

DEFENCE AND SECURITY ALERT

SAARC COUNTRIES : US\$ 20
REST OF THE WORLD : US\$ 25

June 2015

INDIA : ₹ 120

VOLUME 6 ISSUE 9

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

DSA™

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



MODERNISATION OF POLICE FORCES

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!

A lot of India is living in the 21st century with 19th century policing structures and manuals. The living conditions of many are of course still some centuries behind, but they're largely out of the policing page. Those that are exposed to the police on a regular basis have to deal with a service that is manned, trained, managed and reports, in a 19th century cultural ethos. Society and the crimes it commits, are now largely 21st century. But the governing ethos of the police is still in its imperial era origins. That has to change for India to modernise as a country and as a lifestyle.

The modernisation of the police is largely a case of modernising the minds firstly. It is not about changing uniforms or weapons or cars. It is really about what the police ought to be in an emerging 21st century society. Much baggage has to be shed, by those who are in police uniforms, as well as those who govern how the service runs. The onus lies on the police hierarchy as much as it does on the politicians who determine how the service is to be managed. The long-term goal has to be the elimination of the dreaded police-politician nexus, where each is cared for by the other, while the public suffers.

The primary focus, therefore, has to be a greater level of confidence between the public and the police, something which is sorely lacking, in every part of the country. For that to happen the starting point must be the complete elimination of colonial style policing, where the ruled and the ruler are divided by deep absence of confidence. For the people to have confidence in the police the relationship between the two has to change from ruler-ruled to that of a protector of the people. It is not a colonial service any longer, but that of a democratic republic. It must behave in that manner and it must also look the part.

The police in India wears military style ranks and star plates, which is completely contrary to the ethos of policing in a democratic society. Such ranks and star plates were part of the course when India was ruled by imperial Britain who created these institutions to govern colonial subjects. That is no more the case. Appearances must change to begin the process of modernising the service according to 21st century democratic Indian requirements.

After this fundamental statement of change is instituted the process of modernising must begin with current man management techniques. The beat constable, the most vital link in the chain between the public and police higher ups, is the most mismanaged Indian public servant. He or she, functions under the greatest stress levels of all government servants. Their hours of duty, as well as areas of responsibility, have no logical charts or structures. Ad hoc is the rule of the day as far as they are concerned. So the frustration they feel against their higher ups is invariably taken out on the hapless public. And thus, frequently the police resort to extortion and sometimes even contract killing to make their day.

Human touch and kindness to the public and an empathy rather than disdain are the order of the day. But for these to become a reality the entire edifice of policing structures has to change, not simply evolve. There are plenty of studies, including the dusty National Police Commission report, that delve on the matter. They are certainly not the last word but merely a beginning point to take this process to its logical end.

India has one of the lowest policemen to population ratios in the world. Even as the population has increased manifold the intake of policemen has not kept pace. What has grown disproportionately, however, is the increase in the number of higher ranks. When the actual requirement is for more beat constables to the daily duties and interaction with the public. Because of these lacunae the performance and credibility of the police has taken a beating. What needs to be done immediately is to increase the interaction with the public, more akin to citizens police force rather than that of some alien ruler.

The modern digital age is based on an interactive sense of life. And that is also going to be the agenda of the hundred smart cities coming up across India. These smart cities can only be secured and thus allowed to prosper, when those who are the protectors behave as such, interact with the people and are caring toward them. That would be the greatest modernisation of the Indian policing system. Rest will follow without a worry.

Manvendra Singh



**NECESSITY
 THE MOTHER OF INVENTION**

Any progress and development is based on the truism: "Necessity is the mother of invention". I am deeply impressed by the edicts of Chanakya and had adopted his quotation as the Mission Statement of **DSA**. He wrote: "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 negligence of the State."

Defence and Security have been the two very important and enduring 'necessities' of life down the ages. **DSA** has, in this edition, made an indepth analysis of how the Indian nation state has failed to make the necessary 'inventions'/acquisitions to ensure the security of the people against emerging threats. One such failure is in the absence of modernisation of the police force to meet the emerging threats even as the habitat has grown both horizonatally and vertically and the narrative has shifted swiftly to 'mega cities' and 'smart cities' in this day and age of urban guerrilla warfare and Internet instigated violence.

The 'mighty arms' of the modern nation state are its military, paramilitary and police, each operating within their designated ambience. The police is the context of modern 'mega' and 'smart cities' and how it is managed and maintained illustrates its relevance to modern times.

Our police forces are still governed by laws written by Britain to sustain its Empire. It is shocking and unfortunate that not much has been done by the past governments to modernise our Police and Security Forces. So I can say that in the face of the growing new necessities the Indian nation state has failed to make the requisite inventions in the criminal justice system, the material wherewithal and the management of the Security establishment to confront the existentialist problems.

When anti-national elements have increased, they have ganged-up and developed a nexus with each other and have equipped their cadres with the latest weapons, arms and ammunition and communication technologies, then why are our forces still not equipped with the best technologies to handle the counter-insurgency and counter-terrorist operations in the country? The past government introduced a special fund of some thousand crores of rupees for each year with guidelines to all the State governments for the modernisation of Police but unfortunately the fund was hardly ever used for the intended purpose in a planned manner. Thus our police forces are still compelled to use the obsolete weapons, arms and ammunition and with no interceptive gadgets and strong telecommunication devices to counter and deal with a menacingly equipped opponent.

I am sure that the current government is reviewing this matter very seriously and sincerely not because it has to upturn the decisions of the past government but to actually empower our police to secure the nation and its people from all sorts of inimical anti-national elements in every part of the country.

The announcement of the current government to create 100 Smart Cities in the country in the next few years is a big step which will enable the people to have access to all the modern services for comfortable living. A lot of new infrastructure will be developed, millions of people with different cultures, languages and backgrounds will be living in these smart cities. And for a peaceful and harmonious environment in these smart cities the most important factor will be to protect their inhabitants from any kind of threat to their lives and their belongings be it by natural or man-made disasters (as in a CBRN environment).

So it is very important that this concept of Prime Minister Modi should not go in vain and we actually are able to establish the first hundred smart cities which can be increased in the years to come for the overall progress of India.

Jai Hind!

Pawan Agrawal

**ANNOUNCES
 JULY 2015 ISSUE ON**

**MAKE IN INDIA
 IN DEFENCE**

The advertisement features a central graphic of a map of India, where the landmass is formed by a dense arrangement of various defense-related logos and images. The logos include: TATA, HAL, Ministry of Defence, Reliance Industries Limited, Sikorsky, Airbus, BrahMos, OFB, KAMOV, Lockheed Martin, Bharat Forge, HATSOFF, Reliance, BAE SYSTEMS, Hero, EADS, Punj Lloyd, ADANI GROUP, Sukhoi, ELETTRONICA S.p.A., DYNAMATIC TECHNOLOGIES, IAI, BOEING, DASSAULT AVIATION, AEGUS, GENERAL DYNAMICS Canada, SPECK, Mahindra DEFENCE, and Hinduja. The map is surrounded by images of military aircraft, a naval ship, and a tank. The text 'ANNOUNCES JULY 2015 ISSUE ON MAKE IN INDIA IN DEFENCE' is prominently displayed at the top, and 'MAKING INDIA SELF-RELIANT' is at the bottom.

June 2015 Contents

ARTICLES

Central Government Funding For Modernisation Of State Police Forces 10
GK Pillai

Aerial Policing For Securing Smart Cities 13
Air Marshal Anil Chopra (Retd)

Community Policing And Homeland Security Lessons From The USA Experience 16
Satyajit Mohanty IPS

Police Community Relations A Bridge Too Far? 20
Dr MZ Khan

Training For Police Modernisation 24
Rohit Choudhary IPS

Guidelines And Challenges For Policing A Smart City 27
Dr Muktesh Chander IPS

Disasters And CBRN Threats In Metropolitan Areas 32
Maj Gen VK Datta (Retd)

Police Leadership Management Of Man-made Or Natural Disasters 35
V Balachandran

Integrated Emergency Response 38
Dr Rupali Jeswal And Joe Marchese

Law Enforcement Personnel Keeping Pace With Developments And Technologies 42
Dorin Muresan



CBRN Security For High Visibility Events 46
Col (Dr) Ram Athavale (Retd)

Cyber Weaponisation And Cyber Deterrence 50
Dr Kamlesh Bajaj

Advanced Technology Solutions Policing For Mega Cities 54
Jo S Birring

Women In Police 57
Vimla Mehra IPS

Criminogenic Factors 58
Sharda Prasad IPS

Police Forces For CI And CT 61
Team **DSA**

Vehicle Thefts In India Hi-Tech Approach To Cut Down The Menace 64
Bijay Kumar Singh IPS
Bhushan G Borase IPS
Abhinav A Khare IPS

Sneak Peek 3



Exclusive Interview 6
His Excellency Patrick Suckling
High Commissioner Of Australia To India



Know The Chief 23
BPR&D

Get Connected 67

EXCLUSIVE INTERVIEW

WITH HIS EXCELLENCY

PATRICK SUCKLING

HIGH COMMISSIONER OF AUSTRALIA TO INDIA

His Excellency Patrick Suckling has been High Commissioner to India since January 2013. Previous overseas assignments include Washington (2003-2007) and New Delhi (1997-1999). Between 2009-2011 he managed international issues for two Prime Ministers of Australia, encompassing foreign, economic and international aid policy. He has combined foreign policy with trade and economic policy throughout his career. He joined the Department of Foreign Affairs and Trade in 1994. He holds a Master of International Relations from Monash University and honours degrees in economics and English literature from the University of Sydney. He also holds a graduate diploma in Hindi from Sydney University

Defence and Security Alert: The evolution of India's Look East Policy and the growing bonhomie between Prime Minister Modi and Prime Minister Abbott have brought our countries closer in the recent past and this augurs well for the future. How do you visualise our bilateral relations developing in the emerging regional and global security environment?

His Excellency Patrick Suckling: The relationship between Australia and India has never been in better shape. It is more dynamic, more diverse, broader and deeper than ever before. Indeed, unprecedentedly so. The Strategic Partnership agreed in 2009 was roundly affirmed during Australian Prime Minister Abbott's visit to India in September 2014 and again during Prime Minister Modi's visit to Australia only two months later. Both sides have a strong commitment to deepening the relationship.

The positive momentum in the relationship is being driven by economic complementarity, community ties and geostrategic shifts in the Indo-Pacific.

DSA: India is one of the fastest growing economies in the world but economic cooperation between India and Australia is not commensurate with the potential that exists. What is your government doing to encourage Australian companies to venture out and increase their participation and share in investments, joint ventures and trade and commerce?

HE Patrick Suckling: We have been investing a lot of time and energy to strengthen and broaden the investment, trade and commercial links between our two countries. Senior business leaders accompanied both

highly successful Prime Ministerial visits. Australia's Minister for Trade and Investment, the Hon Andrew Robb AO, led the largest ever Australian business mission to India in January of 450 Australian business leaders across 14 sector-specific programmes to a number of India's cities. But much potential remains.

To create a strong bilateral framework for deepening our economic and commercial cooperation, both our Prime Ministers have committed to concluding a Comprehensive Economic Cooperation Agreement (CECA) between India and Australia by the end of the year. A CECA would unlock the economic potential of the relationship, providing new trade and investment opportunities to take the relationship to the next level. It would help provide transparency and certainty and inspire investor confidence to attract more inward FDI from Australia into India.

The Australia India CEO Forum brings together key business leaders from both sides and is co-chaired by Rio Tinto CEO Sam Walsh and the Chairman of the Adani Group, Gautam Adani. The annual Australian Innovation Showcase promotes Australian capabilities across life sciences, health, materials, IT and advanced manufacturing. In mining, energy and agriculture where Australia has world-class expertise we are encouraging greater engagement. We believe this engagement will increase the productivity and efficiency of Indian business, promote economic growth and create jobs in India.

In defence, security and policing, Australian companies are already offering Indian customers a range of specialty products and services – from radio equipment to video surveillance applications. We are working to increase the cooperation between our defence and associated industries, including through joint ventures.

Our Government is determined to see Australia become a key economic partner for India as it continues to grow and take its place as a major global economy.

DSA: Since India and Australia are large maritime nations cooperation and engagements between our naval forces should be pretty high on our bilateral defence agenda. But the maritime interaction between our navies has not attained the critical mass needed for a self-sustaining relationship. What more needs to be done to energise our maritime partnership?

DSA: The world is transiting from a unipolar to a multipolar world order and there is much ado about US rebalancing the pivot and from a mere geopolitical entity Indo-Pacific metamorphosing into a unique



His Excellency Patrick Suckling with Urvashi J Agrawal, President of DSA magazine

geostrategic theatre of global importance. What is the relevance and significance of Indo-Pacific to Indian and Australian maritime security interests?

DSA: Joint Military exercises significantly enhance defence cooperation between friendly countries. What is the status and scope for such Indo-Australian joint military exercises?

His Excellency has chosen to give one detailed answer to the above three questions (DSA).

HE Patrick Suckling: Major trade, investment and energy flows are binding the great Indian and Pacific Oceans and their nation states into a new strategic arc where the prosperity and stability of one will be indivisible from the other. Economic integration, connectivity and cooperation amongst countries within these two regions will be essential for peace and prosperity for both India and Australia.

The connectivity between these regions is so important for our strategic outlook that Australia finds it useful to think of them as one large strategic entity called the Indo-Pacific. It is particularly useful for Australia as our country straddles both the Indian and Pacific Oceans. Defining our region this way also recognises that a rising India is not at the periphery, but indeed, at the very heart of our strategic outlook. It also underlines the crucial role that the maritime environment will play in our future strategic and defence planning.

But we believe the concept of Indo-Pacific is useful for India too as it provides a coherent framework that highlights the importance not only of connectivity to the east coast of Africa where India has long had substantial interests, but across to important markets in South East Asia, China, Japan and the US. The term Indo-Pacific connects the two great oceans and rightfully recognises India as a key player in Asia's strategic mix.

In this region, the Indo-Pacific, Australia and India increasingly find that we have intersecting interests. We share a commitment to ensuring the free movement of trade, combating transnational crime and disaster preparedness.

The Framework for Security Cooperation agreed by Prime Minister Abbott and Prime Minister Modi last year provides a platform for enhanced engagement including in the maritime domain. We are looking forward to the inaugural bilateral maritime exercise to be held off the east coast of India in September this year. I believe that this is the natural evolution of our robust Navy-to-Navy cooperation and it is an exciting development. This exercise will involve the deployment of both Royal Australian Naval and Air Force personnel and assets to engage with the Indian Navy. Last September our Prime Ministers affirmed a shared commitment to this exercise taking place on a regular basis.

Australian and Indian Chiefs of Navy meet on a regular basis. As do our other senior military counterparts. Ship visits are an opportunity for exchange between our Navy personnel: there have been four ship visits over the past 18 months including most recently the visit to Mumbai by Australian frigate *HMAS Newcastle* in April this year.

Australia and India also have a history of active engagement through multilateral exercises. In March 2014, Australia sent *HMAS Childers* to participate in the Indian Navy's Exercise MILAN, a biennial multilateral maritime activity in the Bay of Bengal. On our own shores, we have previously welcomed Indian Navy participation in the Royal Australian Navy's biennial Exercise KAKADU, to which India sent an observer in 2012. We will continue to welcome Indian involvement in future iterations of this exercise.

Australia also conducts the biennial Exercise PITCH BLACK, which is the Royal Australian Air Force's premier operational aerospace exercise and is the largest tactical air activity conducted in Australia. It provides Australian and international aircrew, controllers, combined air operations centre staff and base support personnel with a challenging opportunity to conduct air combat and ground support operations in a multinational environment. Two Indian Air Force members attended the International Observer Programme for Exercise PITCH BLACK 12 and our Prime Minister recently extended an invitation for India to participate next time the exercise is held.

