT LINK IN NATIONAL SECURITY CHAIN

While theft is bad, the fact that someone did have unauthorised and undetected access to commit these offences or the integrity of someone within the employ of airport or airline is compromised, is a serious matter. The incidents could have been committed as a test case by the enemy agents to assess the vulnerability of aviation security set-up. Such incidents therefore need to be resolved quickly before the enemy could strike in full force.

Security of a nation depends on securing all its assets. These assets consist of geographical area of the nation and other assets like human resources, physical resources and non-tangible assets like reputation in the world community and intellectual property. Physical resources include transportation infrastructure and related facilities. The security of transportation assets especially aviation systems assumes an important position as any harm to them is widely seen as lack of capacity of the nation to protect its assets and people from the enemy.

Effect On National Morale

Any unlawful interference in civil aviation by incidents like hijacking of aircraft, causing explosion in it or seizure of airport or aircraft on ground is a serious threat to national security. Hijacking of Indian Airlines Flight IC 814 in December 1999, from Kathmandu to

Kandahar and subsequent release of three terrorists held in Indian jails in exchange for hostages, showed how national security had to be compromised on account of failure in aviation security even though at a foreign airport. The tragic events of 9/11 in USA, in which civilian flights were commandeered by terrorists and used as missiles to hit Twin Towers and other strategic buildings like the Pentagon, shook the confidence of the entire world in the capability of USA to defend its people and assets against such attacks. It made the USA think deeply about the gaps in its own national security. Earlier, a single bomb planted in Pan Am Flight 103, in December 1988, (Lockerbie Bombing) not only destroyed the aircraft and killed all its passengers and crew but eventually wiped out, in compensation, the assets of the airliner company itself. On the other hand, French Airliner Flight 139 flying out from Tel Aviv to Paris (June 1975) and having large number of Israel nationals on board was hijacked to Ugandan Airport at Entebbe.

The hostages were rescued by the Israeli Defence Forces Team, in a meticulously planned and surgically executed operation. The successful raid at Entebbe raised the morale of their people to all time high-level.

Aviation Vulnerabilities

It is clear that even if the enemy (country or group) is unable to invade the country physically, it can still cause tremendous damages by hijacking aircraft, causing explosions in aircraft or at airports, taking control of civilian aircraft and using them as missiles and attacking the vital systems. Any hijack of passenger aircraft or seizure of airport or aircraft on the ground results in feeling of insecurity in the minds of travellers specially tourists and many amongst them would drop the concerned country from their itinerary. Therefore securing the aviation assets like aircraft, airports, passengers, crew, cargo, mail and stores is important even from national security standpoint. In the Indian scenario, the problem is quite huge. Here a large number of extremist groups (35 of them stood banned as on 31st March 2015) operate. Some of them have support and links with Pakistan's Intelligence Agencies or terrorist groups like Al Qaeda and Taliban in neighbouring countries. If we examine the previous hijack incidents in India, the complicity of Pakistan is evident in at least five of them. Also, new threats like attack by laser beams and cyber-attack are emerging. Further, as per the data from Airports Authority of India, the Indian airports handled more than 188 million passengers and more than 2.5 million metric ton of cargo in 2014-15. There are more than 120 airports in the country, some of them being operated by State Governments, private parties and by Defence Forces as well.

Each airport has to be secured to complete the security chain because each link in the national security chain is equally important. Aviation security (AvSec) exactly deals with this issue.

ICAO Jurisdiction

Internationally the ICAO has developed Protocols, Rules, Regulations and Practices in the field of Aviation Security which are to be followed by the member nations. ICAO Chicago Convention 1944, as amended by Beijing Convention and Protocol of 2010, is to be followed in aviation matters. Annexure 17 to the Chicago Convention contains Standards and Recommended Practices for aviation security. Each Signatory Country is to notify an 'Appropriate Authority' for aviation security matters. In India, Commissioner (Civil Aviation) Security, Ministry of Civil Aviation, Government of India has been notified as the 'Appropriate Authority'. It has framed Rules and prescribed Procedures for ensuring Aviation Security at Indian Airports and also for all Indian Registered Aircraft in India as well as abroad. 'Aviation Security Programme' has been prescribed for all stakeholders. To meet any national contingency like hijack of aircraft or seizure at airport, it has a 'National Civil Aviation Contingency Plan'.

Petty Crime Could Be Precursor

The airports are physically secured by Government of India Security Forces or Police Forces of the State Governments. Security Procedures are implemented through the trained personnel of these forces and airlines. Also, most of the airlines maintain a posse of security staff of their own, duly trained in aviation security duties. Thankfully no hijacking has taken place for the last 20 years from any Indian airport. The last hijack of Indian Aircraft was not from Indian soil but from Kathmandu, Nepal in 1999. But In spite of best efforts, security incidents like trespass into the Security Restricted Area of the airport and communication facilities, illegal carriage of individuals in aircraft belly or cargo containers (stowaways), damaging of airport boundary and theft of communication equipment from airport taxiways and runways do take place from time to time. While theft is bad, the fact that someone did have unauthorised and undetected access to commit these offences or the integrity of someone within the employ of airport or airline is compromised, is a serious matter. The incidents could have been committed as a test case by the enemy agents to assess the vulnerability of



Sharda Prasad IPS (Retd)

The writer is a Former Officiating Commissioner (Civil Aviation) Security, Bureau of Civil Aviation Security and Subject Expert Member, Security Advisory Committee, Civil Aviation, Ministry of Civil Aviation, Government of India.



aviation security set-up. Such incidents therefore need to be resolved quickly before the enemy could strike in full force. Considering the present level of threat and aviation security practices, following suggestions are being made:

Set Up Active Defence

● **Use Of Available Intelligence:** Information sharing on security needs should be more free-flowing, timely and go to the right units for their development, enhanced analysis and dissemination on need to know basis. We may recall Purulia incident (December 1995) in which a low flying foreign aircraft was used by some agency to drop large quantities of arms and ammunition in some villages of Purulia District in West Bengal. It was designed to cause widespread armed unrest around dropping area. In this case though Intelligence was available timely, it was never applied to detain the foreign aircraft while it refuelled on the Indian territory before dropping of the weapons. The Intelligence was simply disseminated to States who deployed police to watch the sky for possible droppings. Bomb threat calls and hijack calls should likewise be analysed and disseminated appropriately.

● **AvSec Objective:** The objective of deployment of aviation security personnel is to ensure safe and secure travel and transportation of cargo, mail and stores and also to secure our aviation assets. They should be entirely devoted to that task. The present trend of deployed security force in earning cheap popularity by publicising on work not directly related to security performance and publicly expressing disagreement with security regulator or pointing out security deficiency may only help the enemy in finding the weak link in the security chain.

● **Know Your Workers:** Airports work like a mini-city with only difference that those who work there do not have their homes inside. Everyone comes from outside the airport to work there. At any airport there are a large number of persons reporting for work. Some work for short duration (like delivering supplies, carrying out special repairs, take measurements) and some for long periods (like passenger and aircraft handling staff, cargo, conservancy and maintenance staff). Each worker required for long-term assignment must have his credentials verified before he or she joins duties. The practice of unescorted movement of workers inside Security Restricted Area of the airport on the basis of temporary pass should be discontinued. Those who are required for a short duration inside the Security Restricted Area should be issued Temporary Passes on production of Requisition from indenting

authorities and issued only to those carrying valid identity papers. They should be escorted at all times so long they are inside the Security Restricted Area. Each such worker must be issued a pass individually by name which could be verified on ground by tallying with ID papers on him or her. Passes should not be issued collectively (for example issued to: Mr X with five persons) as it leaves scope for manipulation and entry of undesirable elements.

● **Know Your Passengers:** Many countries have Advanced Passenger Information System. The information available on it is of rudimentary nature. In some cases the Frequent Flyers information might be available on it. We can get additional information if we can incorporate in it the PAN Number or Aadhaar Card number. This can further be linked to other systems of Intelligence Agencies to flag down persons of suspicious antecedents. While it may not be appropriate to debar them from travel, certainly the security apparatus can be extra vigilant in their case and take appropriate measures to thwart their anti-national plans. They can be subjected to special screening and their baggage can be double checked for any weapons or explosives. It

can also be checked if such passenger is travelling alone or there are others travelling by same flight who could be acting as accomplices in incidents in the air. Another improvement, as suggested by ICAO to States, which can be brought about at International Airports is the introduction of Machine Readable Travel Documents. This will help in identifying passenger along with all required Data about him.

ICAO has provided necessary technical know-how and training for its implementation. It has fixed a deadline for its implementation by the member countries as of 24 November this year.

Autonomous Control Agency

Above measures, if taken would certainly improve the aviation security scenario in the country. Added to this, if we could have a dedicated organisation exclusively to look after the Security implementation on ground, as with our neighbour Pakistan the AvSec would be further strengthened. This step will be conducive to develop expertise in the AvSec field and in the long run be economical as attrition rate for the organisation would come down and efficiency levels will increase.

If we want the national security chain to be complete and strong, the aviation security has to be made foolproof and the loopholes coming to the knowledge of the authorities must be plugged expeditiously. Further, there is need for regular threat assessment to the aviation security and the aviation security measures must be brought up to a level commensurate to meet the threat. **DSA**

If we examine the hijack incidents in India, the complicity of Pakistan is evident in at least five of them



ROLE AND CHALLENGES

The ITBP was raised in 1962 in the wake of Chinese aggression. Originally conceptualised as an integrated 'guerrilla-cum-intelligencecum-fighting Force' self-contained in supplies, communication and intelligence collection, it evolved with passage of time into a conventional Border Guarding Force capable of performing multifarious assignments.

Role Of ITBP

The primary role of ITBP is to safeguard the security of India-China Border and promote sense of security among the people living in Border areas. Prevent transborder crimes, smuggling, unauthorised entry into or exit from the territory of India and any other illegal activity. Provide security to sensitive installations, banks, persons of security risk. Restore and preserve order in any area in the event of disturbance therein

Area Of Responsibility

ITBP is presently guarding 3,488 km of Indo-China Border on altitudes ranging from 9,000 ft to 18,750 ft along the Himalayas from Karakoram Pass in Ladakh to Jachep La in Arunachal Pradesh. Most of the forward posts remain cut-off by surface route during winter season. The Border posts are located in extreme high altitude areas which are exposed to the fury and violence of nature in the shape of high velocity storms, snow blizzards, avalanches and landslides, besides the hazards of high altitude and extreme cold, where temperature falls up to minus 40 degree Celsius. ITBP conducts large number of Long Range and Short Range Patrols upto the altitude 20,000 ft and above on the remote, rugged and inhospitable terrain of India-China Border. The ITBP troops are also deployed at Nathu La in Sikkim for Border trade duty. 02 coys of ITBP are deployed to

escort the traders from Nathu La to Serathang and back. Besides, ITBP troops are also providing security to IB check posts located on India-China Border in Arunachal Pradesh.

Tasks Of ITBP

The primary task of ITBP is to ensure the security of India-China Border by conducting patrolling and physical presence on the Border Outposts (BOPs). Ensure internal security by conducting Counter Insurgency Operations in insurgency affected areas. Conduct Anti-Naxal Operations in Naxal infested states and Internal Security duties during riots and disturbances within the country. Provide security to the Indian diplomatic missions abroad. Provide protection to VIPs on the directions of Government of India. Serve as Lead Intelligence Agency (LIA) for providing intelligence related to India-China Border for Western and Central Sector.

Challenges In Border Guarding

■ Western And Central Sector

● Most of the BOPs are not road connected and ITBP troops have to move on foot through narrow valleys, passes and gorges with acute gradient for many days to reach the BOPs. The movement is entirely valley based due to which cross-country movement is difficult. Due to non-existent/poor road connectivity, it has to depend on porters, self-man pack, ponies or helicopter drops for ration and stores. Almost all the BOPs are devoid of electricity and have to use kerosene oil for cooking and solar lanterns and diesel generator sets for lighting purpose.