Australia currently chairs the Indian Ocean Naval Symposium and the Indian Ocean Region Association. Australia is working closely with India to strengthen these organisations. Last year, as part of the Indian Ocean Rim Association's activities, India hosted the inaugural Indian Ocean Dialogue. The event was so successful that Australia will host the second dialogue in September this year, with a focus on maritime security and transnational crime. We will partner with India to make sure the dialogue is a success. Later this year Indonesia will take over the chair of IORA, followed by South Africa in 2017; that will mean four G20 countries consecutively in the chair. This must help IORA build momentum as an effective organisation. In IONS, Australia's Chief of Navy has introduced a revised Charter of Business as well as working groups that focus on humanitarian assistance and disaster relief, information-sharing and counter-piracy.

DSA: With growing Chinese assertiveness, interest and territorial claims in South China Sea and East China Sea the security environment in the region is getting vitiated. What are your views on this developing scenario which may erupt into an avoidable conflict?

HE Patrick Suckling: Australia does not take sides on competing territorial claims in the South China Sea, but we are concerned that land reclamation activity by China and other claimants could raise tensions in the region. Australia has a legitimate interest in the maintenance of peace and stability, respect for international law, unimpeded trade and freedom of navigation in the South China Sea.

Australia strongly opposes the use of intimidation, aggression or coercion to advance any country's claims or unilaterally alter the *status quo*. We urge claimants to exercise restraint, take steps to ease tensions and refrain from provocative actions that could escalate tensions.



His Excellency Patrick Suckling in conversation with Pawan Agrawal, Publisher and CEO and Urvashi J Agrawal, President of DSA magazine

DSA: How do you view the state of the world today, the global security environment and the role of the UN in the emerging scenario? Do you support the expansion and reconstitution of the UN Security Council and India becoming a permanent member of the UNSC?

HE Patrick Suckling: Australia is a founding member of the UN, an active participant in UN institutions and the 12th largest contributor to the UN regular and peacekeeping budgets. Australia was a non-permanent Member of the Council during the 2013-14 term and established a strong reputation as an active, pragmatic and outcomes-focused Member. Australian leadership of the Council's response to the downing of Malaysia Airlines flight MH17 and our advocacy against ISIL and foreign fighters were prominent examples.

Australia supports India's bid for permanent membership of the United Nations Security Council, which would provide geographic balance to permanent Council membership.

DSA: Global jihad and terrorism are spreading their tentacles all over the world. What bilateral and multilateral strategies and mechanisms have India and Australia devised to counter and contain these scourges which are disturbing world peace and security?

HE Patrick Suckling: Both Australia and India have been victims of global terrorism and know the devastation caused within the community from such futile loss of life. We believe it is important for the international community to maintain a strong and united stance against terrorism.

The Australia-India Joint Working Group on Terrorism provides a platform for our officials to discuss these issues and work together to prevent terrorism. The forum has recently been expanded to include transnational crime issues.

DSA: In the Joint Statement during Prime Minister Modi's visit to Australia it was announced that India and Australia have 'decided to extend defence cooperation to cover research, development and

industry engagement'. Do you think we will now see wide-ranging collaboration and cooperation between India's DRDO and Australia's DSTO?


HE Patrick Suckling: As our Prime Ministers highlighted in the recent framework, this is an area of potential growth. I am confident that we will see links between our respective defence science establishments increase, as we start to explore the complementarities between our organisations.

For example, the Australian-built *Bushmaster* protected mobility vehicle for infantry personnel is well proven in Iraq and Afghanistan and could be developed further for specific Indian military requirements. There is also much to be gained from greater engagement on the common threat of improvised explosive devices. DRDO and DSTO are scheduled to engage this year to scope out potential projects.

DSA: How do you envision Indo-Australian bilateral relations in the coming years and decades and what ideas and thoughts would you like to share with the people of India and DSA readers around the world?

HE Patrick Suckling: Australia and India are natural partners and our shared interests will draw us together. Trade and investment is growing and the CECA trade agreement will provide a number of opportunities to take this further. Our defence partnership is already on an upwards trajectory.

Our community ties will only bring us closer. Already 450,000 people of Indian origin live in Australia. India is our largest source of skilled migrants and second largest source of international students; 46,380 Indians studied in Australia in 2014. As Prime Minister Modi's visit to Australia in November last year demonstrated, there is a great appetite among Australians to increase their understanding of India. Tourism and education will help us know each other better.

I am optimistic about the trajectory of our relationship. There is every possibility for us to take advantage of our growing number of shared interests to improve our own economies and to enhance regional prosperity. 



CENTRAL GOVERNMENT FUNDING FOR MODERNISATION OF STATE POLICE FORCES

Technology has taken giant strides in the last two decades and if less than 10 per cent of the Police Force underwent refresher courses in their entire career, then the bulk of the police force had become obsolete. This could be seen in the lack of scientific investigation of crimes and traffic accidents and consequent low conviction rates.

Police and Law and Order are subjects exclusively to be dealt with by the states. Yet under Article 355 of the Constitution of India, it is the duty of the Central Government to protect states against internal disturbances and to ensure that the governance of every state is carried on in accordance with the provisions of the Constitution of India.

It is a fact that since Independence all State governments have neglected the professional development of the state police establishment.

State Negligence

Parliamentary Standing Committees have been unanimous in holding that states are extremely sensitive over their exclusive rights over the Police Forces and Law and Order, yet have failed miserably to provide adequate funds to ensure that Law and Order can be maintained and that the State Police

Forces have been adequately trained and equipped to handle Law and Order situations on their own. At the slightest deterioration in the Law and Order situation, State governments have been requesting for Central Police Forces to control the situation. This has led to a very large expansion of Central Police Forces in the last decade at the cost of the state police forces with severe long-term implications on the overall Law and Order situation in the states.

It is well known that just over one per cent of the state GDP is spent on the Police. Of this more than 85-90 per cent is spent on salaries and very little on equipping and training the State Police Forces to tackle the existing and emerging threats to Law and Order.

Central Contribution

Historically, it was only in 1969, twenty two years after Independence that the Centre realised that it was necessary to supplement the efforts of the State

governments to improve the capability of the State Police Forces to meet the emerging threats to Law and Order. It is no coincidence that this followed the first serious threat following the Naxalite movement in West Bengal. However, the assistance was meagre and the total Central Assistance to all States/UT's from 1969-70 to 1999-2000 was only ₹ 536.76 crore. A BPR&D survey in the year 2000 estimated the deficiency in funding at over ₹ 25,000 crore. As a result, the Cabinet Committee on Security in January, 2001 approved the allocation of ₹ 1,000 crore every year from 2000-2001 for the modernisation of State Police Forces. Initially, this was a 50 per cent CSS scheme which was amended to a 75 per cent CSS and then further amended from the year 2005 to Cat A and Cat B States, with 90 per cent and 60 per cent Central assistance.

It is well known that just over one per cent of the state GDP is spent on the Police

Half Measures

State governments, during this decade, got Central funds and with certain deficiencies were able to partially modernise their police forces. But the funds released were wholly inadequate considering the deficiencies that existed and the ever increasing demands on the Police Forces. Certain State governments used the Central Grants as an excuse to cut down on the State allocations, so that ultimately there was no incremental improvement and the *status quo* of deficiencies

continued. This was brought out in several CAG reports and internal reviews.

One aspect that got neglected upto 2009 was the need to improve the quality of the Police manpower. If one had a poor quality of manpower and they were not being trained properly, then all the modern equipment supplied would not be of any help. This was borne out during the 26/11 terrorist attack in Mumbai, which revealed the lack of training and lack of adequate SOP's of the local police, notwithstanding individual heroics of the constabulary.



GK Pillai

The writer is an IAS officer of the 1972 batch of Kerala cadre. He is the former Home Secretary of India.

Obsolete Police

Technology has taken giant strides in the last two decades and if less than 10 per cent of the Police Force underwent refresher courses in their entire career, then the bulk of the police force had become obsolete. This could be seen in the lack of scientific investigation of crimes and traffic accidents and consequent low conviction rates. Training was a low-priority in the State police and with a few exceptions, postings to police training schools and colleges were punishment postings with disastrous consequences for the new recruits.

In 2009-2010, the recommendations of some outstanding young Police Officers in the mini missions resulted in SOP's being published for recruitment of the lower Police personnel. The realisation had dawned that unless one could ensure an element of integrity in the recruitment process which had to be transparent and merit based, it was futile to expect the Police Forces to deliver. The MHA also took up the matter with the 13th Finance Commission and thanks to its Chairman Dr Vijay Kelkar was able to have the Commission recommend allocations of ₹ 2,441 crore for creation/upgradation of training infrastructure. It is another matter that only ₹1,354.89 crore could be released to the states and bulk of the grants lapsed.

The allocation and releases of funds by the MHA to the states during the last 3 years are given below.

Finance Slashes Funds

In June 2014, it was reported that the Union Home Minister after reviewing the Modernisation of Police Forces Scheme had directed officials in the Ministry to prepare a proposal for doubling the ₹ 1,500 crore budget for Police modernisation. In the meanwhile, the 14th Finance Commission submitted its report which was accepted by the Central government. As a result, the devolutions to the states went up to 42 per cent from the existing 32 per cent of revenues and the Ministry of Finance unilaterally




Details of funds released to various State governments under MPF Scheme during 2012-13 to 2014-15

Name of State	Funds released (₹ in crore)		
	2012-13	2013-14	2014-15
Andhra Pradesh	21.31	85.92	54.17
Arunachal Pradesh	2.00	10.77	9.69
Assam	13.41	59.93	43.29
Bihar	15.03	55.99	49.08
Chhattisgarh	4.93	30.88	37.36
Goa	0.52	2.76	1.86
Gujarat	12.99	78.43	72.65
Haryana	6.06	21.61	28.25
Himachal Pradesh	1.78	7.10	5.75
Jammu & Kashmir	22.47	101.00	105.17
Jharkhand	4.67	29.86	34.52
Karnataka	19.49	77.50	103.65
Kerala	8.19	48.26	42.00
Madhya Pradesh	13.78	61.37	58.18
Maharashtra	29.63	92.93	76.65
Manipur	4.85	20.64	28.45
Meghalaya	1.91	8.12	6.98
Mizoram	6.40	17.92	19.03
Nagaland	5.46	37.15	31.39
Orissa	7.92	53.71	42.92
Punjab	8.34	30.50	38.13
Rajasthan	15.88	62.83	102.50
Sikkim	0.90	5.09	3.57
Tamil Nadu	17.70	69.95	85.74
Tripura	3.99	20.19	22.69
Telangana	0.00	0.00	68.13
Uttar Pradesh	32.10	176.08	169.23
Uttarakhand	3.61	12.89	8.81
West Bengal	14.68	62.24	47.40
Total	300.00	1341.62	1397.24

decided to slash the Modernisation of Police Force Scheme among others from ₹ 1,500 crore to just over ₹ 300 crore and also eliminate major schemes for augmentation of Police Infrastructure in LWE States etc with serious implications for the whole strategy of fighting this serious national security threat.

Three major schemes, namely the Modernisation of Police Forces, the Special Infrastructure Scheme for upgradation of Police stations in LWE States and the Crime and Criminal Tracking Network Scheme have been seriously affected.

While theoretically, State governments may provide the necessary funds for these in their respective budgets, all available indications are that this has not been done. The CCTNS scheme is a Central Scheme and has to be funded by the Central government. If this does not happen, we are in for serious Law and Order implications, which may have a negative impact on investor sentiment and consequent economic development and the creation of jobs so vital for India's young population. One only hopes that the policy makers both at the Centre and the States take note of this. 

AERIAL POLICING FOR SECURING SMART CITIES

A big advantage from aerial policing is the reduced requirement for manpower. On the spot policeman who is often considered a corrupt nuisance can now be deployed for other duties. VVIP route sanitisation would not require 1,000 policemen any more. Aviation may come to the rescue of India's dismal population-to-police ratio of 130 to every 100,000.

Prime Minister Modi recently approved the mission for building 100 smart cities and earmarked ₹ 48,000 crore amounting to ₹ 100 crore per year for five years for each selected city. In very simple terms, a 'smart city' is meant to use modern digital technologies to enhance performance and well-being of the population, reduce costs and resource consumption and to engage more effectively and actively with the citizens. The key elements include transportation, energy, health care, water and waste management. Concept is supported by cyber/digital action allowing quick, free and intelligent

information flow. The cities will have to cater to climate change, growing economic aspirations, ageing populations and will need participative financing. More and more countries are working towards the cities of the future. Cities like Stockholm (Sweden), Gangnam (Seoul, South Korea), Waterloo (Ontario, Canada), Taipei (Taiwan), Mitaka (Japan), Glasgow (Scotland),



Air Marshal Anil Chopra
PVSM, AVSM, VM, VSM (Retd)

The writer was a pioneer of the *Mirage 2000* fleet and commanded a *Mirage* Squadron, two operational airbases and the IAF's Flight Test Centre ASTE. He was the Team Leader of an aircraft upgrade project in Russia. Currently he is a member of Armed Forces Tribunal at Lucknow and a member of Executive Council of Jawaharlal Nehru University, New Delhi.





New York (USA), Barcelona (Spain), Shanghai (China) and Singapore have made significant progress. In the near future 75 per cent of India's wealth will be generated by urban population. The cities have to be made more efficient. Indian Government wants the entire strata of population irrespective of level of education, skill and income to benefit. Among the various elements, governance, mobility and the smart citizen require policing support.

Policing The City

Policing the cities is required to enforce law, protect property and prevent disorder so that citizens can live in peace and tranquillity. To achieve these there is a need to monitor vehicular traffic, crowd control, prevent illicit trafficking, theft and other crimes against society. Important elements to achieve this are surveillance and control. Indian police has also to routinely monitor large religious gatherings sometimes as large as the *Kumbh mela*. Police thus has an administrative, economic and social duty. Prevention is the primary target of the police. They also have auxiliary tasks like issuing arms licenses and monitoring their misuse, bomb disposal, crash investigation, homicide, fraud etc. Some Islamic societies have religious policing to enforce application of Sharia Laws. Today there is also aerial threat of an attack by a bomb-loaded UAV or micro-light. Departments like Military, Railways and Forests etc have their own police forces. Police requires secure quick communications, rapidly deployable vehicles with warning devices and modern equipment for surveillance. Some of the enabling new technologies for policing include cloud-based Internet services, smart phones, RFIDs (Radio-frequency identification), infrared and visual cameras, robots, radars and host of other sensors.

Aviation Allows Vantage Point

Advances in aviation have permeated and made positive difference to every aspect of human life. Aviation's biggest civil boon has been quicker transportation. Advances in Unmanned Aerial Vehicles (UAVs) and micro drones have allowed aviation to replace the man in many daily tasks, including newspaper to milk bottle deliveries at the doorstep. While more and more aerial functions are taken over by UAVs, they offer a totally new dimension to policing functions. Long endurance solar powered UAVs could be airborne for days and months. Air refuelling of UAVs is already a reality. Their position in the air, large ground footprint and quick mobility allow them to be used for both communications and surveillance. Modern UAVs can also be flown with autonomous control. FAA and ICAO are working towards regulatory clearance for civil operations of UAVs in airways. While the initial UAVs were only for surveillance, later ones are also armed with missiles. Over 50 countries operate UAVs and several of them make their own. Since most

cities have high traffic airports, usage of UAVs for law enforcement needs close regulation and control.

Active Aerial Policing

The first targeted UAV terrorist killing took place on 3 November 2002, in the Marib, Yemen. Six alleged terrorists were killed in their SUV by United States using a UAV-fired missile. The command centre was in Tampa, Florida, USA. The most commonly used UAVs for policing are the tactical UAVs that operate at up to 10,000 feet altitude and have operating range of 150 km. They are primarily for surveillance and limited secure police data transmission. Also used are hand-held UAVs operating below 2,000 feet and covering short ranges up to 2 km for specific operation. Micro or Nano UAVs are used for snooping in confined spaces for targeting individual terror cells. Micro drones which are already used by logistics firms to deliver parcels can be used to drop a smoke or tear gas grenade. As part of policing, UAVs are increasingly being used for highway patrolling, flood monitoring, emergency rescue aid dropping, fire and large accident rescue and investigation, earthquake and landslide monitoring, illegal landfill detection, crowd monitoring etc. After the Mumbai attacks, policing the coast and coordinating the operations are functions best handled from the air. Media is using more and more UAV video footage to keep the public informed of events. Policing the huge crowds during a cricket match are roles meant to be assigned to UAVs. Traffic lights on main city arterial roads can actually be operated based on aerial picture to decongest roads. Animal rights activists are using radio controlled quadcopters to film hunters.

Multiple Uses

Low cost UAV applications include wildfire mapping, water and oil pipeline security, home security, road patrol and anti-piracy. Movie makers are replacing the more complex helicopter with UAVs for aerial shooting. Drones were used for filming skiing events during 2014 Winter Olympics and for extreme sports photography. There are already licensed UAV photographers in some Western countries. Drone journalism is a subject in some American universities. US and Canadian cities are already using UAVs for policing and law and order monitoring. Police caught a car thief by using a UAV in 2010. UAVs are being used in Naxal hit areas in India for policing Naxal movements. UAVs have a big role in disaster management both in search and rescue and damage assessment. UAV will assist a police chase against a speeding runaway criminal. Drones can help in disaster relief by gathering information of affected area to improve situational awareness and help direct resources. Nuclear disaster like Fukushima that restricts human intervention can effectively use drones. Drones were the first to help Japan assess tsunami damage and support relief operations. Peruvian archaeologists routinely use drones for

survey work and protect sites from squatters, builders and miners. Drones are very effective to get a quick over-the-hill view for policing in mountainous areas. Infrared cameras allow night vision and also can detect heat footprints. Long queues of trucks at city borders or vehicles at toll plazas can be policed from the air. Water wastage policing, unauthorised tree cutting, pollution monitoring, accident rescue, street light monitoring, traffic bottleneck control, political demonstration monitoring, city-parks policing, are some of the other uses of aerial policing. A single UAV can replace thousands of CCTV cameras. They act as great deterrent for civic indiscipline through minimal human intervention.

All-weather Capability

UAVs carry payloads like optical sensors and synthetic aperture radar which can provide images through clouds, rain or fog and in daytime or night-time conditions, all in real time. Micro UAVs like *Aeryon Scout* have been used to search missing persons. UAVs have been tested as airborne lifeguards, locating distressed swimmers using thermal cameras and dropping life-saving gear to swimmers. Part of United States' war against terror, *MQ-1 Predator* UAVs armed with *Hellfire* air-to-ground missile were used to assassinate high profile individuals (terrorist leaders) inside Afghanistan, Pakistan, Yemen and Somalia. Unmanned airborne systems not only improve coverage area and response time, they reduce human risk. Technology is being employed in order to save as many lives as possible. UAVs have a great role in anti-smuggling and anti-wildlife poaching. Quadcopters are used for monitoring cruelty to animals. Policing uninhabited islands for sparsely populated cities is another area of advantage. UAVs can transport medicines, supplies into remote or otherwise inaccessible regions. UAVs are a great asset for disaster relief management. Quick damage assessment would allow directed relief delivery. A mini hand-held system can be launched in minutes. The 4-5 kg vehicle could climb up to a kilometre in less than a minute and cruise at 50 kmph. In India Hindustan Aeronautics Limited (HAL) along with DRDO's Aeronautical Development Establishment (ADE) and National Aeronautical Laboratory (NAL) Bangalore have developed mini and micro UAVs of 3 kg class. HAL designers are working on 8-10 kg UAVs, which are expected to receive certification by the year end.


Opportunities And Challenges

Like the Internet and many other technologies, UAV development has been driven by the military. UAVs can have multiple sensors, like satellites and could perform multi-functions. USA and Israel currently dominate 80 per cent of the world UAV market. China is fast catching up. Northrop Grumman and General Atomics are big US manufacturers. IAI and Elbit of Israel are into UAVs in a big way. Indian Armed Forces operate nearly 150 mid-sized UAVs and many more hand-held ones. Their experience

will be available for police forces. India needs to push its 'Make in India' initiative for UAVs. India has made a beginning in Jharkhand. Mumbai and New Delhi police are on the verge of acquiring UAVs. A big advantage from aerial policing is the reduced requirement for manpower. On the spot policeman who is often considered a corrupt nuisance can now be deployed for other duties. VVIP route sanitisation would not require 1,000 policemen any more. Aviation may come to the rescue of India's dismal population-to-police ratio of 130 to every 100,000. Terrorist using a UAV for a low-level drone attack is a reality. Seats of national government and VVIP residences are known targets from the air. The Osama raid at Abbottabad, Pakistan and the undetected microlite landing in the Red Square, Moscow are indicative of penetration by use of enabling technology and the risk of usage by terror groups. Similarly some Western companies are developing lasers to damage or knock-down UAVs and these could reach unwanted hands.

Misuse

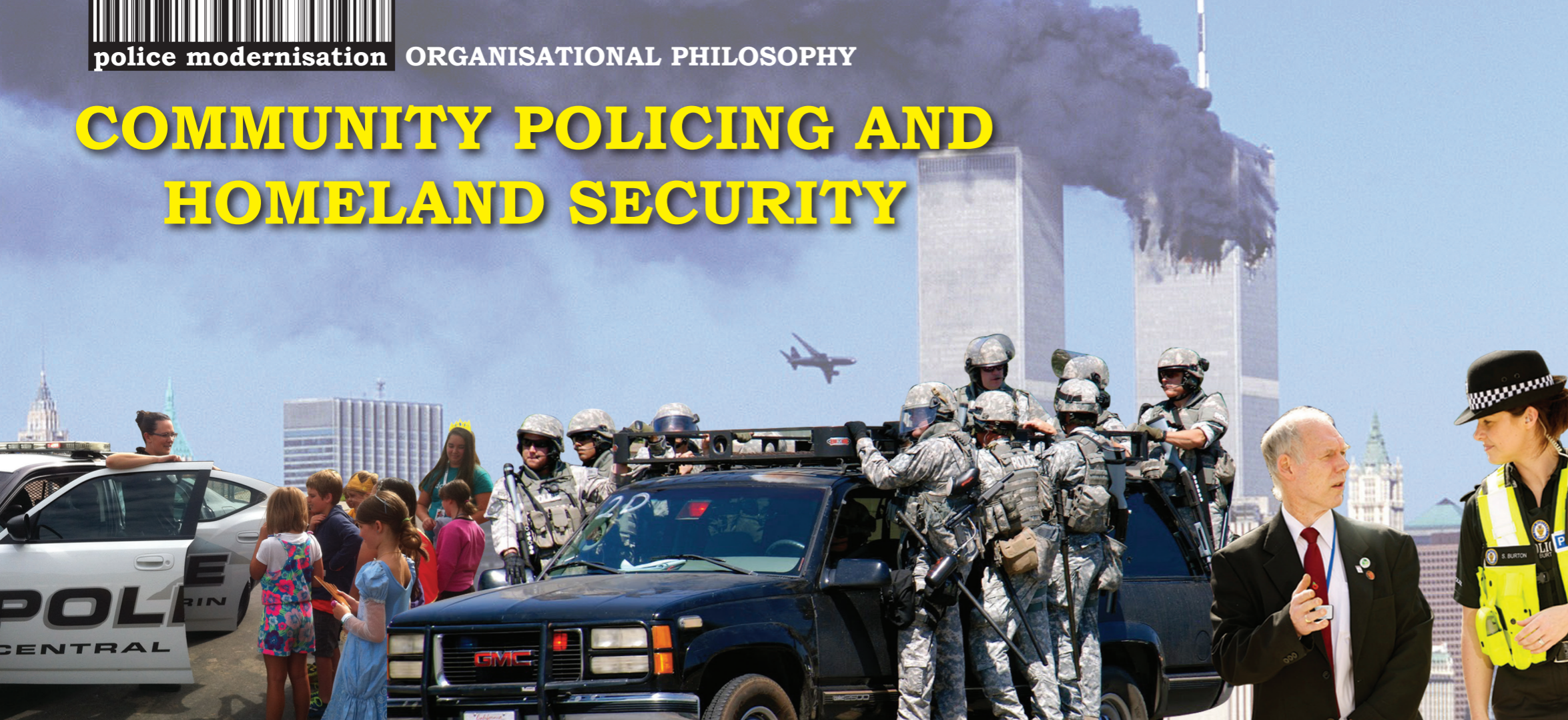
Any drone based attack in a civil area has risk of collateral damage and death of innocent civilians. This has been seen in Gaza, Afghanistan and Pakistan. A 2009 Brookings Institute report indicates that at least ten civilians died for every militant killed in a drone attack. Extensive use of UAVs for policing could be an issue for privacy rights. Imagine a UAV monitoring young people sharing private moments in Lodi Gardens in Delhi. An errant policeman could use the pictures for blackmail. CAA rules prohibit flying a UAV within 50 metres of a person, however high resolution cameras could snoop from many kilometres above. Governments could use them as a tool against political opponents. UAV sensors or data links could be jammed rendering them ineffective. They could be brought down by hard-kill. With increase in aviation density, mid-air collision risk needs attention. There have been cases of small drone being ingested in an airliner engine.

USA is already acquiring more UAVs than manned aircraft and training more drone operators than pilots. Major future air strikes will be by unmanned systems. Time is not far when a criminal could use a nano-UAV to inject poison into an official, but time is also not far when all retail delivery from pizzas to Alfonso will be through UAVs. USA operates nearly 10,000 UAVs with significant number in policing roles. The upper end UAVs like *MQ-9 Reaper* cost around US\$ 12 million *vis-à-vis* US\$ 120 million for an *F-22*. Small cheaper ones could cost just a few thousand dollars. Like the telecom revolution, India may transit direct from a low paid policeman to a tech-savvy drone cop. Soon the drone market will exceed 10 per cent of all aviation deals. UAVs will be used in swarms. UAVs are undoubtedly the best policing tool. Air is the medium of the ultimate dimension. Aerial policing is the way of the future. 

India needs to push its 'Make in India' initiative for UAVs

VVIP route sanitisation would not require 1,000 policemen any more

COMMUNITY POLICING AND HOMELAND SECURITY



LESSONS FROM THE USA EXPERIENCE

The threat of terrorism and extremism posing concomitant threats to the internal security of the nation has never been so challenging since independence as has been the case in past one decade or so. In addition to the equipping and training the State Police and Central Armed Police Forces (CAPFs) to enhance their operational capabilities, there is a need to integrate Community Policing into the organisational philosophy as studies world over have proved that when the community becomes the co-producer of safety and security along with law enforcement agencies, it contributes to national security.

As an alternative policing strategy that is adopted worldwide, community policing advocates forging of problem solving partnership between the police and the public. Community Policing revolves round the principle of proactive policing through people friendly policing practices, community participation and problem solving leading to crime prevention and maintenance of order. Community Policing allows the law enforcement to get back to the principles upon which it was founded, to integrate itself into the fabric of the community so that the people and the police collaborate even before a serious problem

arises and not merely as a knee-jerk reaction after a crisis either of crime or when a law and order situation arises. The community plays a crucial role in helping police resolve crime and disorder. Thereafter, a collaborative approach to solve the community problems is called for. Here, police act as a catalyst in the social engineering experiment. To state succinctly, community policing is a useful holistic and proactive concept and a tool to transform the police image, strengthen the force and create attitudinal changes both within the force and among the public. In its strategic dimension, it contributes to the individual, state and national security.

Core Components Of Community Policing

Community Policing consists of two complementary core components, community partnership and problem solving. To develop community partnership, police must develop positive relationships with the community, must involve the community in the quest for better crime control and prevention and must pool their resources with those of the community to address the most urgent concerns of community members. Problem solving is the process through which the specific concerns of communities are identified and through which the most appropriate remedies to abate these problems are found. Community Policing does not imply that police are no longer in authority or that the primary duty of preserving law and order is subordinated. However, tapping into the expertise and resources that exist within communities will relieve police of some of their burdens. Local government officials, social agencies, schools, church groups, business people – all those who work and live in the community and have a stake in its development – will share responsibility for finding workable solutions to problems that detract from the safety and security of the community. In other words, community becomes the co-producer of public safety and security.

Community
policing is a
useful holistic
and proactive
concept

Homeland Security

In the aftermath of the September 11, 2001, terrorist attack in the United States, a new organisational

policy was introduced as 'Homeland Security'. Both as a concept and a governmental department, Homeland Security became the 'in' policy and as such invented a new organisational approach to public safety. There was this initial apprehension that the dominant policing policy up to that time – Community Policing – would be sidestepped by the Homeland Security efforts. But in reality the two public safety policies actually have a great deal in common and that both complement each other. The policy makers of Homeland Security have integrated the principles of community policing in its localised strategies to achieve the objectives (Friedmann, Cannon 2007). Study by Kenith Roland Adcox (Community Oriented Counter-terrorism, 2014) has shown that by integrating Homeland Security responsibilities into already established and proven

community policing philosophy of local police agencies, it is possible for police agencies to successfully address both local crime and national security needs. This makes the concept of community oriented counter-terrorism a preferred organisational practice.

Community Orientation

The core philosophy of community policing has been recognised and integrated into the strategies of Homeland Security. The official website of the US Department of Homeland Security (DHS) underscores this aspect in no uncertain terms. It states 'Homeland Security begins with hometown security'. DHS continues to work closely with state and local partners and individual citizens, to raise awareness through initiatives such as the 'If You See Something, Say Something™' public awareness campaign and the Nationwide Suspicious Activity Reporting Initiative. As part of its effort to support local networks to counter violent extremism (CVE), DHS has launched a number of core initiatives, including: expanding support for local, information-driven community-oriented efforts to prevent violent crime and build safe, secure and resilient communities. The approach has proven successful in preventing crime and improving the quality of life in communities across the nation. When done effectively, community



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 a member of the National Police Mission and has been active in formulating sound policy proposals on community policing.



oriented policing has provided the foundation for dealing with a broad range of violent crime issues including those associated with violent gang activity. (<http://www.dhs.gov/countering-violent-extremism-support-local-law-enforcement>)

Utilising Volunteer Resources

After the events of September 11, 2001, the idea of involving citizens in crime prevention has taken a new significance with greater citizen involvement in homeland security through initiatives such as Citizen Corps and Freedom Corps. These programmes were introduced so that the citizens could participate directly in Homeland Security efforts in their own communities. This network of volunteer efforts uses the foundations already established by law enforcement in order to prepare local communities to respond effectively to the threats of terrorism and crime. Community policing encourages the use of non-law enforcement resources within a law enforcement agency such as volunteerism, which involves active citizen participation with their law enforcement agency. The Community policing element dovetails perfectly with the objectives of Citizen's Corps, which was developed to harness the power of every individual through education, training and volunteer service to make communities safer, stronger and better prepared to respond to threats of terrorism, crime, public health issues and disasters of all kinds. There are four programmes in Citizen's Corps: Neighbourhood Watch, Volunteers in Police Service (VIPS), Community Emergency Response Teams (CERT) and Medical Reserve Corps (MRC), all of which integrate well with the community policing philosophy. In fact, Neighbourhood Watch has been an integral component of the community policing philosophy virtually since its inception (Jose Docobe, 2005).