● Due to long monsoon and winter season, the working window for developing infrastructural works is very short. The construction and other infrastructure development activities are possible only for 6-7 months (April to October) in states of Jammu and Kashmir, Himachal Pradesh and Uttarakhand.

● It is difficult to carry out patrolling activities due to lack of oxygen in high altitude areas and difficult terrain. Even scanty rainfall in the areas of Jammu and Kashmir, Himachal Pradesh and Uttarakhand causes landslides, mudslides, flash floods and rivers to overflow which restricts the movement of troops. The BOPs experience heavy snowfall in winters causing extreme cold conditions (up to minus 40 degree in winter) and snow hazards. The long winter duration limits the movement of troops from forward areas and the troops are forced to stay in BOPs for long durations. The troops deployed at BOPs have to sanitise the water from streams using chloroquine tablets and by boiling before using it for drinking purpose. During winters the troops melt snow to make drinking water as all the rivers and streams get frozen due to extreme cold (up to minus 40 degree in winter).

● The troops posted in high altitude BOPs are exposed to physical and psychological health hazards

such as frost bites, snow blindness, pulmonary odema, chillblains etc. The exposure of troops to high altitude causes loss of memory, stress, indigestion and deterioration in reflexes.

● Ensuring medical facilities to the personnel deployed in BOPs is another big challenge, especially during monsoons and winters as the land routes are blocked. The evacuation of patients from BOPs becomes extremely difficult as the aircraft cannot operate due to bad weather and poor visibility in high altitude areas. During monsoons/winters, the surface routes to BOPs are also almost inaccessible due to the overflowing rivers, nullahs and snowfall enroute to BOPs. The route for patrolling up to international passes is even more difficult due to non-existent tracks, snow covered areas and glacial regions. The weather is unpredictable, restricting the movement of troops. There are limited means of communication due to non-availability of mobile network and landline connectivity.

● The efficiency and shelf-life of equipment is also reduced due to extreme cold climate. The batteries of telecommunication equipment get discharged instantly and have to be recharged constantly to ensure timely communication. Other equipment have to be constantly checked, to ensure that they do not go faulty due to humidity and rust.

■ Eastern Sector

● Thick undergrowth in Eastern Border restricts visibility and movement. Due to non-existent /poor road connectivity, it has to depend on porters, self-man pack, ponies or aerial dropping. The BOPs are devoid of electricity and use kerosene oil, solar lanterns and diesel generator sets for lighting purpose. In order to make the water from streams suitable for drinking purpose it is sanitised by boiling or by using chloroquine tablets, before using it for drinking purpose.

● Due to long monsoon and winter season, the working window for developing infrastructural works is very short. The construction and other infrastructure development activities are possible only for 5-6 months (November to March) in Arunachal Pradesh and Sikkim.

● It is difficult to carry out patrolling activities due to thick vegetation and difficult terrain. Entire NE region during monsoon experiences heavy rainfall causing landslides, mudslides, flash floods and rivers to overflow, restricting the movement of troops. The long duration of monsoon and winter limit the movement of troops from forward areas and have to spend long durations in BOPs.

● The troops posted at BOPs are exposed to leeches, snakes, bees, insects, mosquitoes etc. The long inter-BOPs distance and lack of proper roads /tracks, causes fatigue to the troops. The medical facilities at BOPs are also of limited nature and the evacuation of patients for treatment to higher centres is extremely difficult due to absence of roads. The patient cannot be transported through land

route also due to undulating ground and absence of proper roads and tracks. The evacuation of patients from forward areas is also possible only at helipad due to narrow valley and dense forest.

Internal Security Challenges

■ Naxal Theatre

Apart from its primary role of border guarding, ITBP is also being utilised for Anti-Naxal Operations in the state of Chhattisgarh since year 2009. The duties in Naxal scenario are equally challenging as that of Border guarding as it is very difficult to differentiate between Naxals and innocent tribals. However, ITBP has been able to tackle the Naxal situation in Chhattisgarh with professional acumen. ITBP has been successful in curbing the Naxal menace to a great extent. The above units are dominating their AoR effectively by conducting area domination patrolling, night domination patrols etc. During encounter with Naxals ITBP has eliminated many Naxals and has also been successful in recovering huge quantity of arms, ammunition and explosives from the Naxals, to keep themselves safe from the wicked motives of the Naxals ITBP personnel carry out extensive patrolling through thick forest, hilly terrain and tribal habitations in their area of responsibility. To prevent casualties from IEDs, they avoid moving by road and have to carry out long-range patrolling moving through forest areas. The patrolling also varies from 1 day to 4-5 days and the troops have to stay in jungles with barest minimum amenities where they are vulnerable to ambushes and IED blasts. The Naxals are mostly limited along the interstate border. Whenever the security forces launch an operation, they manage to move across the state boundary and manage to flee taking advantage of the local population and restrictions imposed on the forces to cross state boundary. Apart from the Naxal threat, the troops are exposed to snake bites, fungal infections, insect bites and mosquito bites. There are always high chances that the troops suffer from dehydration, sunstroke, malaria and other diseases during operations.

■ Law And Order

Although, ITBP is a trained force deployed on the India-China Border for border guarding, it is also being utilised for tackling Internal Security and law and order duties, VIP Protection etc. 02 ITBP Battalions are performing sensitive duty of VIP security at Delhi, Jammu and Srinagar. Besides, ITBP is providing security to various installations of national importance throughout the country, which includes Rashtrapati Bhawan, Vice President house, Tihar Jail etc. ITBP is also providing security to other vital installations such as NTRO and ARC installations. ITBP is also deployed in various parts of India for maintaining law and order in the states. ITBP is also being utilised for providing security during elections and post poll duties in various parts of the country.

■ Indian Missions Abroad


Deployment of force in war-torn Afghanistan is another feather in the cap. A highly trained and motivated team of elite Commandos has been deputed for this task since 2002. ITBP troops are deployed in Afghanistan since 2002 and providing security to EoI Kabul and Indian Consulates in Jalalabad, Kandhar, Majar-e-Sharif and Herat. ITBP troops are providing mobile security to the Ambassador at EoI Kabul and Consul General in the 4 Consulates apart from providing static security to the Embassy and Consulate Complexes. The troops deployed in Afghanistan are guarding the Embassy and Consulates under the constant threat of IEDs and suicidal attacks by Talibans.

On 23.05.2014, a well-planned suicide attack by a group of determined *Fidayeens* was successfully defeated by our brave troops deployed for the security of Consulate General of India at Herat in Afghanistan in which 4 *Fidayeens* were killed with recovery of arms, ammunition including 04 primed Hand Grenades and Rocket Propelled Grenades. For their gallant act, Government of India has honoured them with Gallantry medals (Shaurya Chakra -01 and PMG -04) on the eve of Republic Day, 2015.

Major Challenges

Most of the ITBP BOPs are situated at isolated places which are not connected by roads and communication systems. The personnel deployed at these BOPs have to remain away from their families for long time. The means of entertainment are also limited, which causes them to suffer from loneliness, depression. Although best efforts are undertaken to provide quality medical facilities to the BOPs but still the medical facilities are not very satisfactory at the BOPs. There is shortage of medicines and very limited life-saving facilities. Many BOPs are not road connected and have to be dependent on air support for ration items. The movement of personnel from BOPs especially during winter is a major challenge. Some of the BOPs get so isolated during winters that a person can move only after the accumulated snow melts and spring arrives.

The multifarious duties being assigned to the force also affect the morale of the troops. The ITBP troops serving in plain posting have to undertake many other assignments of internal security, law and order and disaster management etc that they hardly get any time to stay with their families. These strenuous duties affect their mutual as well as their family relations causing distress among them.

Despite the odds being faced by ITBP, the troops are performing their duties in inhospitable and uncongenial climate, under stressful conditions with dedication and devotion. 



GLOBAL BEST PRACTICES SMART AND SECURE CITIES

Governments all over the world are facing increasing budget constraints. At the same time, agglomeration of urban clusters and evolution of urban habitats are irreversible and there is a clear mandate now on public sector leaders to provide Smart City services to ensure that the citizens receive the service at the right place, at the right time and at the right cost.

The world is moving to the cities at an incredible rate. Today over 4 billion people, more than half the global population, live in urban environments. In less than thirty years, urban populations are expected to reach six billion in total. This massive increase in population significantly increases pressure on cities to address complex problems from education, transport and public safety to city-governance and sustainability. To add to these challenges, cities need to optimise resources. The financial crisis forced many cities to review their income and expenses. Since cities already account for a majority of greenhouse gas emissions and consume about two thirds of the world's energy, city corporations are moving quickly to reduce energy demand while resourcing sustainably. Also, considering most of urban centres are coastal, recent disasters highlighted the need for increased viability in the face of changing weather and rising sea levels. There exists a clear priority for sustainable economic development.

In this article, global best practices are considered and a viable and proven framework deployed in the solution-context is discussed.

Demographic And Environmental Trends

Developing the infrastructure of these new cities will require unimaginable amount of money and effort. The environmental impact of this massive urbanisation is significant. It is believed that cities consume three-fourths of the world's energy and are responsible for most of greenhouse gas emissions. The need for all these cities to sustainably balance social, economic and environmental resources is more critical than ever before. Previous centuries saw industrial infrastructure such as rails, roads and telephone lines paving the way for new cities and new connections. The future is about urbanisation based on information and the network as the underlying platforms. Today, urban infrastructure including homes, offices, cars, public transport, hospitals, schools, energy and appliances are all being connected via wired or wireless infrastructure to the Internet. The Internet has expanded into an 'Internet of Things' beyond traditional computers and mobile

devices. Cities using the network as the platform to plan, build and manage day-to-day operations will gain significant new efficiencies in every aspect of community life: enhancing productivity among city employees, improving availability and access to public services and creating new models to generate needed revenues. These communities will reap significant benefits that include all of the following gains:

- Environmentally and economically sustainable urbanisation
- Richer and enhanced quality of life for citizens
- Efficient and improved city management
- Steady and continuous economic growth

The Opportunity

The smart city uses a combination of technologies to address urban challenges. For example, traffic management features prominently on the list of issues for cities. Successful approaches in cities like Stockholm or London make use of congestion pricing to reduce demand for limited road infrastructure in city centres. A maze of sensors, riding a solid and underlying network infrastructure, is leveraged to monitor usage and increase charges during peak times to reduce demand. Cities are understandably cautious when considering those qualified to design, build and manage these large, complex systems. Hence, for example, the renewal of London's Congestion Charge contract was a race between at least three publicly traded firms. Making cities smart has largely been associated with making government smarter by designing, building and operating dedicated custom infrastructure and systems. There is telecommunication infrastructure that distributed sensor networks depend on for everything from traffic to energy measurement. There are clouds in which to house applications and large sets of data. And, there are city command centres to bring all of this information together and enable coordinated responses.

The Priorities

In a survey done among modern European cities, the priorities for any city government seemed to appear as follows in decreasing order: Environment,

Economic Development, Mobility of Citizens, Systems and Services, Education, Inter-dependent Processes, Health, Government Functions and Tourism.

Objectives Of The Smart Cities

Most modern cities which are either retro-engineered to a smart and secure habitat or are built as greenfield habitats, have some common objectives.