Community Policing does not imply that police are no longer in authority

Comparison Of Two Ideals

"Although both Homeland Security and Community Policing policies are designed to thwart serious crime and terror, each maintains a similar conceptual design that centres on effective reaction and response to potential disasters and instances of serious criminal activity. Both strategies incorporate a traditional reactive function, alongside a proactive approach, in which they seek to utilise the bonds that are formed from partnership with community and government agencies" (Friedmann and Cannon: Homeland Security and Community Policing, 2007). The authors have summarised the commonalities between both the policies as follows:

- Use of information gathering as a preventive tool
- Emphasis on cooperation between local, state and federal agencies
- Work to build successful community partnership

- Utilise both proactive and reactive measures (with different emphasis)
- Aim at enhancing public safety

Key Features Of Community Policing

Community Oriented Policing (COP), Community Based Policing, Community Oriented Policing and Problem-Solving (COPPS) all refer to a model or philosophy of policing that is based on three fundamental concepts.

- Focus on **problem-solving**, rather than simply handling calls. This is a very **proactive** approach, rather than a traditional more reactive approach. It has spawned many programmes to improve the ability of the police to be effective in crime prevention.

- **Decentralisation** of service and decision-making.
- The final fundamental component is in developing **partnerships** with other governmental agencies, NGOs and local groups in the community. This component recognises the inability of the police alone to solve social or individual problems that may lead to crime. Depending on the nature of an underlying, causative problem the police may need to partner with organisations as diverse as public works, domestic violence groups, churches etc.

Since 1994 the Federal Government has been making sustained efforts to promote the culture of community policing among the police agencies in the United States. The Violent Crime Control and Law Enforcement Act of 1994/Public Safety Partnership and Community Policing Act of 1994 passed by both the House and the Senate paving the way for financial assistance to police agencies. The office of the Community Oriented Policing Services (COPS) was created under the Department of Justice to coordinate the programmes nationwide. With the support of COPS a number of community-oriented training programmes have been introduced, important ones being New Perspective on Community Policing, Police Training Officers Programme, Regional Community Policing Institutes (RCPIs). The COPS collaborate with a number of universities and engage academics to do research in the field of Community Oriented Policing and provide rich inputs to the police leaders and practitioners.

In the years since September 11, 2001, terrorist attacks on WTC there has been increasing emphasis by the local, state and federal law enforcement agencies on the community oriented policing in the prevention and response to terrorism. The US Department of Homeland Security has been emphasising the significance of community policing in its mission of protecting and preventing terrorist attacks and has recognised that Community Policing and Homeland Security complement each other.

Community Policing: The Indian Scenario

A number of successful community policing schemes have been launched in the States/UTs of India, either with the initiative of the State/UT governments or with that of police leaders. Individual initiatives, it is seen at several instances, suffer from predecessor-successor syndrome. There has been lack of uniformity in application of the initiatives. The initiatives have rarely been implemented as a public policy except, which could have ensured much needed legal, institutional framework and budgetary support for the scheme to be integrated into mainstream policy of the state. However, in recent years, states like Kerala and Odisha have introduced their respective community policing schemes as public policy – the *Janamaithri* and *Ama Police* respectively.


The National Police Mission (NPM) under the aegis of Bureau of Police Research and Development, Ministry of Home Affairs, constituted in the year 2008, is mandated with creating a new vision for Police. There are several micro-missions under the NPM, each charged with a specific area of policing like Human Resource Development, Community Policing, Communication and Technology, Infrastructure, Process Engineering etc. Micro Mission-II is charged with formulating sound policy proposals on community policing. The Mission has submitted several policies on community policing including an overarching model which has been approved by Ministry of Home Affairs. However, policing being a state subject, it remains the prerogative of the state government whether to adopt these schemes as a public policy.

Lessons To Be Learned

The threat of terrorism and extremism posing concomitant threats to the internal security of the nation has never been so challenging since independence as has been the case in the past one decade or so. In addition to equipping and training the State Police and Central Armed Police Forces (CAPFs) to enhance their operational capabilities, there is a need to integrate community policing into the organisational philosophy as studies world over have proved that when the community becomes the co-producer of safety and security along with law enforcement agencies, it contributes to national security.

- As the office of the Community Oriented Policing Services (COPS) under the Department of Justice, US Government, the Micro Mission-II (Community Policing) of National Police Mission, BPR&D, Ministry of Home Affairs of Government of India may act as the Nodal Agency for the entire country.
- Like the Ministry of Justice of the US Government, the Ministry of Home Affairs of Government of India may make provision for annual budgetary allocation for sponsoring and funding community policing schemes by the State/UT Police under Modernisation of Police Force.

- Ministry of Home Affairs, Government of India may issue advisories to the State/UT governments for implementation of the national overarching model on community policing submitted by the Micro Mission-II of the National Police Mission.
- The new Draft Police Bill, which underscores the importance of community policing, is to be legislated by the State governments expeditiously to provide the states with statutory powers for introducing various schemes of community policing akin to that in the Public Safety Partnership and Community Policing Act of 1994.
- The mission statement of the Indian police should be redefined with emphasis on community policing as in case of majority of the police agencies in the United States.
- Like in the US, the Homeland Security underscoring the need of community policing in prevention and response to terrorism the National Security Council may play a similar role in advising the State and UT governments to implement various community policing initiatives.
- As in case of COPS, Ministry of Justice (MoJ), the Government of USA, the Bureau of Police Research & Development (BPR&D), Ministry of Home Affairs (MHA) should collaborate with academics and universities to encourage research in the field of community policing.
- The BPR&D may identify State Police Academies as State level Community Policing training centres for training of the police personnel and civilians (PTO programme of the COPS, DoJ, USA).
- The Bharat Nirman Volunteer (BNV) is an individual who comes voluntarily from a rural household to act as an organic link between a group of families and hosts of various line departments with a purpose to ensure the unreached households to access benefits under various government sponsored programmes. They could be excellent resources for partnering with the local law enforcement agencies like the Citizen Corps of the United States.

In spite of differences between the organisational structures of police between the USA and India, both nations are democracies with rule of law as the guiding principle. The accountability and scrutiny of the police function is enormous in both the nations by the independent judiciary and robust oversight agencies monitoring and overseeing the police functions. The legal and institutional framework for adopting community policing as the organisational philosophy by the police departments in the USA and the focus on community policing by the Homeland Security in the aftermath of 9/11 terrorist assault are the vital learning points for India which faces far more challenging threats to national security than the USA. It is time that community policing be given its due and be introduced as public policy by the police organisations with financial support under the modernisation of police forces. 

POLICE COMMUNITY RELATIONS A BRIDGE TOO FAR?

Governed by the Police Act of 1861, police organisation smacks of colonial hangover: It was meant primarily to control *subject* people, rather than to serve the people. May it be noted that Model Police Act, put together in 2006, underlines community participation (Sec 102) and provides for ‘PS Community Liaison Group’, ‘Village Guard’, ‘Village Defence Party’, ‘Citizens’ Policing Committee’ etc. Pity that the ‘model’ is yet to be adopted and implemented anywhere, in any State or Union Territory.



In modern times, police make for the pivot on which civil society moves. Praise it or criticise it, but the society has to have police in one form or the other. And India has had *regular* police for a long, long time. In post-independence period, this institution has served the country well. Although the country had a long feudal and colonial background and little or no experience of

democratic governance, it opted for democracy and all that goes with it. Skeptics and naysayers made gloomy predictions, yet democracy has survived in the country. Quite a few studies underline the role of the police in lending a helping hand in nurturing democracy and related democratic institutions in this sprawling subcontinent-size and populous country. Similarly some studies underscore its

enabling role in economic development. At the time of independence, the country was face-to-face with acute economic problems and it opted for planned socio-economic development to overcome these. And the implementation of planned projects and schemes required administrative and logistic support – in which the police readily joined forces.

Over past sixty years, the country has taken long strides in economic development and in raising the quality of life of the people; and, in this, the contribution of police is described to be substantial. The experience and situation of other developing countries in south-east Asia and elsewhere, mostly indifferent, reinforces these assertions.

Role Reversal

However, it would be difficult to ignore the flip side of police and the shortcomings in the functioning of the police. The main function of police is prevention of crime – which enables people to have a sense of security, live in peace, exploit their talent and work to their potential, so as to experience growth and contribute to the growth of the society. The police function of crime-prevention is followed by crime investigation and maintenance of law and order including *bandobast* for VVIP security. This is also globally accepted order of priority in police functioning. Yet, in most States in India, this order of priority in police working appears to have gone upside down – the VVIP *bandobast* is accorded top priority and every other police function is subject to the availability of time. Rural policing and night-patrolling have reduced to being namesake. Few worry about police ‘response time’ to reports of criminal occurrence, especially in rural areas. Investigation of crimes by police, too,

leaves much to be desired, both in terms of time and quality. And both of these limiting conditions cumulatively show up in the abysmally low conviction rates in courts, heavily telling upon the popular perception of the majesty of law and criminal justice. Although the eggheads have all along been insisting that the ‘third-degree method’ is not used by ‘the best investigation officer’, the use of these wholly illegal methods of crime investigation has persisted, as is evident from deaths in police lock-up and from frequent media reports, issues of human rights and fundamental rights notwithstanding.

Corruption

While monetary corruption is not unique to police department, it is certainly most visible. Over the years, several anti-corruption agencies have been set up (for example Vigilance, ACB, CVO, CBI etc), but public perception about corruption in police has seldom dimmed: Street vendors pay *hafta*, truck-drivers pay for *chai-pani*, suspects pay gratuity or *shukrana* for diluting the gravity of their offence or even for tinkering with incriminating evidence. Maybe the police force has only a fringe of unscrupulous officers given to bribery, it maligns the entire force, nevertheless.

That in many States police personnel are still given to feudal, coercive and high-handed approach in their working is abundantly shown by what happened in Hashampura in Uttar Pradesh 28 years ago and very recently in Tirupati in Andhra Pradesh. Police picks up scores of persons *suspected* for some minor offence, takes them to a solitary place and summarily shoots them dead. Does it speak well of police accountability? At best, police is enforcing law through unlawful means and, at worst, police is still deep into antediluvian barbaric style of functioning.

All this has added to the distance between police and public. Not many would voluntarily report a criminal occurrence to police; few would willingly appear in court as witness; and still fewer would stand by police in maintaining law and order and in crisis situations. That the hiatus between police and public is adversely affecting police working and effectiveness is apparent.

Underlying Reasons

Why police remains wanting in its functioning could be explained in many ways. In a cynical way, it may be said: People get the type of police they deserve.



Dr MZ Khan

The writer is former Professor of Social Work and also served as Dean, Faculty of Social Sciences, Jamia Millia Islamia University, New Delhi. He is associated with several governmental, professional and voluntary organisations. He is past President of Indian Society of Professional Social Workers and past President of Indian Society of Criminology.

For healthy police-community relations, the KOBAN system of Japan could be referred to

STATE POLICE IN INDIA (2014)	
Police Zones	101
Police Ranges	179
Police Districts	718
Police Stations	14, 786
Number of police persons (in lakh)	17.2
Police persons per one lakh population	140
Police persons per 100 square kilometre	54.4

Source: NCRB New Delhi

There may be an element of truth in this. People, particularly those in rural and tribal areas, have low literacy and information level and are less assertive. Only rarely do they raise their voice should the police working be unfair or arbitrary. Besides, there are several structural reasons, also. Governed by the Police Act of 1861, police organisation smacks of colonial hangover: It was meant primarily to control *subject* people, rather than to serve the people.

May it be noted that, since the beginning, India has had 'State police' and not county police or prefecture police, as is the case with several forward-looking countries. 'Superintendence of the police is to be exercised by the State government' and it is only the State headquarters, often situated at a far off distance, which acts or reacts to what police functionaries do or do not do. As a result, local communities or local bodies have little or no say, should a police functionary go astray and transgress legal boundaries or rules.

This kind of disconnect between police and community augurs well neither for police working and efficiency nor for peace and tranquillity in society. From among a large number of countries, which lay store on healthy police-community relations, the KOBAN system of Japan could be gainfully referred to.

KOBAN

Japan has evolved a community-based security system which is called KOBAN. Under this system, Police Boxes are set up in urban areas and Residential Police Boxes in rural areas. Typically both are manned by a police officer equivalent in rank to an Assistant Sub-Inspector. Located in urban neighbourhoods, Police Boxes are sourced, on shift basis, by the concerned police-station. On the other hand, in small towns and villages, there are Residential Police Boxes, each having one residential officer who lives in the Box along with her/his family. Both Police Boxes and Residential Police Boxes function to ensure crime-prevention and to strengthen security in the community. These police officers keep a watch on the goings-on in the neighbourhood, day and night. They undertake patrolling of the area under their charge and, while patrolling, they also question suspicious persons moving around in the locality. They speedily reach the scene of crime, should a criminal incidence take place in their area and accordingly inform concerned higher police authorities. Furthermore, they remain in close touch with the members of the community: They pay door-to-door visit, have a chit-chat with residents, send out from time-to-time newsletters and set up Liaison Council comprising community members and leaders in order to have stable peace and security in the neighbourhood.

A while ago, Japan had 6,500 Police Boxes and 7,600 Residential Police Boxes. Together, these have made 'the land of the rising sun' as one of the most peaceful and safest countries. Hardly surprising,

Singapore and many cities in the USA have also opted for KOBAN. Does the KOBAN system have a relevance to policing in India, also?

Police-community Relations In India

This is not to say that we in India have been unaware of the importance of police-community relations. Section 17 of the Police Act of 1861 does provide for the appointment of Special Police Officers (SPOs) from among neighbourhood residents. However, this provision has been rarely implemented; and still more rarely implemented is Sec 18 which specifies that SPOs would have equivalent (police) powers. May it be noted that Model Police Act, put together in 2006, underlines community participation (Sec 102) and provides for 'PS Community Liaison Group', 'Village Guard', 'Village Defence Party', 'Citizens' Policing Committee' etc. Pity that the 'model' is yet to be adopted and implemented anywhere, in any State or Union Territory.

This apart, over the years, police has often tried to reach out to the community. Earlier on, in some States, police had organised Juvenile Aid Police Units and Juvenile Aid Bureaux (which have now been replaced by Special Juvenile Police Units under the Juvenile Justice Act). For quite some time, the NCT of Delhi has had honorary Traffic Wardens. In Tamil Nadu, police districts have Counselling Centres for rape victims; and so is the case with Crisis Centres in Delhi. Many more similar initiatives could be mentioned which bring out, at least partially, the intent to bring police closer to community. Nonetheless, these remain essentially episodic, mainly for want of formal and institutional arrangements.

Ripple Effect

Preventing crime and instilling a sense of security in the people is an uphill task and for this steady and institutionalised police-community partnership is not mere desirability but it is a necessity. Such a partnership would augment police resources (even otherwise the present ratio of 140 police persons per lakh population in the country is patently on the lower side). This would garner public support and cooperation in different functional domains of police working – be it maintenance of law and order, reporting of crime, crime investigation or testimony in court. Not only would this brighten the image of police in public mind but it would also enhance its efficiency and effectiveness. Towards this, an amount of strategic thinking is called for to involve community in police work at different levels. Perhaps KOBAN system may be considered in this regard. Maybe *panchayati raj* institutions can also be roped in. Above all, policy makers and police hierarchy have to do some out-of-the-box thinking to rejuvenate police-community relationship and to endow police and police working with the ability to face challenges of the twentyfirst century. **DSA**

Strategic thinking is called for to involve community in police work



NAVNEET R WASAN
DIRECTOR GENERAL
BUREAU OF POLICE RESEARCH & DEVELOPMENT

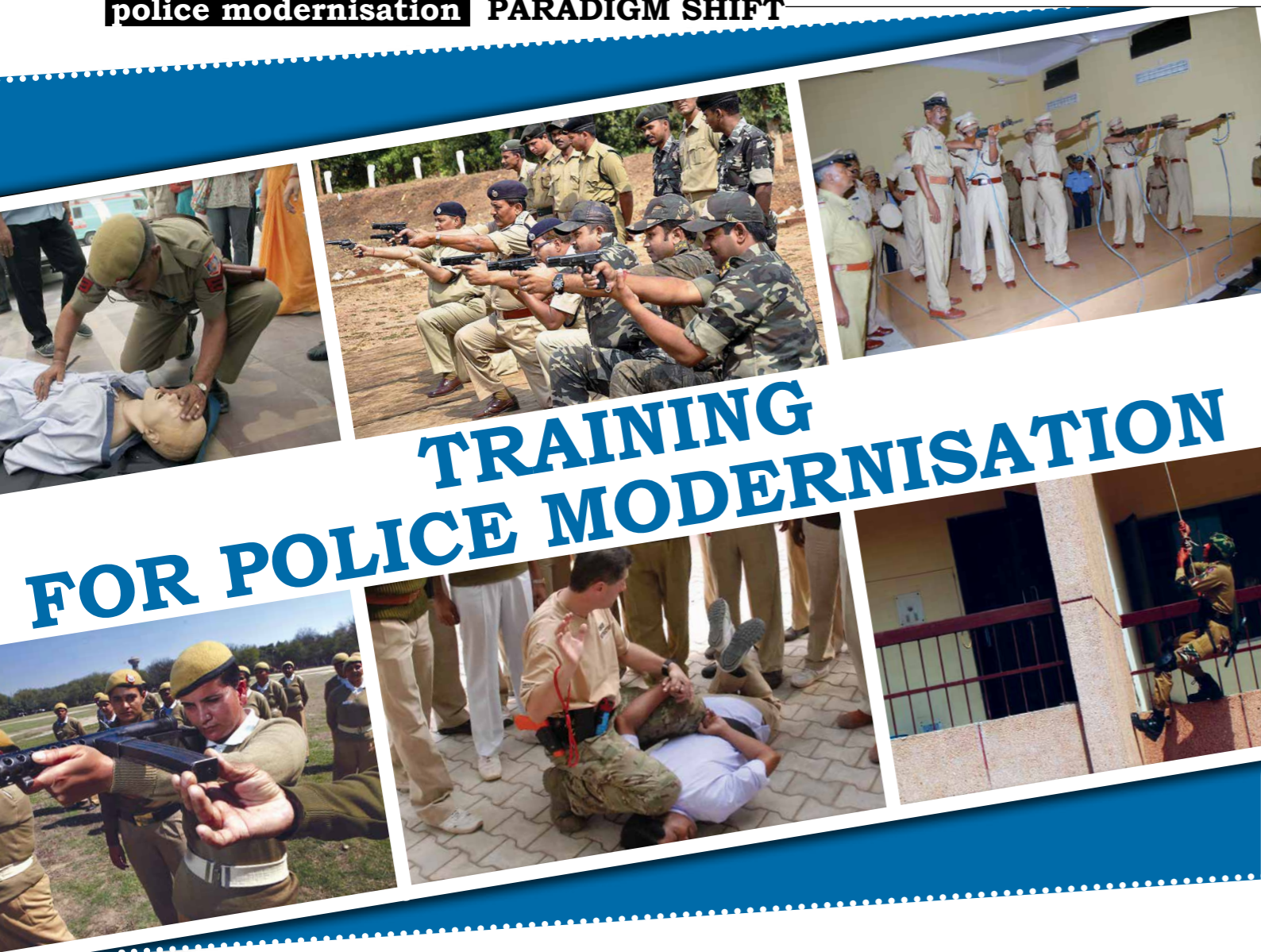
Navneet Rajan Wasan, an Indian Police Service officer, holds a postgraduate degree in International Relations and MPhil from School of International Studies, Jawaharlal Nehru University, New Delhi. He later earned Law Degree from University of Delhi and Post Graduate Diploma in Management (PGDM) from Management Development Institute, Gurgaon.

In his thirty three years of police service, he has served in different capacities in State of Andhra Pradesh, Central Bureau of Investigation, National Investigation Agency and is now working as Director General, Bureau of Police Research & Development, New Delhi, where he is supervising research in police related subjects and also handling training of senior police officers in India and outside. He was decorated with Indian Police Medal in 1996 and with President's Police Medal in 2004 for his illustrious service.

After handling district policing at important towns in State of Andhra Pradesh he was with Central Bureau of Investigation for over seventeen years and held major assignments which included supervising investigation of corruption related offences, bank and financial frauds, economic offences, conventional offences and collection of intelligence. He also supervised the functioning of National Central Bureau, India (INTERPOL) and handled international cooperation in investigation of criminal cases. He has interacted with several countries on matters of mutual interest. He worked as Special Director & Director General with National Investigation Agency, a Federal Investigation Agency where he supervised investigation of terrorist related cases.

His major area of interest has been investigation and use of Information Technology in Police functioning. He has made presentation at the meeting of heads of NCBs in 2006 at Interpol Headquarters on need for International Cooperation in Cyber Crime and addressed delegates on issues relating to Cyber Crime Investigation at 1st Cyber Security Conference held at Hong Kong in September 2010.





TRAINING FOR POLICE MODERNISATION

In the Indian Police departments, the training remains a neglected wing and very often the people sent for training are those who are considered spare, near retirement and many a time they are working in a unit not related to the training theme. And on return from training, the skills acquired by the police officers in the training programmes are seldom put to use as their job responsibility is rarely decided on the basis of training programmes attended.

The Gore Committee set-up in 1971 by the government to look into the aspect of police training came to the unflattering conclusion that police training had been badly neglected over the years and training arrangements, by and large, were unsatisfactory, both in quantity and quality. It found that training institutions failed to take note of the changing situations and develop realistic training programmes.

The police departments today remain stuck with antiquated and uninspiring training methods, contents that have little applicability in the field and to future policing needs and an organisational environment that has little support for training. As rightly observed by the Supreme Court, a paradigm

shift in the basic approach to police training is the need of the hour and the police departments will have to adopt some of the new strategies as the current practices in training suffer from some fundamental flaws in content and approach.

Absence Of Specificity

Police training is rigid evolving from the law, policies, procedures and rules that are followed in strict conformity by the police department. However, the studies and practical experience show that traditional police training curricula are designed to instruct recruits in what they will be doing just 10 per cent of the time while on duty ie law enforcement functions. The traditional police training does not deal with

specific problems the police are expected to handle and the methods to deal with them. This is one of the major reasons why recruit training has so often been criticised as having no relevance to the job. As soon as a police officer reaches the police station, he has first of all to unlearn what he has been taught in training institutions.

The other neglected aspect in police training is that it is weighted towards technical aspects of police work and does not prepare the officers for the everyday interactional tasks that they perform. For effectiveness, the training needs should be identified through a top-down and bottom-up approach, with inputs from the staff at the police stations, so that there is a 'connect' between the teaching and practical daily police work at the cutting edge.

Problem Based Learning

As per the report of the National Police Commission, 1977, 49 per cent duties performed by a constable call for exercise of higher degree of initiative, discretion, judgement etc and 37 per cent duties involve a combination of application of mind and exercise of judgement – together they constitute about 86 per cent of the duties. However, the present police training process still lays emphasis on the lecture mode for teaching suited for children, whereas adults learn new knowledge, understanding, skills, values and attitudes most effectively when they are presented in the context of application to real-life situations.

The basic approach to police training should, therefore, highlight Problem-based learning (PBL) on the part of trainees that engage the recruit in real-world ill-structured problems that interconnect the curriculum and cause the recruit to think. This can be extremely important for the police officers when they are relating to problem-solving, conflict resolution, cultural, religious and social diversity at work. While the police recruits at present, even at the level of Assistant Sub-Inspectors and Constables, are highly qualified, police training must be active, engaging and relevant for the recruits and in-service personnel who attend professional development courses.

Numerous law enforcement agencies are moving to the PBL training model. Academies in Washington, Kentucky and California are changing their instructional style to reflect current learning and teaching needs. The Royal Canadian Mounted Police has used PBL in their training academy for years and are the leaders in self-directed training.

Emotional Intelligence Is Critical

Emotional intelligence includes the way police officers manage their emotions and the way they manage their contacts and relationships with others. Emotional intelligence has an enormous role in policing, particularly in developing new officers and solving the most common issues that create problems for the department and the individual such as police

misconduct and brutality. These problems develop when police officers are unable to empathise with others or control their impulses and emotions.

Therefore, in order to prevent incidents of police brutality more inputs on personality development, communication skills, human values, sense of belongingness to society, self-awareness, problem-solving, describing and analysing police misconduct, training on ethical standards and police myths and cynicism may be more useful. Once the recruit has a solid foundation in these areas he or she will be prepared to better understand his or her professional value system and the environment during the formative period in the academy.

Capacity Building

With the advent of the Internet, increased flow of manpower, trade and crime, even the training needs are becoming globalised. Exchange of ideas, information and expertise can play an important role in the training of police officers. In the Netherlands, the Police Knowledge Network (PKN), which is a form of digital databank, occupies a special position among the centres of expertise.

The databank serves as a repository of the knowledge of the Police Training and Knowledge Centre, the police forces and the external partners and can be consulted online by police officers. The data consists not only of documented knowledge taken from textbooks and training modules, but also practical information that can be used in situations the police officers confront on a daily basis.

A similar network of the police academies in India would strengthen and supplement their training resources, further their integration with the international networks and can help them to access from international standards and wide knowledge database in policing.

Organisational Support

Organisational support to training remains one of the most important issues. If the police department itself remains hostile or indifferent to training, any amount of good training will not show significant positive effect. Since 1997, the Singapore Police Force (SPF) has been a fervent practitioner of learning organisation concepts. Recruiting only the



Rohit Choudhary IPS

The writer is Additional Director General of Police, Punjab. He is IPS officer of 1988 batch and has served in Punjab state as police chief of three districts and played a key role in combating militancy in Punjab and has held various headquarters and field positions as Deputy Inspector General and Inspector General of Police. He was awarded with two gallantry medals for action in anti-insurgency operations and the President's Police Medal for Meritorious Service. A postgraduate in Public Policy and Management from Syracuse University, New York, he is credited with path-breaking book *Policing: Reinvention Strategies in a Marketing Framework*.

A paradigm shift in the basic approach to police training is the need of the hour



best talent, a majority of SPF recruits are degree or diploma-holders, ensuring intellectual propensity for learning. Subsequently, the mental models of officers are then shaped through training.

In the Indian Police departments, the training remains a neglected wing and very often the people sent for training are those who are considered spare, near retirement and many a time they are working in a unit not related to the training theme. And on return from training, the skills acquired by the police officers in the training programmes are seldom put to use as their job responsibility is rarely decided on the basis of training programmes attended.

Not only the training academies at the state level, but also training schools in every district should function as subsidiary knowledge centres and should be given their due importance and earmarked funds. Regular, short and focused capsule training courses of two to three days in the district police lines with the help of faculty from outside could be of immense benefit to the police officers in polishing their soft skills for the interface activities with the public.

Exchange of ideas, information and expertise can play an important role in police training

- Economic and political situation with social and political unrest, economic crunch, massive population, unemployment, juvenile crime and further migration waves to exploding mega cities
- Challenge to tackle terrorism, underworld and spreading Naxalite movement, which is affecting one-third districts in the country
- Developing the necessary skills for maintaining quality standards that the public has begun to expect would be critically dependent on the skills developed in the policemen at the cutting edge. Unlike other professions where the entrants to the service are selected on the basis of their professional competency and the necessary skills are predominantly pre-acquired, the policemen get to learn the basics of their profession only through in-service training. Therefore, their skills, attitude and competencies depend to a large extent on the training they receive in the police academies. The training programmes should be used to herald a new strategic thrust and a commitment to the police department's mission, vision and values.

Future Training Needs

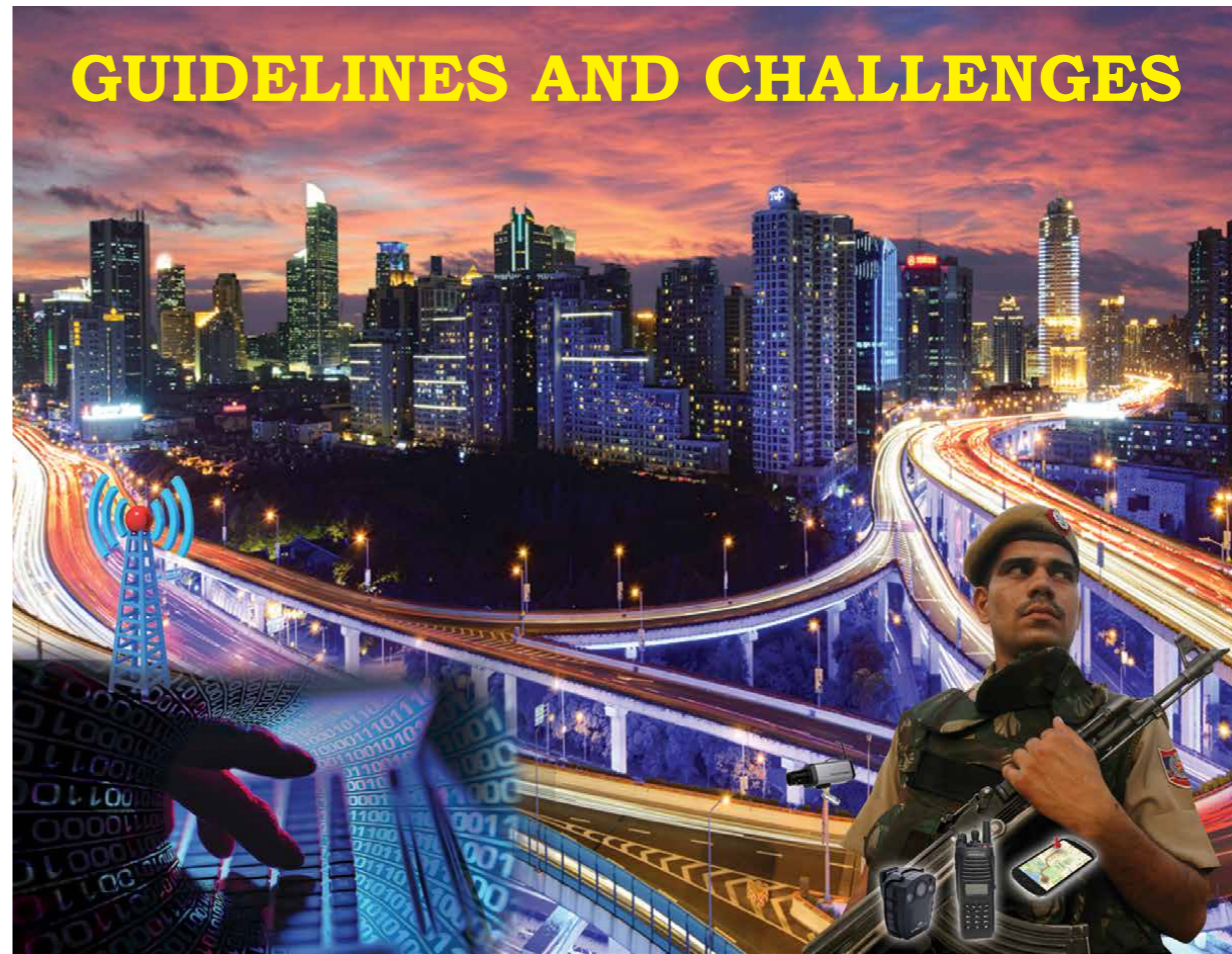
Training programmes for the police, which remain outmoded, should be reviewed and continuously improved to maintain their relevance and efficacy. While taking care of the current needs it is essential that the training also looks at the preparedness of police officers in terms of what demands future would place on them. For a future police training and planning, the following external factors have to be taken into account:

- Increase of the police product in volume, gravity and complexity, aggravated by the expanding international dimension requiring new resources, connections and information exchange
- Development of new technologies providing criminals new means to commit crime and effective communication systems

Broad Base Training

Here is a synopsis of strategy for the training of personnel for police modernisation:

- Move to the problem-based learning method
- Determine the training needs through a top-down and bottom-up approach
- Developing emotional intelligence of police officers should be a critical part of every teaching in the police department
- Strategic partnerships between training institutes, police knowledge networks and individuals for online exchange of ideas and expertise
- Regular short capsule training courses in every district on soft skills
- Supportive environment within the department for training **USA**



GUIDELINES AND CHALLENGES

FOR POLICING A SMART CITY

A Smart City cop would be equipped with necessary gadgets such as GPS enabled smart phone, wireless communication, body-worn camera etc. A smart patrol car would have ruggedised laptops from where information from field would be uploaded and queries made from central server. Smart City of future may also have completely autonomous and intelligent Robocop to interact with humans while patrolling public places.