- Bringing improvement in residents' quality of life
- Bringing greater efficiency and lowering the cost of services delivery
- Promoting local industries, SMEs and drivers of technology capacities
- Improving citizen traction with public services and government Agencies
- Building a foundation for the creation of new services in the form of an open network, data and services architectures
- In the next few years, it aims to progress from a focus on data provision in isolated silos to become a platform for value-added services
- Smart City means more than advanced infrastructure and state-of-the-art technological solutions but also includes reengineering business services to meet demands of greater citizen engagement and transparency of city governance

Smart City Practices And Solutions

Depending on the priorities of the government and the communities, evolution of Smart City strategies and plans take place in a consensus-driven stakeholder ecosystem. One of the core responsibilities of governments is to protect and serve citizens. Whether

it is crimes, fire, accidents or natural disasters, every city has a unique mixture of safety concerns. Education, healthcare and entertainment are a prime focus for the constituents of any community. Stringent budgets, limited resources or time and handling vast amounts of data all make managing cities a mammoth task. Imagine a government experience that is engaging, where you can access the information you need to live, work, play and learn in your community. Public safety and security are stable platforms and government offices and community transportation systems are designed for citizens of all ages. Smart City Solutions provide organisations the ability to be more connected with constituents, while managing operational costs. It provides governments with the technology and facilities that enable constituent engagement and access to the information they need. For example, you can renew your driver's license from your home.

The following set of tables give a broad overview of the benefits to stakeholders and the solution features, as is seen from exemplar strategies – you will notice that at the foundation of these solutions rest a sound network architecture.



KPM Das

The writer is Vice President, National Security and Defence Solutions, Cisco Systems.





Remote Expert Solutions	Cities are always challenged in the asymmetric ratio of experts and officials to citizens – there is a need for pooling expertise and service points for citizens to access from places of their choosing.	
	Benefits	Solution Features
	<ul style="list-style-type: none"> Improved citizen services while reducing the overall operating costs for the government Reduction in real estate and staffing costs for government Improved employee productivity through centralisation of expert resources Increased access to government services in rural areas Reduced carbon footprint by minimising travel to government centres Improved traffic flow management by dispersing PoDs in key areas of large cities Better overall citizen satisfaction and perception of the governance 	<ul style="list-style-type: none"> Easy to use and initiate sessions Creates a virtual pool of experts that are located in a centralised environment, maximising the effectiveness and reach of their knowledge base Provides high-quality audio and video for citizen interactions, delivering a compelling citizen experience Allows experts to conduct a complete service transaction including document sharing and printing Enables citizens to have personalised experience maintaining confidentiality of the transaction Allows integration with security cameras, digital signage and queuing systems for additional capabilities

Smart Parking **Increasing urbanisation and mobility of citizens have increased the ratio of vehicles to road and parking space manifold. There is clearly a need to bring transparency, automation and efficiency to the parking function within cities with clear incentives for placing a premium on parking spaces, use of public transport and monetising this critical city service function.**

	Government Benefits	Solution Features
	<ul style="list-style-type: none"> Increased revenue through improved capture rates and tickets issued for parking violations Additional revenue from pricing changes powered by analytics Higher enforcement officer productivity and empowerment through the use of technology Improved success rate in parking ticket disputes 	<ul style="list-style-type: none"> Parking Guidance: Search for parking space based on point of interest or preferences, receive voice guidance to parking space and make payments using mobile phone Parking Enforcement: View live video feed of parking and no-parking zones; detect and report parking violations in no-parking and loading zones via video Administration: Easily configure and manage sensors, video infrastructure and policy/rules for parking violations Analytics: Gather parking occupancy, revenue and enforcement reports with details on time of day, day of week etc to assist with pricing decisions
	Citizen Benefits	
	<ul style="list-style-type: none"> Reduced circling, leading to savings of time and fuel Less overall congestion and general improvement in quality of life 	

Secure Cities **As cities continue to grow in number, size and complexity, their infrastructure and services come under increasing stress. Keeping cities safe is critical; safe cities attract the investments, businesses and skilled labour necessary for economic growth and development. Smart City Solutions helps protect cities against crime, terrorism and civil unrest. It helps law enforcement monitor public areas, analyse patterns and track incidents and suspects, enabling quicker response. By combining information from video surveillance cameras, social media, citizen reports and other sensors, the solution provides a richer view of urban safety.**

	Law Enforcement Benefits	Solution Features
	<ul style="list-style-type: none"> Reduced crime Increased attractiveness to businesses and workers Improved planning and resource allocation Higher rate of incident detection Automated incident detection and quicker response Increased situational awareness More effective operations 	<ul style="list-style-type: none"> Location monitoring: View live feeds of any surveillance camera to assess conditions; collect data on crime type and location; and monitor social media for possible threats Incident detection and management: Use video feeds and analytics to verify and detect threats and incidents; alert operators to potential incidents; create incident records; and collect all data regarding the incident lifecycles Administration: Easily configure and manage sensors, video infrastructure and policy Analytics: Report security incident distribution over districts/precincts, time, day and month to aid planning of deploying security assets. Identify areas with recurring crime and law-order issues
	Citizen Benefits	
	<ul style="list-style-type: none"> Safer streets and neighbourhoods Ability to report city safety incidents Improved communications about incidents 	

Smart Lighting **As cities continue to grow in number, size and complexity, urban infrastructure and the services that rely on it are increasingly stressed. Of all urban utilities, street lighting comprises one of the largest expenses in a municipality's utility bill, accounting for a large proportion. Furthermore, electricity prices have increased significantly worldwide, which add to a city's expenses. Cities are looking for a solution to help reduce lighting expenses and at the same time improve operating efficiencies while minimising upfront investment.**

	Benefits	Solution Features
	<ul style="list-style-type: none"> Energy savings by adjusting light levels based on traffic density and the use of dimming, which extends luminary life Central monitoring and reporting of individual street lights, enabling more effective maintenance Improved accuracy and simplification of asset management through the use of tagging and tracking lights Reduction in carbon emissions plus energy savings of up to 50%, rising to 80% with the introduction of Smart Lighting Control Improved response to emergencies and alerts due to easier identification of the crisis scene 	<ul style="list-style-type: none"> Remote monitoring: Lighting failures are automatically reported by the system, saving time and costs Asset management: The system intelligently plans and routes maintenance work to minimise street blockages Automated dimming and scene setting: Lights are dimmed during low traffic hours to save energy or enhanced in problematic neighbourhoods to improve safety Intelligent energy metering and billing: A smart meter accurately calculates energy consumption, taking into account varying rates and automatically bills all entities

Smart Traffic **More than 25 per cent of traffic congestion is non-recurrent, according to the US Federal Highway Administration. Instead, it is caused by traffic incidents. As a result, detecting incidents early and responding to them effectively makes for safer roads, less congestion and smoother traffic flow. The Smart City Solutions combine IP cameras, sensors, applications and the Smart City Wi-Fi infrastructure to provide visibility of live traffic conditions for traffic management authorities in real time. The solution provides insight into urban traffic patterns so that traffic authorities can make better decisions and long-term plans.**

	City Benefits	Solution Features
	<ul style="list-style-type: none"> More efficient traffic flow Less pollution and other environmental impacts More efficient use of budget Better visibility into traffic conditions Better infrastructure investments 	<ul style="list-style-type: none"> Traffic Monitoring: View colour-coded, live traffic conditions on a map, including overlays of camera feeds. Prioritise camera feeds based on high-incident areas. Make it easier for citizens to report traffic hazards and incidents Incident Detection and Management: Use video feeds and analytics to verify and detect traffic incidents, traffic flows and violations. Create incident records and collect all data regarding the incident lifecycles Administration: Easily configure and manage sensors, video infrastructure and policy rules Analytics: Report traffic incident distribution over time, day and location to aid planning. Identify areas with recurring traffic and flow issues
	Transportation Department Benefits	
	<ul style="list-style-type: none"> Automated incident detection and quicker responses Better-informed operational decision-making Improved planning and resource allocation Greater collaboration among response Agencies More effective operations 	
	Citizen Benefits	
	<ul style="list-style-type: none"> Improved road safety Less congestion, reducing frustration and fuel costs Better driving and commuting experiences 	

Conclusion

Governments all over the world are facing increasing budget constraints. At the same time, agglomeration of urban clusters and evolution of urban habitats are irreversible and there is a clear mandate now on public sector leaders to provide smart city services to ensure that the citizens receive the service at the right

place, at the right time and at the right cost. Citizens continue to expect same or higher level of services pertaining to their various needs, such as taxation advice, legal advice, social security queries, disability payments, pensions etc. Network is at the centre of this evolution and Smart City Solutions are here to transform. **DSA**



CYBER SECURITY OF DIGITAL INDIA

Indian organisations have not paid adequate attention towards cyber security. The widespread absence of even the most routine security tools and policies has left many Indian organisations vulnerable to serious cyber-attacks and the inevitable financial losses that follow ... Although spying has been an accepted part of statecraft for centuries, digital era is termed as the golden age for spying.

On 31st July 2015, Prime Minister Modi launched the flagship programme 'Digital India' with the vision to transform India into a digitally empowered society and knowledge economy. Recently he had also shared his vision of building 'Smart Cities' in India and Union Cabinet has already approved the 'Smart Cities Mission', with an outlay of ₹ 48,000 crore, under which 100 new 'Smart Cities' would be developed to promote efficient use of public resources and enhance the quality of urban life. The vital components of Smart Cities and Digital India would necessarily be highly dependent on digitally interconnected, interdependent and complex

Critical Information Infrastructure (CII), which may become highly vulnerable to cybercrime and cyber-terrorism, if not protected adequately. In such an India cyber security would become an integral and important subset of national security.

March Towards Digital India

India is already on the path of becoming a digital nation. There are more than 900 million mobile users and 200 million Internet subscribers in India. According to 'India@Digital.Bharat' report of The Boston Consulting Group, by 2018 there will be 550 million Internet users in the country, most of whom will be rural, older, more gender-equal, more mobile and more vernacular than

their counterparts of today. We have a booming market for BPO and IT/IT Enabled services, which is likely to reach US\$ 300 billion by 2020. E-Governance, Mobile Governance and E-Commerce are likely to get a big boost under the Digital India programme. Riding on the Information and Communication Technology (ICT) backbones, private companies, government institutes, organisations and citizens in Digital India will be using computers, computer networks and smart phones like never before. Vital sectors of our economy such as power, communication, transportation, Internet backbones, finance, health, defence, space, critical manufacturing, emergency response etc are also embracing ICT in a big way, thereby increasing their digital dependence. These Critical Information Infrastructures (CII) are increasingly becoming highly complex, distributed, interconnected, interdependent and heterogeneous making them highly vulnerable to cyber-attacks from cyber mercenaries, cyber-terrorists, non-state actors and hostile states. The attack vectors are becoming easily available and require minimum skill levels to operate. The cyber threat landscape is changing and expanding very fast. Digital India cannot afford to remain isolated from it.

New War Template

After land, air, sea and space, cyber has now become fifth domain of warfare and cyber-attacks on Estonia in 2007 have already heralded the era of cyber war. Estonia, one of the most wired societies in Europe and a pioneer in the implementation of E-governance, became victim of politically motivated cyber-attacks, lasting three weeks, affecting the Estonian presidency and its parliament, almost all of the country's government ministries, political parties, three of the country's six big news organisations, two of the biggest banks and firms specialising in communications. This was followed by large-scale cyber-attacks on Georgia and Lithuania in 2008. The discovery of 'Stuxnet' virus in 2010 has marked the beginning of cyber weaponisation in the world and several countries are now suspected to be pursuing it seriously. It is widely believed to have been introduced into the secured and isolated systems of Iran's Natanz nuclear facility through unauthorised malware infected ubiquitous pen drive. 'Stuxnet' was primarily designed to infect Programmable Logical Controller based Industrial Control Machines, on Windows platform, in the fuel enrichment facilities of nuclear power plants of Iran. But a large number of computers in several countries including India also got infected. This invisible virus has revealed the ugly, anonymous and devastating aspects of cyber weapons of mass disruption. In 2012 'Shamoon' virus infected 30,000 computers of State-owned Saudi Arabian firm, which produces 40 per cent of the world's crude oil, using 'Spear Phishing' email. Although spying has been an accepted part of statecraft for centuries, digital era is termed as the golden age for spying. More and

more sensitive data of individuals, organisations and nations are being stored in digital form. Snowden revelations have shown the depth and extent of mass cyber surveillance and espionage activities at global level. Hostile nations, state sponsored actors and hactivists are now actively targeting sensitive organisations for stealing information in electronic form for military, political and economic espionage. 'Flame', a complex virus, designed to take over and convert computers into spying machines, is one of the several of spyware which target and collect sensitive information from computers. Cyber terrorism is no longer a subject of academic discussion but a reality, finding a place in our Information Technology Act.

Existing Vulnerabilities

Preparedness for cyber security by Indian organisations, both in public and private sectors, is far from satisfactory and some of the recent incidents are a pointer to the level of existing vulnerabilities and gaping holes in the Indian cyber security environment.

Cybercrime in India is on the rise and Indian Computer Emergency Response Team had handled 1,30,338 cyber security breach incidents in 2014, showing increase of 81 per cent over previous year. More than 25,037 Indian websites were defaced and about 77,28,408 'Bot' infected Indian systems were tracked. These are indicators of the extent of cyber-attacks we are facing. In the year 2007, a Swedish 'ethical hacker' blogged details of e-mail accounts and passwords of several Indian Government institutions. In October, 2008, five educated cyber criminals were arrested by Noida Police when they illegally transferred ₹ 16.6 million from the bank account of victim by hacking into his Internet bank account. A major Manesar based multinational IT company had reportedly decided to shift its US\$10 million R & D facility to Australia due to an incident of data theft in electronic form, which caused it an estimated loss of ₹ 7.54 billion. Kingfisher Airlines reportedly incurred a loss of ₹ 170 million and several other airline companies suffered similar losses due to fraudulent ticket purchases from their online booking. In a globally coordinated operation, cyber criminals were able to withdraw US\$ 45 million from thousands of



Dr Muktesh Chander IPS

The writer is Special Commissioner of Police heading Delhi Traffic Police. Prior to this he was Joint Commissioner of Police, Prime Minister's Security. He is former Centre Director of Centre for Cyber Deterrence and Information Assurance in NTRC, Govt of India. He has been DIG of Police, Goa, Additional Commissioner of Police Crime and Traffic, Delhi and Inspector General of Police, Daman and Diu. He has been awarded Police Medal for Meritorious Service and President's Police Medal for Distinguished Service.

India has still not been granted a data-safe nation status by European Union



ATMs using credit card data obtained by hacking into the two card processing companies based in India. According to a report, commissioned by Delhi High Court, cybercrimes had cost India about ₹ 24,630 crore in 2013 alone. These are few examples to show that Indian organisations have not paid adequate attention towards cyber security. The widespread absence of even the most routine security tools and policies has left many Indian organisations vulnerable to serious cyber-attacks and the inevitable financial losses that follow.

There has been a history of cyber skirmishes between hackers of India and several other countries.

related sections, such as definition of cyber security, CII, cyber terrorism and its punishment, monitoring and collection of data to enhance cyber security, role of Computer Emergency Team and nodal agency for the protection of CII etc were later added in its amendment in 2008 and several rules have since been framed under this Act. ISO 27001 also finds mention in Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011. India announced National Cyber Security Policy in 2013 with a mission to protect information and information infrastructure in cyberspace, build capabilities to prevent and

Privacy and Data Security Framework. There are still serious gaps in our cyber security framework such as ambiguity about the role of multiplicity of Agencies, lack of comprehensive cyber security law, absence of mandatory cyber security compliance regime, declaration of protected systems under Section 70 of IT Act, insufficient involvement of private sector and academia in cyber security programmes, absence of a nationwide cyber security awareness and culture, inadequate funding of cyber security functions, insufficient preparedness of police forces to detect, investigate and prosecute cybercrimes, almost negligible cyber intelligence, shortage of skilled cyber security professionals, inadequate development of indigenous hardware and software etc.

is also a need to formulate sector specific cyber security guidelines, make cyber security breach disclosure mandatory, nominate and empower Chief Information Security Officer in all critical sectors, evaluate the cyber security compliance of critical sectors regularly, increase multi-disciplinary research and development in the field of indigenous hardware/software and encryption algorithms, education/awareness and capacity building of all stakeholders in critical sectors.

From IT Power To Cyber Power

India has already shown its IT power to the entire world. However when it comes to protection, we have a long way to go. India has still not been granted a data-safe nation status by European Union. We have a huge deficit of cyber security professionals, which is likely to increase in future as the demand is expected to grow exponentially. As India marches ahead on its digital journey, we need to bridge the gap from being an IT power to cyber power. This not only means defending our cyber space, being resistant and resilient to cyber-attacks but also being deterrent. Cyber space

While walking the path towards Digital India we must transform India from IT power to cyber power

has already emerged as a global common but it is still very early to expect any evolution of norms of conduct by nation states in it. Westphalian model of sovereignty is in its infant shape. Given the complex and amorphous nature of cyber space and absence of even a global treaty under UN umbrella to deal with cybercrimes, it may not become a reality soon, notwithstanding that cyber arms race has already begun. International Group of

Experts has come out with 'Tallinn Manual' which deals with the international law applicable to cyber warfare but it is only a theoretical exercise.

Cyber security is now an integral part of national security in any digital nation and needs proportional importance attached to it. Establishment of a Cyber Command by USA, Israel, Korea, Iran and some other countries clearly demonstrates their resolve to become cyber powers. India also needs to create a unified cyber command to defend its cyber space by removing ambiguous role of multiple organisations handling cyber security. We may also establish Centre of Excellence for Cyber Defence similar to NATO 'Cooperative Cyber Defence Centre of Excellence' based in Tallinn, Estonia. In order to build a secure and resilient cyberspace for citizens, businesses and government, we need to articulate our cyber defence policy in clear terms as we have done in respect to our nuclear capabilities. It requires a paradigm shift in our approach to deal with the dynamic cyber security challenges. We need not wait for a 26/11 type attack on our cyber space to proceed proactively in the direction of developing defensive and offensive capabilities to deal with cyber threats. While walking the path towards Digital India we must also transform India from IT power to cyber power. **DSA**



Use of unsecured Wi-Fi networks, to send terror E-mails by Indian Mujahideen operatives and other groups after blasts in Delhi, Ahmedabad, Jaipur, Varanasi etc has once again highlighted cyber vulnerability exploitation. Top ranking officers in several sensitive government organisations are constantly under 'Spear Phishing' attacks emanating from advanced persistent threats resulting in loss of sensitive information.

Cyber Security Framework In India

The Information Technology Act came into existence in 2002 but largely it was an Act to facilitate and enable E-Commerce although it contained few provisions to deal with cybercrimes also. A number of cyber security

respond to cyber threats, reduce vulnerabilities and minimise damage from cyber incidents through a combination of institutional structures, people, processes, technology and cooperation. A number of Agencies are involved in implementation of this policy. State police and other law enforcement Agencies to deal with cybercrimes, Computer Emergency Team to deal with cyber security incidents, National Critical Information Infrastructure Protection Centre for the protection of CII, Cyber Security Coordinator, National Security Council Secretariat, Intelligence Bureau and various intelligence Agencies, Ministry of Home Affairs and Department of Electronics and Information Technology are involved in cyber security functions etc. In the private sector Data Security Council of India has come up with its own

Protecting Critical Information

National Critical Information Infrastructure Protection Centre has now been established under section 70A of the IT Act and rules regarding its functioning have also been notified. Its vision is to ensure safe, secure and resilient information infrastructure for critical sectors of our economy, national security, public health and safety. It has also issued guidelines for protection of CII in India which need to be made mandatory for all critical sectors both in government and private sectors. The strategy for the protection of CII must be prediction, prevention and early warning, detection and mitigation of cyber-attacks. In case of an attack, quick and coordinated response to ensure early recovery and increasing resilience are required. This is possible by establishing a National Cyber Security Operation Centre to monitor cyber threats to our critical networks on a 24x7 basis. There



IN TRANSITIONAL STAGE

The length, physical conformation and large unpopulated stretches of the Indian coastline make coastal security an extremely challenging task. Addressing the vulnerability of our coastal defences is the need of the hour. The Navy and the Coast Guard are reorienting themselves towards establishing a credible capability.

India has a coastline of 7,516 km. Of this over 5,400 km is along the mainland and 2,200 km is along the strategically located and extremely vulnerable island territories, 572 islands in the Andaman and Nicobar group in the east and 27 islands of the Lakshadweep group in the west. The topography of the Indian coastline with a plethora of creeks, rivulets, landing points, bays, sandbars and forested land make this an ideal haven for clandestine activities.

The strategic vulnerability of India's vast and porous coastline was cruelly exposed on the night of 26 November 2008. Ten men in a fishing boat were able to penetrate India's layered coastal defences and enter its financial capital through a popular entry point teeming with people and wreak havoc in space of a few hours. The swiftness and precision of the attack laid bare the inadequacy of the establishment's coastal security structure.

This was not the first time that the country's coastline had been breached with impunity. On 12 March 1993, the serial bomb blasts in Mumbai which targeted commercial centres like the Bombay Stock Exchange and led to over 250 deaths and more than 700 injured had been executed with explosives smuggled in through the Raigad coast in Maharashtra. There was much talk of strengthening the country's coastal security apparatus even then. Initiatives like Operation Swan were launched to carry out patrolling but a comprehensive review was not undertaken; no long-term measures were introduced towards ensuring a more robust defence of entire coastline.

The security threat is not restricted only to the physical coastline. Maritime boundaries extend beyond the coast and our area of concern should be the entire 2 million odd sq km of the Exclusive Economic Zone. A major part of our indigenous energy requirement is met from the offshore

installations on the western and eastern seaboard and some of our most vital infrastructure including atomic power stations, large refineries and shipyards are located along the coast. Over 90% (by volume) and 77% (by value) of India's trade passes through the 13 major and 187 non-major ports, all of which are susceptible to a seaborne threat which could have devastating economic consequences. This vulnerability would fit perfectly into the plans of any force inimical to our national interests.

Robust Mechanism

Subsequent to the successful Kargil operation of 1999, a review of the Indian security establishment was undertaken by a group of experts. A Group of Ministers was then constituted to suggest and implement the recommendations with the aim of making the security apparatus relevant to the contemporary threat scenario. This included a detailed review of Border Management including the coastal boundaries. However the apathy in implementation of the recommendations got further highlighted as a number of measures implemented post the Mumbai carnage of 26/11 had been recommended in 2001 itself.

The 26/11 attacks were a rude wake-up call to the nation and the government. It was the sheer audacity and ferocity of the attack that led to a review of coastal security at the national level. For perhaps the first time all stakeholders were sought to be integrated into the security architecture which inter-alia included various Agencies like the Navy, the Coast Guard, the Police, Customs, the Border Security Force, the fishing community etc.

The Cabinet Committee on Security (CCS), the highest decision-making body in the land on issues of national security has issued various directives to address this core threat to the nation's territorial integrity. This includes the setting up of a multilayered arrangement for enhancing adequate depth in surveillance capability. While this was also recommended in 2001, the difference this time around is the resolve to ensure implementation. In addition to the organisational changes, it was the allocation of budgetary resources and the financial commitment coupled with a phased procurement plan which indicated the seriousness being accorded to coastal security.

At the apex level the National Committee for Strengthening Maritime and Coastal Security against threats from the sea (NCSMCS), headed by the Cabinet Secretary, coordinates all matters related to Maritime and Coastal Security. This apex committee is represented by the Director General, ICG along with heads of other stakeholders.