Smart City is a buzzword today. Barcelona, Da Nang, Edmonton, Fort Lauderdale and Rio de Janeiro are some of the cities already on a path to make themselves smarter. During the recently held 49th Annual Conference of Directors General of Police/Inspectors General of Police and heads of all Central Police Organisations, honourable Prime Minister Narendra Modi gave a new slogan for 'SMART' police which is Strict and Sensitive, Modern and Mobile, Alert and Accountable, Reliable and

Responsive, Techno-savvy and Trained. He has also shared his vision of building 'Smart Cities' in India and Union Cabinet has recently 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. City-wise task forces are also being set-up by the Urban Development Ministry. Apart from smart citizens, a Smart City is also likely to attract smart and hi-tech criminals



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 NTRO, 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 graduated in Electronics and Telecommunication Engineering from Delhi University in first class with distinction. He also holds a law degree from Delhi University and Masters Degree in criminology. He has recently been awarded PhD in Information Security Management by IIT, Delhi. He has been awarded Police Medal for Meritorious Service and President's Police Medal for Distinguished Service.



from both physical world and cyberspace, throwing enormous challenges for police. It is time for the police leadership of the country to assess and anticipate the policing needs of Smart Cities and prepare 'SMART' police which is fair, transparent, efficient, effective, participative and accessible.

Evolving Standards

There are several ways of visualising a Smart City. A Smart City is necessarily a mix of smart infrastructure, smart people, smart governance, smart environment, smart connectivity and smart mobility etc, all of which are aimed at providing better quality of life to its citizens through better governance. It is a digitally connected city with intelligent systems communicating with each other. At its fifth meeting in June 2014, the Focus Group, set-up by International Telecommunications Union (ITU), agreed on the definition of 'Smart Sustainable City' as follows: "A smart sustainable city is an innovative city that uses information and communication technologies (ICTs) and other means to improve 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". Venkaiah Naidu, Minister of Urban Development and Housing and Urban Poverty Alleviation, Government of India, has broadly defined a Smart City as one that makes urban life comfortable and improves living standards through good governance, efficient health care services and education, 24x7 power and water supply, efficient transport, high quality sanitation, employment to the needy and robust cyber connectivity and benefits all irrespective of income, age and gender. India Smart Grid Forum (ISGF) is developing a standard framework for infrastructure domains of Smart Cities, including a Smart City Maturity Model (SCMM). An Expert Committee has been set-up recently by the Bureau of Indian Standards (BIS) on determining the standards for the various components of Smart Cities.

India Smart Grid Forum (ISGF) is developing a Standard Framework for Infrastructure domains of Smart Cities

Criteria For Inclusion

It is proposed that 100 cities would be selected according to the following criteria:

- One satellite city of each of the cities with a population of 4 million people or more (9 cities)
- Most of the cities in the population range of 1-4 million people (about 35 out of 44 cities)
- All State/UT capitals, even if they have a population of less than one million (17 cities)
- Cities of tourist, religious and economic importance not included in above (10 cities)
- Cities in the 0.2 to 1.0 million population range (25 cities)

International Organisation for Standardization (ISO) has published ISO 37120:2014, "Sustainable development of communities – indicators for city services and quality of life", which lists a set of clearly

defined city performance indicators and a standard approach for measuring each of them. Section 14 of the standard deals with Safety. British Standard Institute (BSI) has also come up with PD 8101:2014 "Smart Cities – Guide to the role of the planning and development process". This is a part of a suite of BSI publications related to Smart Cities:

- PAS 180, Smart Cities – Vocabulary, which defines terms for Smart Cities, including Smart City concepts across different infrastructure and systems elements and used across all service delivery channels;
- PAS 181, Smart City framework – Guide to establishing strategies for Smart Cities and communities, which gives guidance on a good practice framework for decision-makers in Smart Cities and communities (from the public, private and voluntary sectors) to develop, agree and deliver Smart City strategies that can transform their cities' ability to meet future challenges and deliver future aspirations and
- PAS 182, Smart City concept model – Guide to establishing a model for data interoperability, which provides a framework that can normalise and classify information from many sources so that data sets can be discovered and combined to gain a better picture of the needs and behaviours of a city's citizens (residents and businesses).

Core Police Functions

From the policing point of view, on the law and order front, providing a safe and secure environment and from traffic management point of view, providing mobility with safety, would be the key areas of focus in a Smart City. The first point of presence of police in a Smart City are its web portal, mobile applications and social media which are designed to minimise human intervention and are capable of offering various police services such as lodging of first information report, missing report about things or persons, crime prevention advisories, status of complaints and other police services. Smart City police would have to use various social media platforms to connect with its citizens for functions such as updating police activities, issue press releases, traffic alerts about congestions, special events, diversions, road conditions, crime prevention advisories, dispel rumours, tracing suspects and missing persons, emergency notification, community policing, identification of criminals, their activities and locations etc. They would also need to patrol cyber beat of Smart City to collect Social Media Intelligence. Social Media Monitoring would also be required for extracting effective tactical and actionable intelligence, collect evidence, prevent rumours etc. The core functioning of police would necessarily be computerised with police having real time access to databases of other systems such as driving licences, vehicle owners, telephone subscriber

information, banks, airlines etc. This big data would be continuously refined and advanced analytics would be used to find patterns and relationship for predictive policing. There would be a vibrant public interface unit for two-way communication with citizens through multiple digital media.

Extensive CCTV Coverage

Smart City would need an extensive, intelligent, IP based CCTV surveillance network which would have built-in video analytics to generate timely alert for operator in case of any incident such as detection of suspect, intrusion, unattended object etc. Facial recognition at airports, railway terminals, large gatherings, shopping malls and business centres would automatically identify and track wanted criminals, suspects and vehicles. Intelligent Traffic and Transportation System would be essential for ensuring efficient 'mobility with safety' in a Smart City. The adaptive traffic signals would be switching intelligently guided by a central computer as per the need of the traffic volume at the junction and adjoining area. It would allocate green time for motorists and pedestrians based on demand. It would be possible to provide 'green wave' between adjacent junctions to minimise the number of stops by vehicles. The traffic management would also need specialised CCTV camera with Automatic Number Plate Recognition (ANPR) system at borders, critical road junctions and other places, which would generate alerts in case of any accident, traffic jam, driving against traffic flow, detection of stolen or suspect vehicles etc. Automatic CCTV based enforcement of traffic signal violations, over speeding, lane indiscipline, stop line violation, wrong parking etc would be needed for prosecution of traffic rule offenders. GPS enabled e-challenging of motorist would not only ensure that prosecution history of drivers is available but also make it possible to realise enhanced penalties for repeat traffic offenders and payment of fine using credit/debit cards. The driver of a vehicle would be able to decide his route intelligently using smart in-car navigation devices and Variable Message Signs (VMSs) which would guide him about congestion, diversions, estimated journey time and available parking slots nearby etc. The traffic signals in a corridor would be able to identify approaching emergency vehicles so as to give priority passage to it by pre-empting the signal.

Mod-bod Gadgets

A Smart City cop would be equipped with necessary gadgets such as GPS enabled smart phone, wireless communication, body-worn camera etc. A smart patrol car would have ruggedised laptops from where information from field would be uploaded and queries made from central server. Smart City of future may also have completely autonomous and

intelligent Robocops to interact with humans while patrolling public places. Real time Geographical Information System (GIS) based crime mapping and prediction using Big Data would be required for crime prevention. An essential requirement of a Smart City would be integrated and intelligent command, control and operations centre with huge video walls where all agencies are able to coordinate their emergency responses with GPS enabled resource mapping on 24x7 basis. For this a Computer Aided Dispatch (CAD) would be a necessity. Smart City police may have to use services of helicopters and drones for aerial surveillance of large events, traffic management and anti-terrorist operations.

Sanitised Against Cyberattacks

Information Communications Technology (ICT) is the most essential backbone of Smart City. The Estonia Cyber Attack of 2007 is a grim reminder that, digitally interconnected, interdependent and complex Critical Information Infrastructure of a Smart City would be highly vulnerable to cybercrime and cyber terrorism if not properly protected. With free Wi-Fi hotspots, Internet of Things (IoT), embedded wireless sensors, Supervisory Control and Data Acquisition Systems (SCADA) spread all over a Smart City, these systems would have to be safe, secure, reliable, robust and resilient. Apart from the Guidelines issued by National Critical Information Protection Centre (NCIPC), Government of India, there may be a need to formulate further directions for the protection of ICT assets of a Smart City. ISO/DIS 37101 "Sustainable development of communities – Management systems – Requirements with guidance for resilience and smartness", which is under final stage of development, would be highly useful. A 24X7 Cyber Security Operations Centre would also be needed to provide early warning, detect and prevent cyberattacks. The occurrence of cybercrimes will definitely be more than any other type of crimes in a Smart City. Since police is authorised to investigate all offences under Information Technology Act, a Smart City may also need a Chief Information Security Officer for the city apart from the Commissioner of Police.

The first point of presence of police in a Smart City are its web portal, mobile applications and social media

Police is an important stakeholder in a Smart City. It is recommended that an expert group is set-up in the Ministry of Home Affairs, Government of India, to go in the details of various requirements of policing a Smart City. It is necessary that adequate financial support is incorporated in the budgetary outlay for this project under police modernisation. Bureau of Police Research and Development (BPR&D) may also start developing a Smart Police Maturity Model (SPMM) to evaluate the preparedness of police for Smart City. Smart City policing should also be included as an agenda item for the Annual Conference of Directors General of Police/Inspectors General of Police.



agencies, other government departments, emergency services, and other operations centers. The Technology Stack provides a platform that unifies the control and monitoring functions of physical security, building and traffic management, and computer aided dispatch systems to name a few.

This tiered, open and fault-tolerant architecture provides for easy repair or routine maintenance of the various system components, the enhancement and introduction of new data sources and analysis /visualization capabilities, and updates to/future exploitation of the overall services (e.g., the addition of new system APIs for external system use) — all while maintaining ongoing operations.

All data is processed by a centralised data center supported by HP servers and infrastructure. HP networking ensures bandwidth-intensive data, such as video, is delivered to the data center efficiently. The virtualized compute and storage systems also provide for very high levels of IT asset utilization, energy efficiency, and the ability to readily scale the system for future growth.

Expected Outcomes:

- Improve safety for pedestrians, cyclists and motorists;
- Tackle inefficiencies by creating a single unified layer across all data silos;
- Gather statistical information for analysis and planning;
- Be predictive instead of reactive;
- Enforce laws and reduce violations;

HP Technologies that include Autonomy & IDOL provide the ability to identify these correlations, which means they can predict possible outcomes before they happen.

Technology enables these correlations and enables different departments to leverage these insights to make needed changes in policy, processes, and people (such as possible training needs or necessary communications).

Prevent

The ability to have visibility into structured and unstructured data across multiple departments can help chart a course of behavior where multiple departments would team up for an integrated response plan. Having advanced information means it could use some intervention procedures to stop a situation from escalating and prevent incidents.

Perform Pro-active

The ability to identify an event before it escalates and prevent a serious situation from developing provides a powerful demonstration to all those involved of the potential of a Technology Solution.

This approach is the heart of the New Style of IT and Partnership where all constituents are engaged, they leverage resources, and become more efficient and effective from having a more holistic view.

At the core of HP Technology Stack is the Autonomy's Intelligent Data Operating Layer (IDOL) that offers a single processing layer thereby automatically unlocking information insights across all information channels - structured and/or unstructured.

The Information flow can be in myriad forms and can pan across documents, emails, video, chat, phone calls, and application data at the same time. As data is stored in a variety of repositories, IDOL streamlines information processing across networks, the web, the Cloud, smartphones, tablets, and sensors. In effect bringing a consolidated view of information wherever it is and deriving in-time insights that could make a sea of difference in security incidents' prevention and control

A Typical Surveillance Solution

The solution is basically structured around Step 1: (1) source data capture and storage, (2) analysis of data to derive video object and event information together with other Big Data intelligence, (3) fusing that information with other physical security information against a set of configurable business rules to provide a unified view. (4) providing these unified views to a wide range of

A Case Study

Dubai, one of seven Emirates that form the United Arab Emirates (UAE), maintains a police establishment with more than fifteen thousand employees with multiple high-level specialties and training. They are proud to be one of the best security institutions on a local, regional, and global scale.

In 2009, the Dubai Police deployed a new type of scanner mounted to the top of their patrol cars, capable of "reading" vehicle license plates and rapidly detecting those whose owners are wanted by the authorities. Associated crimes range from traffic violations to criminal activity.

At the heart of this new Automatic Number Plate Recognition (ANPR) system is HP IDOL, a secure search and analytics engine of the HP Haven platform that delivers actionable intelligence from both structured and unstructured data.

Challenges: Replace a cumbersome, manual task with extensible technology.

Previously, an officer with a printed list of wanted plates would comb through lots and garages full of parked cars, and occasionally find a match.

- To significantly improve effectiveness they needed to automate the process through the use of technology.
- The system needed to work day and night and read a wide range of number plate styles within the seven Emirates of the UAE, which incorporate both English and Arabic lettering and different color codes.
- They also needed the ability to find and track wanted vehicles in moving traffic, but ensure up-to-the-minute data updates so only those still wanted would be ID'd.

Top benefits

In the past 18 months, the system has helped Dubai Police capture 2,739 people locally and internationally.

SAFE CITIES WITH 
Lux rao
HEWLETT PACKARD

CITY SAFETY
THE FIRST STEP IN THE FUTURE CITY JOURNEY

A hundred years ago, only 10% of our population lived in cities. Today, over half of the world's population lives in urban areas, and this trend of massive urbanization continues at an unabated pace.

UN has projected that by 2050, almost 75% of the world population will live in cities. We are living in what has been termed as the "century of the city"—the century in which the world population goes past a tipping point of more people living in urban areas than in rural areas and where the dynamics of cities largely shape our world.

India urban population has been rapidly growing from 286 million in 2001 to 377 million in 2011, constituting 31.16% of the country's population. This is expected to reach 590 million by 2030, nearly 40% of the Country's population and contributing 70% to the country's GDP.