The ICG's five year Development Plan was approved for the period 2012-17 concurrent with the national 12th Five Year Plan with allocation of over ₹ 16,000 crore, more than 2/3rd of which is for capital procurement. This would enable the ICG to reduce its current capability deficit with the induction of

modern surface and air platforms. The entire coastal security plan is to be implemented in two phases. The first phase is well underway and Phase 2 is running concurrent with the national 12th Five Year Plan.

A supplemental scheme called 'Coastal Security Scheme' is under implementation in the nine coastal States and four coastal Union Territories (UTs) since 2005 for strengthening infrastructure for coastal patrolling and surveillance. Under the scheme, assistance has been/is being given to all the coastal States of Gujarat, Maharashtra, Goa, Karnataka, Kerala, Tamil Nadu, Andhra Pradesh, Orissa and West Bengal and the Union Territories of Daman and Diu, Lakshadweep, Puducherry and Andaman and Nicobar Islands to set up 73 coastal police stations, 97 check posts, 58 outposts and 30 operational barracks and to equip them with 204 boats, 153 jeeps and 312 motorcycles for mobility on the coast and in close coastal waters.

Based on the inputs/proposals received from ICG and the coastal States/UTs, Phase-II of the Coastal Security Scheme has been formulated and approved by the Government on 24 Sep 2010. The Scheme proposed to further strengthen marine police infrastructure with additional coastal police stations, boats, vehicles, jetties etc and became operational from 2011-12. A multi-layered defence mechanism has been put in place comprising three principal layers, this delineates the areas of responsibility in geographical terms.

The Indian Coast Guard (ICG) which came into being in 1978 as India's fourth Armed Force is responsible for coordinating all coastal security activities with the Director General Indian Coast Guard (DGICG) designated as the Commander, Coastal Command. The coastal States have been mandated to draw up their own plans and dovetail these into the overall coastal security construct.

The State Governments are important stakeholders in the coastal security of their respective geographical boundaries. The Marine Police Wing is being strengthened with additional manpower, training, resources and equipment. Over 200 coastal police stations have been established and a fleet of about 400 Fast Interceptor Boats (FIBs) are at various stages of procurement.

The Customs are also an integral part of the structure and are enhancing their patrolling and investigative mechanisms with a security orientation.

The Border Security Force has a water wing, which is responsible for the creeks and waterways in Gujarat and in the Sunderbans, both of which are extremely fertile areas for harbouring anti-national elements and rampant smuggling all of which are greatly detrimental to national security.

Joint Operations Centres (JOCs), set up by the Navy as command and control hubs for coastal security at Mumbai, Visakhapatnam, Kochi and Port Blair are fully operational. These JOCs are manned 24x7 jointly by the Indian Navy and the Indian Coast Guard. Coastal patrolling by Navy, Coast Guard and Marine Police has increased sharply over the last

few years. At any given time, the entire west and east coast is under continuous surveillance by ships and aircraft of Navy and Coast Guard. As a result, potential threats have been detected and actions have been taken to mitigate the same in time.

Inter-agency coordination, between nearly 15 national and state Agencies has improved dramatically, only due to regular 'exercises' conducted by the ICG in all the coastal states. Nationwide, over 118 such 'exercises' have been conducted till date since 2008 and this has considerably strengthened the coastal security mechanism.

Coastal Surveillance

A radar network has been set up along the coast to provide complete coastal surveillance up to 25 nautical miles from the coast. Comprising 46 radars for the mainland and the islands, this network should provide near seamless coverage of the coastline akin to an Air Defence network. This would enable the movements of all vessels to be monitored electronically as well as optically. The second phase of Radar Network is on the anvil.

This network also integrates the National AIS network which can track the vessels fitted with AIS transponders (fishing vessels of 20 m and above) and is also linked to the Vessel Traffic Management Scheme (VTMS) which is operational in all major ports and harbours. A comprehensive picture of the region is generated when all components are linked to satellite monitoring/surveillance and feeds from all sources can be collated centrally through the National Command Communication Control and Intelligence network (NC3I). The Home Ministry is also in the process of installation of transponders 'free of cost' in fishing vessels below 20 metres in length for the purpose of tracking their movement up to at least the territorial waters.

As part of the effort to enhance our Maritime Domain Awareness, the National Command Communication and Intelligence Network (NC3I) has also been established. This overarching coastal security network collates data about all ships, dhows, fishing boats and all other vessels operating near our coast, from multiple technical sources including the AIS and radar chain. These inputs are fused

and analysed at the Information Management and Analysis Centre (IMAC) at Gurgaon, which disseminates this compiled Common Operating Picture for Coastal Security to all 51 nodes of the Navy and Coast Guard spread along the coast of India. A second phase of coastal radars is also being implemented to plug the small gaps in some places. This Nodal Hub for the coastal security of our country, which has been conceptualised by the Indian Navy, is a major step in the establishment of a coastal security shield along the coast.

Challenges

A 'rogue' boat entering into the Indian Maritime Boundary has brought the focus on Coastal Security Network that is undergoing major upgradation after the 26/11 Mumbai attacks. In the latest case where the Coast Guard patrol vessel managed to intercept a suspicious vessel, it was the specific intelligence input that helped in tracking the boat.

At an operational level, there has been close coordination in certain areas which has led to some success. These include the promulgation of Standard Operating Procedures, Joint Coastal Security Exercises coordinated by the Coast Guard, formation of Coordination Committees at the state and district levels under the civilian administration and the establishment of Joint Operational Centres (JOCs) at Mumbai, Visakhapatnam, Kochi and Port Blair which are essential for collation and dissemination of information and action to be taken.

The length, physical conformation and large unpopulated stretches of the Indian coastline make coastal security an extremely challenging task. The dynamics of the maritime threat scenario in our region lends itself to asymmetric warfare thus enhancing our vulnerability to forces inimical to our nation.

Addressing the vulnerability of our coastal defences is the need of the hour. The Navy and the Coast Guard are reorienting themselves towards establishing a credible capability. A comprehensive approach at the state level is however essential for ensuring a robust Coastal Security Mechanism. **DA**



ROLE AND CHALLENGES

Some major disasters in India such as Bhopal chemical accident, 1984 (3,800 people died), Latur earthquake 1993 (22,000 people died), Odisha super cyclone, 1999 (7,600 people died), Gujarat earthquake, 2001 (20,000 people died), Tsunami, 2004 (10,700 people died), Mumbai monsoon, 2005 (1,000 people died) and absence of effective mechanism to tackle such disasters led Government of India to think about an effective mechanism/setup to deal with all types of disasters.

Besides loss of human lives, properties worth crores of rupees have been destroyed/lost due to the man-made and Natural Disasters in the past. This horrific loss of human beings and material led the Government of India to form Disaster Management Act-2005, on 26th December 2005.

This Act provides for the effective management of disasters and for matters connected therewith or incidental thereto. Consequently, National Disaster Management Authority was formed in the year 2006 to supervise disasters management in India. A multi-skilled, highly professional **National Disaster Response Force** comprising of 08 Nos of Bns (02 Bn each from BSF, CRPF, ITBP and CISF) was raised

NDRF: Unique Features

NDRF is a specialist disaster response Force which has following unique features:

- Multi-disciplinary, multi-skilled, high-tech, specialist Force, capable of responding to any natural disaster or CBRN emergency
- Response time reduced to the barest minimum with the Concepts of
 - ⊙ 'Proactive availability' to states
 - ⊙ 'Pre-positioning' in threatening disaster scenario
- Single Largest Dedicated Disaster Response Force in the World, trained and equipped as per international standards
- NDRF Bns are located at 12 different places in the country based on vulnerability profile of the region
- Also, NDRF teams are placed at 23 metros /inaccessible regions in the country
- All the 10 Bns of NDRF are trained and equipped for all natural disasters as well as for CBRN emergencies
- Capable of carrying out disaster response operations within the country, in the region and at International level

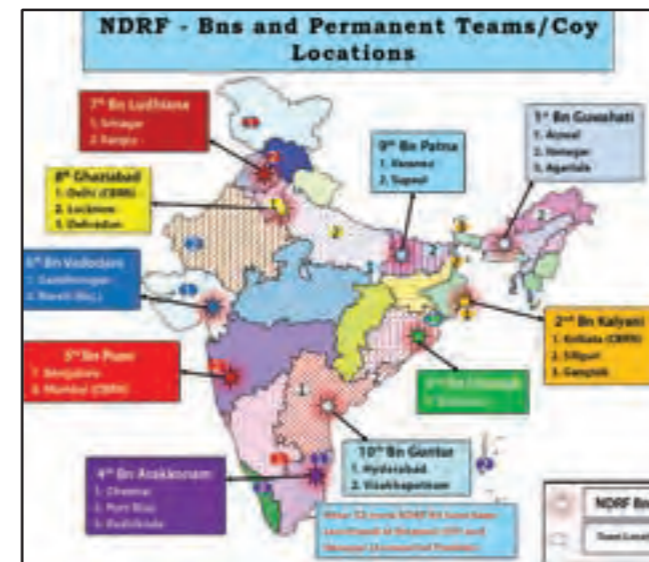
Role And Task Of NDRF

NDRF is serving the needs of all classes of people irrespective of their caste, creed or economic position. The Force is working with a great enthusiasm and courage in various fields like CBRN, Floods, Earthquakes, Cyclones, Tsunamis, Major Accidents etc. The role of NDRF is as follows:

- Provide specialised response for rescue and relief in case of natural as well as man-made disasters
- Deployment in case of impending disasters
- Assistance to civil authorities in distribution of relief material during/after disaster
- Co-ordination with other Agencies engaged in rescue/relief work

Disasters And National Security

As per Wikipedia, National Security is a concept that a government, along with its parliament(s), should protect the state and its citizens against all kind of 'national' crises through a variety of power projections, such as political power, diplomacy, economic power, military might and so on. In order to possess national security, a nation needs to possess military security, economic security, energy security, political security, environmental security, security of energy, cyber security etc. Security threats involve not only conventional foes such as other nation states



as per MHA order dated 19th January, 2006 to tackle/mitigate all types of disasters. As on date, NDRF is having strength of 10 Bns each consisting of 1,149 personnel. The Government of India has also sanctioned 02 Bns from SSB to NDRF which are under the process of the conversion/upgradation at Varanasi (UP) and Itanagar (Arunachal Pradesh).



but also non-state actors such as violent non-state actors, narcotic cartels, multinational corporations and non-governmental organisations; some authorities include natural disasters and events causing severe environmental damage in this category.

We as disaster managers should understand that the National Security is no longer about fighting forces of two enemy groups/countries and weaponry alone. The national security strategy of any country ensures the well-being and resilience of its population. But due to the numerous kinds of pressures emanating from population growth, increased demand for energy and materials and competition for access to land, water, minerals and other vital natural resources, the vitality of our ecological system is getting seriously threatened. This has resulted into changes in global climate and degradation of clean air and water, soil, forests and wetlands, all of which have the potential to compromise energy security, food security, supply chain security and other domestic and international concerns. The relentless assaults of our earthly habitat are heightening the global risks of deadly conflict. Climate change is just one of the ongoing trends increasing the chances that natural disasters and extreme environmental events will lead to social disruptions, aggressive competition for scarce resources, serious political confrontations and even war.

According to the 2005 Millennium Ecosystem Assessment, future global ecosystems will be under even greater pressure when by 2050 global population will reach about 9 billion, some 30% higher than the 2000 population. Poverty alleviation and rising affluence in developing nations like India will inevitably increase the demand for natural resources. The essence of global and regional security is acquisition of economic well-being and social justice for all. Hence, the challenge ahead is to create global conditions that foster economic growth and human well-being in a sustainable manner. How can society address these growing social and environmental pressures in ways that sustain economic growth, assure an adequate supply of natural resources, protect human health and safety and avoid domestic and international conflicts?

Challenges Imposed By Disasters

Natural hazards are the natural physical phenomena that have the potential of adversely affecting humans and their societies. At present, half of the world's population is already twentyfive years old or younger. Projections suggest that, by 2030, the world will need to provide 50% more food and additional fresh water. The challenge is to envision plausible threats and sequential patterns of potential danger – not to scare people but to anticipate potential consequences and devise strategies to prevent or reduce economic, political and social damage.

Natural disasters and extreme environmental events are expected to increase in number and

severity on a global scale, elevating levels of economic, social and political stress that could provoke both civil and international conflicts. Instead, most discussions of natural disasters are largely limited to a 'humanitarian' focus on the most direct impacts. Severity is measured by deaths, destruction, dislocation and disease in the immediate area. But with the increased inter-dependence of the global economy and of global markets and supply chains for food, petroleum and industrial components, we face the potential for major impacts on much wider populations. It is given below:

- Due to increase in the frequency of the natural disasters, would adversely affect the major essential needs such as food, water, land, medicine, energy or subsistence income. An overlapping series of earthquakes, floods and food shortages affecting a megacity could overwhelm the capacity of national and international Agencies to respond adequately. Hence, economy of any country would be adversely affected
- Transportation and communication infrastructures, though widely distributed on a global basis, nevertheless have the features of major arteries and hubs that make them vulnerable to regional or even global disruptions
- Ecologically induced disasters for example the Fukushima nuclear meltdown, led both the Japanese and German governments to announce the phasing out of their nuclear power industries – a major blow to any prospect of curbing global carbon emissions
- Disruptive disasters in major food-producing regions could have dire global consequences. Corn, wheat and rice crop failures would lead to price hikes and shortages in far-flung locations
- Natural disasters can lead to export cut-offs, stockpiling and hoarding, or cartelised supply arrangements. Such developments could create new zones of instability, hostility and populist pretexts for aggressive steps to secure new supplies or assure future access
- Water shortages could be another cause of future conflicts. The peaceful resolution of few disputes over severe water shortages could be very difficult in future
- Medicine can be another life-and-death necessity in times of emergency. It is not difficult to imagine that the government of a state facing the prospect of a deadly epidemic would take steps to seize or intercept supplies of essential medicines. A global pandemic from that virus or a similar microorganism could lead to travel restrictions, news blackouts and other isolationist reactions, but also to more aggressive measures to obtain life-saving medicine
- Natural disasters can also sever transportation and communication links and global supply chains – lifelines for necessities – compounding the catastrophe where the disaster occurs and affecting employment even in distant locations
- Volcanic ash cloud from Iceland in 2010 halted European air traffic for only a week or so but even then had significant effects on both business and tourism

- Major disasters can have social consequences when the intense stress of damage and recovery causes breaks along ethnic, religious, class or geographic fault lines. A major earthquake in a megacity could produce violent confrontations among groups competing for scarce relief supplies and recovery assistance. Or the disaster might create reverse-urbanisation pressures for millions of homeless and jobless people in suddenly uninhabitable slums
- Sudden large-scale migrations are an increasing prospect among the effects of climate change. Low-lying islands, flood-prone coastal areas, large refugee camps and regions of prolonged drought could provoke major population movements. The possibility of Bangladeshis pouring into India to escape delta flooding has already led the Indian government to construct a 4,000-kilometer fence to forestall such influx. Within the continent, such forced movement could compound urbanisation trends. Such cataclysms are unlikely to occur without violence
- Natural disasters can dramatically expose deep social inequities and government indifference or incompetence, fomenting opposition movements
- An earthquake in Karachi or Delhi or a major flood in Mumbai could cripple the economies of their respective countries and further degrade the effectiveness of government authorities to avoid serious ethnic, sectarian or even international conflicts.

Preparedness Of NDRF

In view of the threat of natural disasters which have potential to threaten the National Security, reduction of the direct harm of such disasters will require initiatives in three areas: increasing local resilience, improving relief capabilities, and where unavoidable, facilitating relocation from the most vulnerable areas. In order to meet these requirements, NDRF has greater role to play as a dedicated disaster response Force of the Nation.

Major Contribution Of NDRF

In the field of Humanitarian Assistance and Disaster Relief (HADR), teams of NDRF have been doing outstanding job, not only within the country but abroad also. Over the years, NDRF has not only become the most visible face of the Government of India but has also acquired the image of being a truly specialist response force to deal with any natural disaster and CBRN emergencies. The response time of this force has been reduced to the barest minimum on account of the concept of 'proactive' availability of this Force to the states and also the concept of pre-positioning the Force in threatening disaster scenario. The NDRF is being increasingly requisitioned by the states for rescue and relief operations in floods, cyclones, landslides, train accidents and chemical leakage etc. So far NDRF has saved 4.5 lakh human lives and recovered 2,132 dead bodies.

The performance of NDRF in efficient discharge of HADR operations was highly appreciated by Government of India as well as by the International

Community. Since its inception, NDRF has very effectively handled major disasters such as Kosi Flood, Cyclone Phailin, J&K Urban Flood, Cyclone Hudhud etc.

Japan's Earthquake In Tohoku


On 11th March, 2011, Japan was struck by triple disaster (earthquake, tsunami and nuclear leakage) of unprecedented scale in Tohoku region. One team of 46 members was despatched for providing assistance to Japan in Onagawa, Japan. The team worked in sub-zero temperature, they recovered 7 dead bodies and Japanese currency worth fifty million yen. NDRF's exemplary dedication and compassion was widely appreciated by the Japanese Government, people, media and most importantly by Hon'ble Prime Ministers of both the countries.

Nepal Earthquake

On Saturday 25 April 2015 at 11.56 hrs, a massive 7.8 magnitude earthquake struck Nepal. Nepal's major cities, including the capital Kathmandu, were badly damaged. NDRF despatched its 16 teams which rescued 11 live persons and retrieved 133 dead bodies from the debris. Medical component of the NDRF provided medical assistance to 1,219 persons. NDRF teams were the first foreign teams which arrived at the earthquake stricken areas within 5 hours after occurrence of the earthquake. More than 8,000 people died in this earthquake.

Conclusion

Considering the large size and high vulnerability of India to natural and man-made disasters, NDRF is highly concerned about the capacity building of all the State Response Agencies particularly SDRF, Local Police, Civil Defence and Home Guards and Fire Services to train them adequately to meet any major challenge.

Public education and awareness on disaster risks /hazards has increased tremendously in the recent times. This has often spurred populations in highly at-risk communities to embark on community-based Disaster Risk Reduction activities such as community and inter-community sensitisation programmes, general cleanings etc. Several target-specific trainings have and are being conducted at national and local levels to educated leaders /stakeholders and communities on disaster risks, vulnerabilities and capacities. There is strong and regular engagement of the media (both print and electronics) for publications and broadcasting on DRR and DRM issues nationwide. In the holistic approach of disaster management inclusive of all factors which would be indirectly affecting National Security needs to be given animated attention by all the stakeholders. The contribution of the NDRF in strengthening the Nation's Security shall remain the most significant agenda. 

VULNERABILITIES GALORE

It should be abundantly clear by now that the Pakistan Army Inter-Services Intelligence is trying to create conditions whereby it can intervene directly in Jammu and Kashmir ostensibly at the invitation of Kashmiri militant groups. Duktaran-e-Millat chief Andrabi addressing the Lashkar-e-Toiba/Jamaat-ud-Dawa meeting via telephone is a grim pointer. A Liberation Army is in the making.

Are we safe? The series of attacks by Pakistan along the International Border and the Line of Control; the attacks by the several Naga factions across as broad a frontage as Arunachal Pradesh and Manipur in the Northeast; the unabashed manner in which Chinese troops come and kick down makeshift sheds set up by our nomadic herdsmen in the Ladakh sector of the Line of Actual Control in the northern Himalayas bespeak of a nation low in the regional pecking order. Anyone who wants to, can come and assault us at any time with ease and elan (a televised Press conference for the Pakistani terrorist Naved after he was captured in Udhampur; "I came to kill Hindus, its fun", he said) at any place of their choosing.

Cluelessness

In the series of attacks in the past one year there have been many occasions when our security forces were unable to even pinpoint the point of entry (ingress) of the terrorists. Such cluelessness is the result of absence of personnel and technical means of detection of intruders and a standard operating drill for interception and elimination at the boundary itself instead of deep inside our territory. The areas that are difficult to patrol are known but given the ease with which recent intrusions have taken place shows up an element of carelessness and criminal neglect.

All this has a genesis in the first tenure of the NDA government under Prime Minister Atal Behari Vajpayee. A former Chief of Army Staff, keen to curry favour with the government, decided not to make the usual annual recruitment of about 50,000 new entrants to replace those who retire every year or opt out prematurely. This happened around 1998 when the NDA government decided that the time was appropriate to force Pakistan to bring into the open its bomb-in-the-basement

project and expose the decades long camouflage and subterfuge of China and the US governments. The Government of India failed to understand and prepare for the psychological impact of the series of nuclear tests by both India and Pakistan. For Pakistan it was opportunity to use Fourth Generation Warfare against India from behind its newly-demonstrated nuclear shield. It had already 'softened up' the Drass portion of the Kargil salient by daylong bombardment to keep the Shia Muslim herdsmen indoors and prevent them from detecting movement of troops and munitions and reporting it to the Indian security forces.

Manpower Mismanagement

Short of manpower, India resorted to the usual ploy of withdrawing its troops from higher reaches of the Kargil salient during the winter months. What was projected to be a very difficult mission for Indian troops (to defend the heights in winter) became a moment of opportunity for the Pakistan Army Chief Pervez Musharraf. The rest is well-understood contemporary history. The lesson in it for India was: Not to withdraw troops in winter from the Himalayan heights. It dampened the enthusiasm of those who were ardently advocating a withdrawal of Indian troops from Siachen which was occupied in 1984 when it was discovered that Pakistan was preparing to occupy it under the camouflage of a mountaineering expedition. India pre-empted that. It also brought forth a requisition for raising a new Mountain Strike Corps to defend the Northeast against Chinese machinations and avoid the need to transfer acclimatised troops from one sector to another in the difficult terrain of the Himalayas. It is clear that India needs more manpower to be able to deal more effectively and efficiently with the threats from across its western, northern and eastern borders.

The attempt to 'save money for modernisation' in 1998-99 had a negative cascading effect down the chain of command. Problems posed by non-grant of leave and other personnel matters led to suicides and homicides in the battalions forcing an intervention by the Defence Institute of Psychological Research for remedial action. The attempt to save money to the detriment of national security is being taken to absurd levels as is apparent in the reduction of the manpower strength of the proposed Mountain Strike Corps from 80,000 plus to half. The result will continue to be that we will not have enough manpower to stop the Chinese troops from interfering with our defensive systems (they smashed our camera and returned it to us) and are preventing our herdsmen from visiting traditional pasture lands in the Aksai Chin salient. The result is a creeping territorial aggrandisement or 'salami slicing' by the Chinese People's Liberation Army. Simultaneously, by one estimate 9,000 Chinese troops disguised as engineers and technicians are posted in Pakistan-occupied Kashmir in a manner that allows the Pakistan Army a free hand to conduct its Fourth Generation Warfare against India using jihadi terrorists as the first echelon backed by the regular army with rifle and mortar fire support.