As cities evolve to become massive megapolises', the challenges of ensuring safety for the citizens is becoming increasingly complex. The aspect of safety must be egalitarian in that social status should not be determinants that define the "degree" of safety proffered to citizens.

A city needs to provide assurance to its citizens and the aspect of safety straddles multiple areas namely Disaster Mitigation and Management, Anti-terrorist measures, 24 hours Surveillance, Child & Disabled friendly measures, Fire Safety, Community based Security Support, Early warning systems, Resilience to Natural & Man Made Disasters Rapid Response Teams etc.

Technology can help here, from energy-efficient street lighting to systems that allow many different local agencies to view the same data and orchestrate the most optimal response to incidents.

Cities, with rapidly expanding populations and overstretched financial resources, need to become more innovative in devising solutions to urban security.

Safe cities are those that assure their citizenry a sense of security that adds up to an optimal quality of life. History is witness to the fact that Cities that provided safety and took care of its citizens have been at the forefront of economic and commercial growth and will continue to lead the charge in their aspiration to become Smart/er Cities.

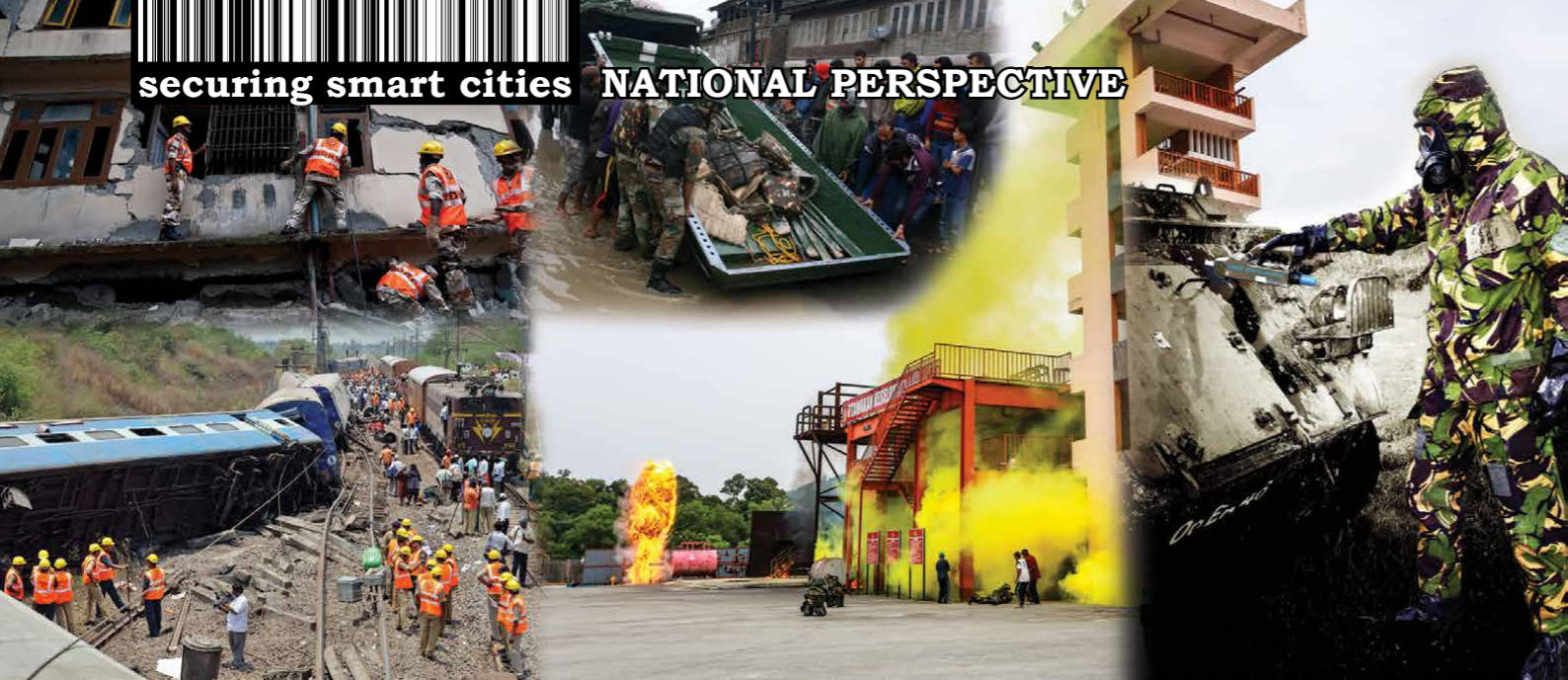
How can Technology help in ensuring a City Safety?

At the core of a technology oriented solution, lies the capability to garner multitudes of data, process & assimilate the same and derive meaningful insights & Predictive Analytics that enable Prevention, Response Optimization and Rapid Recovery.

The Predict, Prevent and Pro-active Performance Methodology ensures a holistic approach to defining and implementing Safety standards in the ever changing complexities of Modern Cities.

Predict

The ability to create the links between structured and unstructured data is the key to generating new insights.



DISASTERS AND CBRN THREATS IN METROPOLITAN AREAS

In order to protect mega cities and smart cities from natural and man-made calamities including CBRN threats, we have to create a proactive integrated system for early warning, foolproof command, control and communications systems, dedicated resource base with highly trained professional force which should be multi-disaster oriented with high mobility. In addition it should provide efficient Incident Response to emergency situations both in crisis and disaster management.

India faces grave challenges from multiple quarters. Managing such situations needs a dynamic approach and a deep understanding by us. Only then will we be able to respond in an appropriate manner

The Indian subcontinent is among the world's most disaster-prone areas. Almost 85 per cent of India's area is vulnerable to one or multiple hazards. Of the 28 States and 7 Union Territories, 22 are disaster-prone. They are vulnerable to wind storms spawned in the Bay of Bengal and the Arabian Sea, earthquakes caused by active crustal movement in the Himalayan mountains, floods brought by monsoons and droughts in the country's arid and semi-arid areas. Almost 57 per cent of the land is vulnerable to earthquake (High Seismic Zones III-V), 68 per cent to drought, 5,700 km of coastline is prone to cyclones and tsunamis and 12 per cent to floods. India has also become much more vulnerable to threat posed by not very amicable neighbours.

As the cities grow the merger of core cities, suburbs and satellite towns creates huge metropolitan areas and thus the very large cities in the world have become mega cities with more than 10 million inhabitants. The United Nations also classifies a city as mega city if it has at least 10 million inhabitants.

A mega city is usually defined as a metropolitan area with a total population in excess of ten million people.

A mega city can be a single metropolitan area or two or more metropolitan areas that converge.

"Mega cities are major global risk areas. Due to high concentration of people in clusters, high rise buildings, multi-agency jurisdiction, political conflicts and extreme dynamics, they are particularly prone to congestion, unplanned slums, natural and man-made disasters. Their vulnerability can be very high".

Mega cities lack proper and sufficient infrastructure and public services (such as sanitation, housing, education and health care etc) to support the growing population. This not only leads to the growth of slums, but also breeds discontent among urban dwellers, leading to high crime rates, as visibly seen in growing mega cities. Mega cities often have large number of homeless people. Traffic congestions interfere with the passage of emergency vehicles, wastage of fuel and delay in reaching place of work.

In smart cities rapid urbanisation is one of the most important changes that humanity has undergone as it has become richer. The trend is set to continue, posing huge challenges in some areas

but creating vast opportunities for those willing and able to seize them. Therefore a smart city brings together technology, government and society to enable the following characteristics:

"A smart economy, smart mobility, a smart environment, smart people, smart living, smart governance and smart, efficient crisis and Disaster Management apparatus with foolproof communication network, based on multi-system redundancy".

The concept is not static, there is no absolute definition of a smart city, no end point, but rather a process or series of steps, by which cities become more 'liveable' and resilient and, hence, able to respond quicker to new challenges. As cities grow, the need for this is especially relevant in the fast-growing economies, where the city authorities, security agencies, emergency services and the citizens are driven by the same objective – making the city more secure and a safe place to be for citizens and businesses from hazards and vulnerabilities.

Both mega cities and smart cities are exposed to hazards like earthquakes, cyclones, tsunamis, urban flooding, urban fire, building collapse, high rate of road accidents, industrial and chemical disasters, epidemics, terrorist attacks and CBRN threats and climate change.

So how do we secure the mega cities and smart cities from various threats? There are four important factors in handling threats.

- Can we **prevent** things from going wrong?
- Are we **prepared** for whatever may go wrong?
- Can we **mitigate** foreseeable threats?
- Is our **response mechanism** adequate?

National Vision

"The vision strives to build a safer and disaster resilient India by developing a holistic, proactive, multi-disaster oriented and technology driven strategy through a culture of prevention, mitigation, preparedness and response".

Therefore based on the National Vision, a mega city or a smart city must enhance performance on safety and security for citizens, their activities and investments and the sustainability of the environment, to thrive as a city.

A 'safe' city is a prerequisite to create an attractive economic and social environment for the citizens and to attract investments for the growth of mega cities and smart cities. With the integration of smart citizen centric services with the safety and security infrastructure, the city would be able to ensure sustainability and socio-economic growth.

Need For Policies And Plans

Disaster preparedness/emergency response plans, are written policies and procedures that prevent or minimise damage from disasters (either man-made or natural). These should be tailored to cover all relevant hazards and vulnerabilities, threats or risks to the concerned city. Contingency planning should be part of the plan. The plan should also outline the responsibilities of various stakeholders to ensure accountability during a crisis or a disaster.

Every district in the country must ensure that their District Disaster Management Plans (DDMPs)

are fully updated and all the stakeholders are competent to handle any situation and they have the training and resources for doing so.

Shortcomings In IRS

Over the years in many crisis and disaster situations, certain features emerged repeatedly and 'are and will' be relevant to any future situations, as listed below:

- Delay in assessment of situation and information dissemination.
- Breakdown of communications both electronic and surface.
- Delay in mobilisation of men, material, relief stores and machines to provide and restore basic lifeline services.
- Need is for enhancement of capacity building of the first responders (common man and community).

Incident Management

While we examined the shortcomings in the response mechanism and tried to find a remedy we also reviewed the incident management and number of weaknesses which were observed are listed below:

- Lack of accountability, including unclear chains of command and supervision.
- Lack of an orderly, systematic planning process.
- Poor communication due to both inefficient uses of available communication systems, conflicting codes and terminology.
- Lack of knowledge with common terminology during an incident.
- Lack of predefined methods to effectively integrate inter-agency requirements into the management structure and planning process.

Need For Incident Response System

Based on the above experience an Incident Response System has been introduced in the country which needs to be incorporated in the administrative structure of all the mega cities and smart cities. The Incident Response System (IRS) is an effective mechanism for reducing the scope for ad hoc measures in response. It incorporates all the tasks that may be performed during disaster management, irrespective of their level of complexity. It envisages a composite team with various components to attend to all the possible response requirements. The IRS identifies and designates officers to perform various duties and get them trained in their respective roles.



Maj Gen VK Datta AVSM, SM, VSM**, PPMG (Retd)**

The writer is one of the most decorated officers of the Indian Army, who has been part of the First Counter Terrorist Unit in the country and took part in raising The National Security Guard (NSG) and later was selected to command the 51 Special Action Group NSG. He was a Bde Cdr in CI OPS in the NE, GOC of an Inf Div on the Line of Control in J&K, COS of a Strike Corp, DDG MO Spl Ops in AHQ. Adviser on Counter Naxal Ops. Presently he is a Senior Consultant (CB & ME) with NDMA.



Disaster Management

One cannot wait for disasters to happen; disaster management is a 24x7 involvement. Therefore all the agencies responsible for safety and security of citizens must ensure that all systems are fully operational and ready for any response at a short notice.

Disaster Management means a continuous and integrated process of:

- Planning
- Organising
- Coordinating and Implementing Measures for expedient prevention, mitigation, capacity building, preparedness, response and relief and rehabilitation

We will discuss the organisation and structure required for disaster management a bit later after examining CBRN threats.

CBRN Threats

Although the chemical, biological, radiological and nuclear (CBRN) threats are non-conventional, they are still a real threat being faced by the country. On one hand, these CBRN agents could be used by state adversaries to create mass impact among civilian or army personnel. On the other hand, chances of these CBRN agents being used by non-state actors to create panic and disruption in densely populated metropolitan cities in form of a dirty bomb (RDD) causing large scale fear psychosis and disruption of life are also looming possibilities.

Chemical Contamination: Chemical contaminant may include toxic chemicals, poisons and chemical warfare (CW) agents. These agents exist in liquid, gas or solid form.

Biological Contamination: Biological agents like anthrax, cholera, plague, salmonella or smallpox can be commonly used for bioterrorism. Weaponised anthrax spores could possibly survive in potable water but the ease with which the agent can be used as an aerosol would dictate the route of infection. Plague and smallpox likewise are effectively transmitted as aerosols. Biotoxins can be added to water upstream of the distributing point.

Radiological And Nuclear Contamination: Large water reservoirs, rivers, water treatment plants, overhead tanks and water supply systems may get contaminated with radionuclides through accidental radioactive fallout following a nuclear detonation or an RDD explosion or intentional addition of water soluble radionuclides in the water body by unlawful elements. The aims of such contamination may be to cause widespread panic and public alarm. The most probable nuclides that can be used for terrorism are H-3, Sr-90, I-131 and Cs-137 because of their water solubility and easy availability.

Plan For Management Of CBRN Threats

CBRN threat necessitates a comprehensive action plan that entails specific set of actions for **Detection, Isolation and Decontamination**, with focus being on prevention, protection, preparedness, crisis management


and recovery. The core strategy for management of CBRN threat entails proper regulations, monitoring, training and availability of detection equipment, Hazmat vehicles, PPE with proper command and control for effective response by the fire and emergency services and the Police besides the National Disaster Response Force (NDRF).

In order to protect mega cities and smart cities from natural and man-made calamities including CBRN threats, we have to create a proactive integrated system for early warning, foolproof command control and communication systems, dedicated resource base with highly trained professional force which should be multi-disaster oriented with high mobility. In addition it should provide efficient Incident Response to emergency situations both in crisis and disaster management. To achieve this we need to have:

- Efficient early warning systems and detection system.
- Detailed crisis and disaster management plans.
- Incident response teams (IRTs) as per the Incident Response System (IRS)
- Efficient Emergency Operation Centres (EOCs) with:
 - ◆ Foolproof communication, with large bandwidth for video, voice and data.
 - ◆ Decision Support System (DSS).
 - ◆ Geographical Information System (GIS) platform.
 - ◆ Digital Map display with layers.
- Adequate staging areas.
- Helibase and helipads.
- Modern medical facilities with surge capacity.
- Efficient traffic management.
- Effective and trained law and order agencies.

Making mega cities and smart cities safer and more efficient the complete, integrated security solution needs to be incorporated using the latest technologies to provide a citywide command, control and emergency management capability. Area and unified command and control system which should have: Computerised Command, Control, Communications and Intelligence (C4I) centre with the EOC. In addition, Mobile Command and Control units with Hazmat vehicles, CCTV cameras for urban surveillance, traffic management and license plate recognition system needs to be incorporated with inbuilt data collection and data warehouse capability.

Conclusion

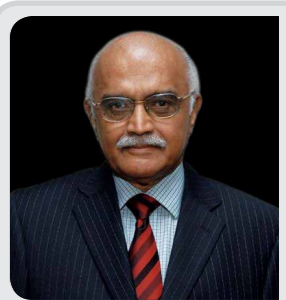
Effective command and control is important for effective management of any situation. Promoting a culture of prevention, preparedness and resilience at all levels through knowledge, innovation and education, along with encouraging mitigation measures based on technology, traditional wisdom and environmental sustainability and mainstreaming disaster management into the developmental and planning process will go a long way. Developing contemporary forecasting and early warning systems backed by responsive and fail-safe communication with information technology support and building capacities of the first responders and conduct of mock exercises on various kinds of disasters are the way ahead for mega and smart cities. 