The OROP Conundrum

The Finance Ministry has indicated that there are not enough funds to raise a full-strength Mountain Strike Corps after raising doubts for the need for such a raising. Presumably, that is also the reason why the Government of India has been deliberately opaque over the issue of redeeming its pledge on the One Rank, One Pension proposal. To deflect the ire of the ex-Servicemen the NDA Government should announce a date for the implementation of the OROP with the unambiguous rider that the first priority would be to ensure a modicum of defensive capability against the Chinese in Arunachal Pradesh and finance would first be allocated for the raising of the full-strength Mountain Strike Corps. Hopefully the ex-Servicemen will agree to putting national security foremost, knowing that OROP will become a reality after the nation is safer. The Government needs to be more circumspect in making promises it cannot keep. Pandering to vote bank politics in national security is fraught with as yet unknown dangers. Talks of politicisation of the military are irrelevant now that the ex-Servicemen have threatened to 'show the Government' what can be done in the forthcoming Bihar elections.

Securing The Western Theatre

By any assessment the more important requirement is the shoring up of defences along the International Border and the Line of Control where they converge at the 'chicken's neck' connecting Punjab's Gurdaspur district with the Udhampur district of Jammu and Kashmir. During the course of the ceasefire violations Pakistan has managed to push in several small modules of 3-4 highly trained terrorists capable not just in close combat but also setting up boobytraps and improvised explosive devices as seen in the

recovery of bombs attached to the railway line that links Punjab to J&K. The political situation is dicey. When the Gurdaspur intrusion occurred there were fears of a revival of the Sikh Khalistan movement which Police chiefs KPS Gill and Julio Ribeiro managed to contain and eliminate. Pakistan is using all assets at its disposal and it is not surprising that it would encourage the Lashkar-e-Toiba to forge links with the Babbar Khalsa and other terror groups operating from as far away as the US and Australia (The US recently took umbrage at the treatment of a Khalistani adherent who is now a US citizen).

However, the more urgent requirement is to be able to stop intrusions at the IB and the LoC itself. It makes little sense if we are able to elicit support from UAE and other neighbours against terrorism when we are unable to defend ourselves by our own means. The objective of the Pak-China collusive intent is seen in the introduction of a new type of bullet that is armour piercing and anti-material. An injured border guard would set off a process of medical evacuation that would divert attention from the intrusion effort and make things easier for the intruders.

Innovative Defence

Admittedly, there are areas along the Line of Control in particular that are extremely difficult to guard.

Counter-terrorism, like counter-insurgency, is a manpower-intensive operation. Not all the work is done by men in uniform. The local civilian population is a force multiplier as the men who captured the Pakistani terrorist Naved have proved. However, the most effective means is a presence either human or technical at any point known to be vulnerable to penetration. To aid and improve the capabilities of the human guards **DSA** had some years ago suggested raising of a larger number of military dogs. The current regenerative capacity of about 250 dogs per year is totally inadequate. Learning from experience the accent should shift to the development of dogs trained to attack intruders on command. The Chinese have learned this lesson well after the beating they received at Nathu La in 1967. They have included these military dogs in their forward patrols along the Line of Actual Control.

It should be abundantly clear by now that the Pakistan Army Inter-Services Intelligence is trying to create conditions whereby it can intervene directly in Jammu and Kashmir ostensibly at the invitation of Kashmiri militant groups. Duktaran-e-Millat chief Andrabi addressing the Lashkar-e-Toiba /Jamaat-ud-Dawa meeting via telephone is a grim pointer. A Liberation Army is in the making. **DA**



Cecil Victor

The writer has covered all wars with Pakistan as War Correspondent and reported from the conflict zones in Vietnam, Laos and Cambodia in South East Asia as well as from Afghanistan. He is author of *India: The Security Dilemma*.

The more urgent requirement is to be able to stop intrusions at the IB and the LoC itself



ROLE AND CHALLENGES

In the wake of the Chinese conflict in 1962, it was felt that weapons alone could not protect the country's borders. The active backing and resolute will of a committed border population was imperative to ensure that the enemy was kept at bay. A need was felt for the creation of an unconventional, unique and specialised organisation which would function in the far flung, vulnerable, strategic, remote, climatically and topographically difficult border areas and motivate the border population across several states towards the cause of protecting our national sovereignty. The SSB (Special Service Bureau) was thus, created in March, 1963 with the objective of achieving 'Total security preparedness' in the remote border areas for performing a 'stay-behind' role in the event of a war. It was started in North Assam, North Bengal, hill districts of Uttar Pradesh (now Uttarakhand), Himachal Pradesh, parts of Punjab and Ladakh area of J&K. Later its jurisdiction was extended to Manipur, Tripura, Jammu (1965), Meghalaya (1975), Sikkim (1976), Rajasthan (1985), South Bengal, Nagaland and Mizoram (1989) and its area of coverage included 15 states. SSB in its erstwhile role was covering a population of more than 5.73 crore living in about 80,000 villages and about 9,917 km of India's international borders. The main thrust of the SSB was on generating a sense of national belonging, security and culture of vigilance in the border population. The SSB trained more than two lakh volunteers who served as the eyes and ears of the organisation.

The area covered by SSB comprised 10 SSB Divisions, 49 Areas, 117 Sub-areas and 287 Circles. It had 32 Group Centres, 14 Training Centres and 3 Storage

Depots. Training Schools were set up in various parts of the country starting with Frontier Administrative Officer's Training Centre at Mahabaleshwar in October, 1963. Besides, the Group Leaders Training School was opened in Gwaldam (then UP now Uttarakhand). Two Advanced Training Schools were started for volunteers in Sarahan (HP) and Haflong (Assam). By 1990, SSB had seven Major Training Centres and seven Women's Advanced Training Schools. Training was imparted to the local population in the border areas of HP, Punjab, parts of J&K, UP, North Assam, North Bengal and South Bengal and NEFA region.

The resources of the Central Government and State Government were pooled and efforts were made through SSB to improve the lot of the border population who came out in large numbers to repair roads, bridges and drains, clean up tanks and wells, lay water supply lines and build public toilets, sports grounds, school buildings, community centres etc. SSB personnel took this scheme to the villagers' doorsteps. They used tape recorders, 16 mm film projectors and gramophones to educate and motivate. They lived with the villagers and addressed their day-to-day issues. Need for unity and integrated action was emphasised. Economic development of the regions was attempted. Villagers were trained in the use of small arms and the art of self-defence to inculcate a spirit of resistance in them. SSB's efforts bore fruit slowly but steadily. A large number of women volunteers were trained and this augmented the SSB's endeavours greatly. In 1965, SSB undertook the task of providing medical support in the border areas where primary health

centres were largely non-existent. This move turned the tide in favour of the Government as the border population felt they had much to gain from being a part and parcel of the Indian Union. By 1998, SSB medical staff were treating an average of 16 lakh patients every year. In the year 1989, SSB augmented its services through a veterinary support system for the border population wholly dependent on cattle and livestock for their livelihood. SSB veterinary staff provided free veterinary healthcare to as many as 5 lakh livestock every year by organising camps in far-flung border villages. SSB played both its overt and covert roles in an exemplary manner and grew in strength as a people's force, guided by its motto of 'Service, Security and Brotherhood'. When epidemics or disasters struck in the form of earthquakes, cloudbursts, floods or landslides, we were the first to go to the rescue of the border population. SSB can claim to be the first Force to take on empowerment and emancipation of women by conducting weapon training, awareness generation programmes and skill development courses to enable them to become self-reliant. SSB also enriched the social fabric, embellished the secular milieu of the nation and rejuvenated dying arts in all the areas we worked. In fact, the spread of Hindi in Arunachal Pradesh is credited to SSB. By our work and efforts we retrained many youngsters from not only falling into the hands of fissiparous elements but also from falling prey to drugs and bad habits.

Border Guarding Force

After the Kargil War, the K Subrahmanyam Committee's Report was considered by a Group of Ministers for relocation of all Paramilitary Forces to achieve optimum efficiency by assigning one border for each Force. SSB was declared as a Border Guarding Force in 2001 under the Ministry of Home Affairs and renamed as 'Sashastra Seema Bal' in 2003. On June 19, 2001, SSB was mandated to guard Indo-Nepal Border (1,751 km) and was declared the Lead Intelligence Agency for Indo-Nepal border. SSB was given the added responsibility of guarding Indo-Bhutan border (699 km) and declared the Lead Intelligence Agency for Indo-Bhutan border wef March 12, 2004. The greatest moment of pride for the Organisation came on March 27, 2004 when it was awarded the President's Colour. SSB is now spread along the International border across Uttarakhand, UP, Bihar, West Bengal, Sikkim, Assam and Arunachal Pradesh. SSB's charter of duties now comprises:

- To promote a sense of security among the people living in the border areas
- To prevent transborder crime, unauthorised entry into or exits from the territory of India
- To prevent smuggling and any other illegal activities

Strength

As on date, SSB has 63 battalions which are fully operational and are performing the mandated duties of SSB including IS, CI (Ops), LWE, L&O and other security duties in addition to 06 battalions under raising.

Besides, 25 Area and 55 Sub-area Offices consisting of 2,168 civilians comprising the Area wing are deployed along Indo-Nepal and Indo Bhutan borders to conduct perception management programmes and collect intelligence. The strength of the Force as on date is 76,337 and at the completion of raising will rise to 91,405.

Structure

SSB is headed by a Director General, BD Sharma who oversees 06 Frontier Hqr at Guwahati, Tezpur, Siliguri, Patna, Lucknow and Ranikhet each headed by an Inspector General, 18 Sector Hqrs headed respectively by DIGs and 73 Battalions with coterminous areas for its operational activity.

Deployment

A total of 45 battalions are at present deployed on Indo-Nepal and Indo-Bhutan Borders. In order to secure the Indo-Nepal border total 471 Border Out Posts (BOPs) have been established. A total of 152 BOPs have been established on the Indo-Bhutan border. Five Battalions are deployed in J&K State for Internal Security duty and Seven Battalions are deployed in LWE areas of Bihar, Jharkhand and Chhattisgarh States. Apart from the above, two Battalions have been transferred to the National Disaster Response Force. A total of 29 Coys are temporarily deployed for IS/L&O duties in the State of Assam.

Achievements

After the deployment of SSB on Indo-Nepal and Indo-Bhutan borders the smuggling and anti-national activities have been controlled considerably. During the year 2013, SSB made seizures of narcotics, Fake Indian Currency Notes (FICNs), wild life produce, forest produce and contraband items etc worth ₹ 113.45 crore and arrested 885 criminals. In the year 2014, seizures were made worth ₹ 126.88 crore and arrested 2,362 criminals. During the current year-2015 (June), total seizures worth ₹ 78.50 crore were made with the arrest of 1,502 criminals. After the devastating earthquake in Nepal the human trafficking from Nepal has seemingly increased. SSB has rescued 357 victims and arrested 82 traffickers from Indo-Nepal border in course of last four months. Thirtytwo (32) victims were rescued and 15 traffickers were arrested from Indo-Bhutan border.

New Initiatives

Some of the new initiatives taken by the Sashastra Seema Bal are as follows:

- SSB has introduced and implemented the concept of plain-clothed 'Border Interaction Teams' on authorised check posts on the border. Keeping in view the friendly relations with Nepal and Bhutan these interaction teams, which include women personnel, are initially deployed at nine crossing points on Indo-Nepal and Indo-Bhutan borders, to reflect the people friendly face of the Force. These men and women personnel have been trained in soft skills in addition to border security related skills. They have made significant achievements in various fields
- A four digit Toll Free No 1903 has been introduced for use by general public in order to communicate

information on anti-national elements as well as to report on corruption and assist the SSB in its role in ensuring national security

- A proposal for holding Joint Ops Exercises between SSB and Armed Police Force, Nepal as well as SSB and Royal Bhutan Police (RBP) once a year has been submitted to MHA with a request to take up the matter with Royal Government of Bhutan (RGoB) at appropriate level for approval. Similar proposal for holding joint exercises between SSB and Nepal Armed Police (NAP) has been submitted to MHA

- Nine Mobile Medicine and Ambulance Services have been placed on specified border points for providing 24x7 services to border people including Nepalese citizens

- SSB is providing Free Cleft Lip and Cleft Palate Surgery for border population in collaboration with 'Darpan-Smile Train'. In all, so far, 80 people have successfully undergone Cleft Lip and Cleft Palate surgery free of cost

- SSB has taken the initiative to promote Central Government schemes in the border areas. Every Company of each of the Border deployed battalions of SSB has adopted one school each totalling to 309 under 'Swachh Bharat Abhiyan'. Regular maintenance and cleanliness drive is being conducted in these schools. So far, 31 toilets have been constructed in different schools

- SSB units have so far facilitated the opening of 3,48,333 saving bank accounts in border areas under 'Pradhan Mantri Jan Dhan Yojana'

Challenges

An old aphorism in military strategy states that the strength of a relationship is determined by the strength or weakness of the neighbours and their friends. The resultant environment of the neighbourhood is also predictable when the socio-politico-economic status, philosophies and inclinations of the strong or weak neighbours are known. The complexities of managing the neighbourhood would further depend on the typicality of the terrain and the ethnic communities of the region. There are a large number of ethnic communities in the frontier region along the INB and IBB who speak different languages and dialects, also some without script. Their life styles, customs and traditions are so different that a border guarding force needs to constantly strive to keep abreast in order to understand the psyche of the people and deal with situations as they arise. The inherent difficulties of the Force personnel who come from multiple communities and regions from across the country and speak an entirely different set of native languages, poses further challenges.

Indo-Nepal relations are guided by the **Treaty of Peace and Friendship** signed by the two countries in 1950. The provisions of the treaty inter-alia envisaged the concept of an open border. With common history and beliefs to share, Nepal is a very special neighbour for us. The *roti beti ka rishta* is an endearing relationship which has weathered many seasons through the centuries. The *rishta* is both the strength and weakness of this relationship. The porous border brings tremendous amount of pressure on a Border Guarding Force. Add to this, the penchant of citizens

of friendly countries preferring to cross over with authorised as well as unauthorised goods without being checked. The slightest provocation has the potential to endanger this friendly relationship. An error of judgment or a moment of indifference can wreak diplomatic havoc.

India's boundary with Bhutan is also an open border which runs through 699 km stretch of Indo-Bhutan border along the states of Sikkim, West Bengal, Assam and, Arunachal Pradesh. The Indo-Bhutan relationship is founded on mutual trust and understanding. Unlike other borders, the Indo-Bhutan border is characterised by a historical continuum of socio-cultural relations that transcend all geopolitical barriers. The relations between India and Bhutan are guided by the revised 'Indo-Bhutan Treaty of 2007' which provides for 'perpetual peace and friendship, free trade and commerce and equal justice to each other's citizens.' This friendship treaty essentially mandates management of the border as an instrument of socio-cultural and economic integration. Thus safeguarding and strengthening of bilateral relations along the border becomes our obvious operational doctrine. This special relationship has been sustained by the tradition of regular and extensive exchange of views at the highest level between the two countries.

The challenges of manning open borders are more daunting than securing a closed border. The 2,450 km long Indo-Nepal and Indo-Bhutan borders because of the porous nature not only provide alluring encouragement to traffickers and smugglers but also offer huge opportunities for third country trained infiltrators to enter India and pose serious threats to our national security. There are many more challenges for the Force including, the tough weather, isolation, indomitable terrain etc. It is extremely difficult to seal the entire border effectively owing to its porosity and visa free regime on the one hand and socio-economic and cultural relationship of bordering countries on the other, but SSB, by virtue of its enormous past experience of working at the grassroots level in the remote areas, is able to muster people's support and cooperation besides physically guarding the border and maintaining its sanctity.

Despite all odds SSB has been able to make its presence felt in the areas of its responsibility by fulfilling its operational commitments with professionalism. SSB because of its expertise and grassroots level contacts has been able to generate actionable information regarding infiltration from across the border and put a tab on activities of insurgent groups as also neutralise anti-national elements. The SSB personnel have sustained the tradition of winning the hearts and minds of people and are maintaining a high degree of devotion towards duty with complete commitment to their assigned goals.

The transition of Special Service Bureau as an organisation to Sashastra Seema Bal as a Force has been very smooth, effective and has had the desired impact on the security scenario on Indo-Nepal and Indo-Bhutan borders, while at all times maintaining its motto of *Seva, Suraksha and Bandhutva*. **DA**



DEFENCE AND SECURITY ALERT

The First and The Only ISO 9001:2008 Certified Defence and Security Magazine in India



Subscribe Now!



TENURE	COVER PRICE	DISCOUNTED PRICE	SHIPPING CHARGES		You Pay	
			DELHI / NCR	REST OF INDIA	DELHI / NCR	REST OF INDIA
INDIA						
1 year	₹ 1440	₹ 1008	₹ 400	₹ 700	₹ 1408	₹ 1708
2 years	₹ 2880	₹ 1872	₹ 800	₹ 1400	₹ 2672	₹ 3272
3 years	₹ 4320	₹ 2592	₹ 1200	₹ 2100	₹ 3792	₹ 4692
SAARC COUNTRIES						
1 year	US\$ 240	US\$ 156	US DOLLARS	120	US DOLLARS	276
2 years	US\$ 480	US\$ 288	US DOLLARS	240	US DOLLARS	528
3 years	US\$ 720	US\$ 396	US DOLLARS	360	US DOLLARS	756
REST OF THE WORLD						
1 year	US\$ 300	US\$ 195	US DOLLARS	240	US DOLLARS	435
2 years	US\$ 600	US\$ 360	US DOLLARS	480	US DOLLARS	840
3 years	US\$ 900	US\$ 495	US DOLLARS	720	US DOLLARS	1215

I would like to subscribe to **DSA** for 1 Year 2 Years 3 Years

I would like to gift a subscription of **DSA** for 1 Year 2 Years 3 Years

Name (Self)..... Organisation

Billing Address..... City..... Pin code

Shipping Address.....City.....

State.....Pin code.....Tel.....Mob.....

E mail id.....

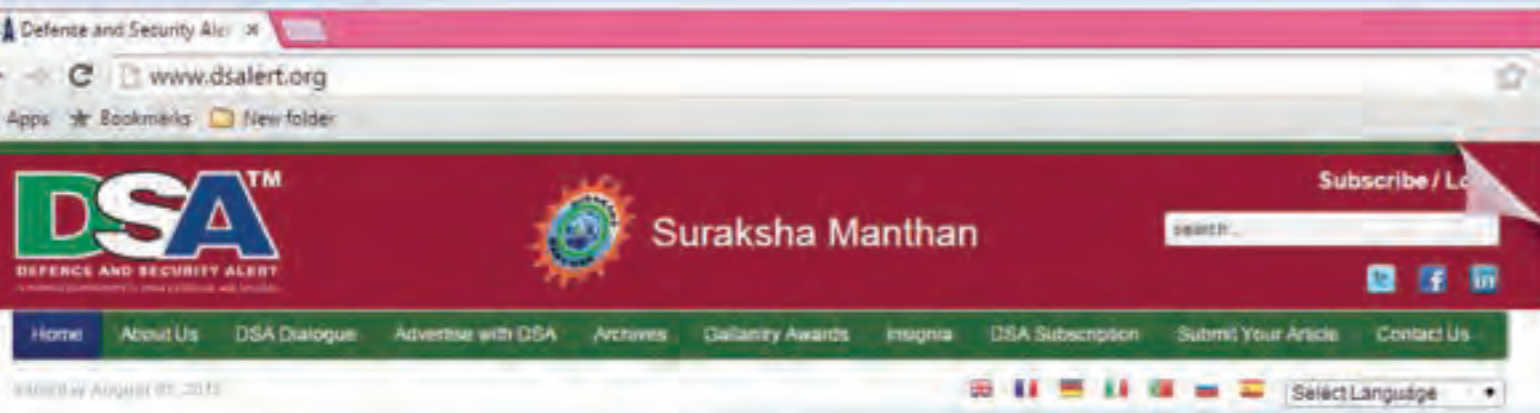
DD / Cheque No.....Dated.....Drawn on.....

for ₹ in favour of **OCEAN MEDIA PRIVATE LIMITED**, Payable at New Delhi. **Please add ₹ 50 extra for all outstation cheques.**

Terms and Conditions

- Minimum subscription is for one year ie 12 issues. Your subscription will start with the next available issue after the receipt of your payment. **DSA** issues will be dispatched through Postal / Courier Services, as advised by the subscriber.
- Please forward the completed subscription form with all the required details. **DSA** will not be responsible for any theft, loss or delay once the magazine has been dispatched. Please mention your subscription ID in all your future communications with us.
- Please inform our subscription department about non-receipt of your copy latest by 20th day of the month, failing which the request for re-dispatch will not be entertained.
- Subscription prices can also be viewed at the following web link <http://www.dsalert.org/dsa-subscription/print-edition>
- Print and Online editions can be subscribed online through credit card via Payment Gateway.
- The terms and conditions may change without any prior notice. This offer is for new subscribers, valid from 1st April 2013.
- This subscription form supersedes all the previous. Please address all your subscription related queries through E-mail: subscription@dsalert.org or call us at: +91-11-23243999, 23287999. Write to us at: Subscription department, Defence and Security Alert (DSA), Prabhat Prakashan Tower, 4/19 Asaf Ali Road, New Delhi - 110002, INDIA.

For print edition login at: www.dsalert.org/dsa-subscription/print-edition
 For online edition login at: www.dsalert.org/dsa-subscription/online-edition



Save Trees, Secure Environment and Save Money!

Subscribe to **DSA** Online

www.dsalert.org

Online Subscription

One Year	Two Years	Three Years
US\$ 30	US\$ 35	US\$ 45

You may pay by Credit Card / Debit Card through Payment Gateway.

*Indian subscribers may pay in INR as per the prevailing conversion rates.

You get

- Access to view and download the current issue.
- Access to **DSA** Archives, Blogs, Newsletters etc.
- Access to other information available only on the **DSA** website.

You can

- Post your comments
- Subscribe to past issues
- Submit articles
- Participate in Quizzes, Competitions and Discussions etc

To subscribe

Mail at: subscription@dsalert.org or Call: +91 11 23243999, 23287999, +91 9958382999

Or write to Subscription Department, Defence and Security Alert, Prabhat Prakashan Tower,
4/19 Asaf Ali Road, New Delhi - 110002, India.

Or Login at:

<http://www.dsalert.org/dsa-subscription/online-edition>

Are you a leader

in defence and security
products and technologies?

For Indian market

Advertise in the leading Indian Defence and Security Magazine

**THE ONLY MAGAZINE AVAILABLE ON
THE INTRANETS OF IAF, CISF AND BSF**



DSA

DEFENCE AND SECURITY ALERT

The FIRST and the Only ISO 9001:2008 CERTIFIED Magazine in India

Prabhat Prakashan Tower

4/19, Asaf Ali Road, New Delhi, India • www.dsalert.org, info@dsalert.org, advt@dsalert.org

To know about **DSA** focus areas, readership, global presence, circulation, distribution and rates etc please ask for our print and online edition media kits.

Buy all past issues of



DEFENCE AND SECURITY ALERT
An ISO 9001:2008 Certified Magazine

From October 2009 to December 2013

Most useful and research based content resource for:

- Defence and security personnel
- Research scholars
- Think tanks
- Defence and security institutions
- All libraries



51

Issues

In

One CD

The First and The Only **ISO 9001:2008** Certified Defence and Security Magazine in India



To order and to subscribe please contact our Sales Team

Mail to: info@dsalert.org

or Call: +91-11-23243999, 23287999, + 91-9958382999