POLICE LEADERSHIP MANAGEMENT OF MAN-MADE OR NATURAL DISASTERS

The concept of Incident Command System (ICS) was developed in 1968 during a meeting in Phoenix (Arizona) of California Fire Chiefs for fighting wild forest fires. The ICS became a national model later to fight crime scenes, fires or major incidents. It was used to tackle the New York City crisis during the first World Trade Center bombing (1993). After 9/11 it was adopted by the Department of Homeland Security as 'National Incident Management System' (NIMS) for all occasions where public assemblies are expected or for natural calamities, emergency and terrorist incidents.

In March 2013 the Government of India extended the 'Mega City Police Plan' to six major cities in India: Ahmedabad, Mumbai, Chennai, Hyderabad, Kolkata and Bengaluru. The capital city of New Delhi was perhaps not included in this list since it came directly under the Central government and the circular was addressed to the states. However the

scheme envisaged in this 'Plan' was not broad enough to cover every facet of urban security challenges. It was limited only to upgrading basic police infrastructure in weaponry, communications, computers, database and crime investigation. As far as I know, none of the cities except Bengaluru had held any public discussion on what would be the problems that the police would



V Balachandran

The writer is a former special secretary, Cabinet Secretariat who was also member of the two-man High Level Committee appointed by the Government of Maharashtra to enquire into the response during the 26/11 terror attacks.





face in dealing with growing security issues in mega cities so that the public, the ultimate beneficiaries of policing, would know at least the broad contours of how the police would meet such challenges.

Chief Minister Siddaramaiah of Karnataka state deserves accolades for initiating the first ever public discussion on what these problems would be by holding a three-day seminar on 'Best International Practices in Building Resilient Cities' (August 5-7, 2013) organised by the Synergia Foundation on behalf of the Karnataka Revenue Department. After the inaugural session which was addressed by the Chief Minister and senior ministers, this writer was requested to be the lead speaker for their second session where he did a case study of the experience of the Mumbai 26/11 terror attacks to analyse problems that would crop up in dealing with natural or man-made urban upheavals in any major Indian urban agglomeration. The writer may state here that immediately after completion of our 26/11 enquiry; he was invited to address senior Singapore police officials in April 2009 on the lessons of 26/11 terror attacks which would be relevant in formulating security architectures in any urban centres. He also delivered the keynote address on 'Securing Population Centers' in November 2009 at the Asia Pacific Homeland Security Summit at Honolulu organised by the Governor of Hawaii. In May 2010 the writer addressed a global group of homeland security officials assembled by a leading commercial group at Orlando on the same subject. Oxford University also invited him to deliver a talk on 'Dealing with the aftermath of attacks: Lessons from Mumbai on what to do and what not to do' in October 2010.

The Indian Situation

'World Urban Forum' meeting (March 22, 2010) at Rio de Janeiro had warned that 'mega cities' were emerging all over the world to form vast 'mega regions'. It said: "Just over half the world now lives in cities; by 2050, over 70 per cent of the world will be urban dwellers." The report said that India had 25 of the world's 'fastest' growing urban centres. Studies by others had found that urban centres in South Asia have become tinderboxes of violence not only from crime and terrorism but also due to non-traditional security threats like migration, urban decay and congestion due to poor civic planning, corruption, poor infrastructure, inadequate urban transport and on account of privatisation of critical public service sectors with inadequate oversight.

Absence Of Legal Authority

The biggest problem for the police in India is that they are not given legal powers to coordinate all aspects relating to planning and protecting mega cities, although in practice all governments and also members of the public expect them to discharge

all such heavy responsibilities in times of crises. Even when the National Disaster Management Agency (NDMA) arrives at the scene, the overall responsibility of tackling such massive problems is left to the police. In Mumbai the traffic police are not consulted either by the Mumbai Municipal Corporation (BMC) or the Mumbai Metropolitan Region Development Authority (MMRDA) who are in charge of infrastructure development like building overbridges or speedways. A couple of years ago the Eastern Freeway over the 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, 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. Instead of having one centralised Operations Room, different sets of supervisory officials met in different 'Control Rooms'.

Tunnel Vision In Mega Cities

Thus the Central Government's Mega City Policing Project is a typical example of a tunnel vision. Faced with frequent urban convulsions, the reaction of national and state governments in South Asia has been towards adopting only a law and order approach and formulating emergency procedures like forming heavily armed squads and conferring special powers to the law and order machinery. No integrated planning is being done to view this trend from a futuristic aspect involving other wings of government. In Mumbai during 26/11 the 'competent authorities' designated under the 'Disaster Management Act' played no worthwhile role as it was a terror attack. The entire responsibility of coordinating with the hospitals, ambulances and fire brigades came on the police who were already overwhelmed by the persisting terrorist attacks and heavy police casualties.

The farmer suicide on April 22, 2015 when the Chief Minister, Delhi was addressing an Aam Aadmi Party rally at Jantar Mantar, New Delhi which startled the nation is another example of how the police was needlessly blamed for not rushing to do the life-saving of that unfortunate individual who jumped to his death from a tree in full public view. People forget that not every policeman is trained in rescue or life-saving. It is only for this reason that the local fire brigade is always made to stand by when a major public gathering is organised. This incident was quoted as

Incident command system can vary depending upon the magnitude of the incident

In Mumbai the defence forces and NSG adopted a superior attitude towards the Mumbai police during 26/11

yet another reason that the Delhi Police should be placed under the Chief Minister. Although the writer is of the view that the Delhi Police should be under the control of the Chief Minister, it was not explained in this case why the Chief Minister, Delhi did not ask his fire brigade, which came under him, to be present?

It is true that the present arrangement of police and public order being placed under 29 states with no concurrent central role is not a satisfactory arrangement. This is based on the Seventh Schedule of the Indian Constitution which in turn was borrowed from the colonial 1935 Government of India Act law which was enacted under different circumstances. But as long as this arrangement exists in our administrative system, we need to strengthen the role of the police who is the pivot of urban crisis management.

Suggested Solutions

During the Bengaluru conference Shashidhar Reddy, former Vice Chairman NDMA outlined the need for an Incident Command System in India. In his speech the writer gave broad features of this system. It may be relevant to point out that the then United States Homeland Security Secretary Michael Chertoff had told a Johns Hopkins University audience on December 11, 2008 that the absence of an operational incident manager as was developed in the US after the 9/11 attacks was clearly a major problem during the Mumbai 26/11 attacks, where there was a glaring lack of coordination between various departments and agencies.

The concept of Incident Command System (ICS) was developed in 1968 during a meeting in Phoenix (Arizona) of California Fire Chiefs for fighting wild forest fires. The ICS became a national model later to fight crime scenes, fires or major incidents. It was used to tackle the New York City crisis during the first World Trade Center bombing (1993). After 9/11 it was adopted by the Department of Homeland Security as 'National Incident Management System' (NIMS) for all occasions where public assemblies are expected or for natural calamities, emergency and terrorist incidents. It is a system in which the concerned government agencies come together seamlessly under a predetermined and pre-trained leadership thus acting in unison and eliminating duplication of resources and confusion. This joint management system, duly modified has been adopted by several countries like United Kingdom, Canada, Brazil, Australia, New Zealand and even followed by the United Nations.

Incident command system can vary depending upon the magnitude of the incident: It can be Single, Unified or Area Command. These commands will be competent to summon extra forces and resources from outside and not wait for long bureaucratic procedures in summoning Army, Navy and NSG help as had happened during 26/11. In Mumbai

although the police had desperately sought help from the Union Home Ministry, concrete action to send NSG was taken only after the Maharashtra Chief minister who was away in Kerala had spoken to the Union Home Minister. In this system there will be a Safety Officer who will decide the safety of operations, a Public Information Officer who will release news to the media and an empowered Liaison officer who will liaise with other agencies. A Joint Information Centre (JIC) would function as the public face of the incident which will release all developments in an organised manner, obviating the totally haphazard manner the media had functioned during Mumbai 26/11. Similarly a Joint Operations Centre (JOC) would function as the **only** centralised control room to guide all operations of concerned agencies like police, civic authorities, ambulances, hospitals, relief agencies and private bodies instead of different control rooms that had existed in Mumbai during 26/11.

Concrete Action In Concrete Jungle

The senior IAS officer of the Karnataka government who had organised the Bengaluru seminar had asked the writer what should be done initially to put in practice the concept of 'Resilient City'. The writer suggested to him that the first step should be to integrate all control rooms in Bengaluru for simultaneous information exchange. Secondly a law should be passed to put in place a system of preventive structural security in every building under construction in Bengaluru like what exists in Singapore for long. No community building plan should be approved without security clearance from the police.

Since the police in India is expected to shoulder the entire responsibility of tackling urban convulsions, a law should be passed by each state government to declare that in case of such mega disasters or terrorist strikes, the Commissioner of Police in each mega city would temporarily take charge of the entire responsibility of supervising the Incident or Unified Command System by placing all civic, emergency, health, relief and temporary rehabilitation services as well as deploying and commanding all extra forces including the defence contingents. In Mumbai the defence forces and NSG adopted a superior attitude towards the Mumbai police during 26/11. This should not happen. This will be akin to the State of Emergency declared by State governors in USA in case of riots or natural calamities. Joint training of such services should be undertaken as is done in foreign countries by creating special training centres like the 'Home Team Academy', Singapore which jointly trains police, defence, immigration, civil defence and airport security officials to evolve a joint approach towards terrorism and natural calamities.

Thus no compartmentalised police modernisation plans will succeed without taking into account the realistic police responsibility in mega cities during such crisis situations.



INTEGRATED EMERGENCY RESPONSE

Failure to have a Unified Command Structure is the most common obstacle to effective emergency management. Not knowing who is incharge or even worse competing commands will create chaos and can cost lives because one team will not know what the other team is doing. It is therefore essential that after the primary stakeholders are identified, the planning team must establish a Unified Command Structure and designate an incident commander.

Emergency preparedness is a state of readiness; it can be defined as pre-impact activities to respond to extreme and critical events that could affect the safety of the community and the systems.

To deliver active response an organisation's system response is put to test during critical crisis be it of natural cause or man-made, this active response when effectively carried out minimises adverse impact of the critical crisis and protects and safeguards people and physical structures of the community.

Integrated emergency response is part of the national integrated management systems. Organisations, resources and processes are the components of interconnected systems. This means citizens, clearly defined national safety policies, practices, equipment and culture are part of the system.

Planning and Preparedness are the actions undertaken before an emergency occurs and include -

- Preparation of emergency plans
- Development of preparedness and response arrangements and the building of capacity for assigned functions, in light of the risks faced
- Education, training and development of staff who will be required to respond to an emergency
- Exercising and testing of systems, plans and procedures
- The procurement of resources necessary to strengthen preparedness

The maintenance of any necessary facilities and

The audit/assessment of preparedness

Integrated Systems

The need for integrated systems is common for all systems of any country. The lack of integrated systems causes 1) confusion due to isolation 2) increased cost to run separate system with separate working order 3) increased audit costs and 4) poor incident management when crisis is encountered.

So several reasons why emergency management system must be integrated:

- Reduce duplication
- Reduce risks and increase efficiency for response (this depends on good planning, anticipation of various threat and crisis scenarios, coordinated response through speed and with accuracy of gathering information about the situation, analysing the available options and making decisions and taking action to implement those decisions)
- Eliminate conflicting responsibilities and relationships
- Harmonise and optimise practices
- Create consistency
- Improve communication

- Facilitate joint training and development (this assists in developing and maintaining pre-existing professional relationships, conducting multi-jurisdictional exercises, table-top and hands-on)
- Strong relationships and successful unified command (commanders, agency heads and political leaders)
- All-hazards including medical system readiness is a state of readiness ensuring the capabilities and capacity to quickly triage and transport the injured from the active crisis scene, aid in damage control, controlling and calming the public where every response system works together as crisis managers and leaders.

Nepal

An example: During Nepal's recent crisis the most effective part that came into effect was their hospital emergency preparedness plan during the earthquake response. From a well working roster system to triage management putting into practice WHO's strategies (2007) during mass casualty. The emergency responders were quick to prioritise the injuries and save lives. The quick response of the health workers was a clear example that preparedness does work well during crisis.

- A functioning joint information centre (example: JIC directly assists with media communication supporting public information, avoids conflicting information which can give rise to panic or escalation of the crisis)
- Emergency management systems must also take into consideration responder safety because this directly means managing risks.

Pretesting

All forms of disasters requiring emergency procedures disrupt the flow of normal safety procedures,



Dr Rupali Jeswal

The writer is an intelligence and terrorism analyst. She is also a trainer for Law Enforcement, Specialised Units and Corrections. She is CEO of Xiphos-ISS, Security Integrator of Impact-Response, Chairperson of Anti-Rad Committee of ICPA (USA), Visiting Researcher with CENTRIC, Sheffield Hallam University, UK and Fellow of RCPS (Romania).



Joe Marchese

The co-writer was the Deputy Director of Criminal Justice for the NYS Division of Criminal Justice Services. He is an internationally recognised consultant/trainer and implementation strategist specialising in areas of emergency planning, management of security threat groups, hostage negotiations, organisational development, leadership and training administration and management. He has trained and served as a consultant to criminal justice agencies in over 45 US States and several foreign nations.



the chaotic environment of a minor or major disaster obstructs flow of accurate information and data, confusion can lead to wrong assessment of the hazard and the specific response needed, anticipating all obstacles such as implementing decisions in a chaotic environment should be tested, analysed and evaluated to acknowledge holes and gaps. Hence local responder agencies along with regional and national management structures need joint trainings and exercises.

Regular table-top exercises when conducted comprising of local district, state and national safety partners enhance cooperation and coordination during the time of emergencies. These exercises also include response to a number of scenarios ranging from natural disaster to man-made disasters
These exercises included the following goals and objectives
Capability demonstrated for: Management and Direction Control Containment and Coordination of response Multi-agency coordination
Including evaluation of local and regional tactical capabilities of Law Enforcement and special units
Including assessment of local and regional resources and evaluation of agencies to respond to critical CBRNE event and the coordination to integrate local police, fire, hospitals and hazmat
Assessment and Evaluation of command centres during crisis
Assess and evaluate the region's ability to properly respond and render services, deployment of tactical units, to be able to deter, detect and disrupt criminal and/or terrorist activities
Test the ability of EMS personnel to provide mass casualty triage and expedient field treatment of multiple casualties while law enforcement tactical teams provide protection, resulting in intra-agency and multi-discipline integration and coordination

Building integrated response mechanism into the existing structures will ensure accurate analysis of the situation and response. All responding agencies must be able to anticipate various problems and install systems so that they can efficiently size up the situation to mitigate, neutralise and cope with circumstances of a dynamic, hazardous and complex situation.

Boston Bombings

Example of Boston Bombings: Good planning and preparedness was evident in this case on how the response was implemented through Threat and Hazard Identification and Risk Assessment (THIRA). This assessment gives the picture of regional capabilities and gaps to prioritise investments in key deployable

capabilities. 'These assessments assist states and urban areas planning and preparing for various scenarios, prioritising the development of capabilities to address known and evolving threats.'

Federal Emergency Management Agency identified 56 states and urban areas including Boston for complex attacks as one of their top threats/hazards in their 2012 THIRAs.

FEMA's approach also empowered communities with the right tools and information needed to be prepared. It was a whole community approach including homeland security and emergency management. A total holistic preparedness system.

"As a result of the NPS, the whole community plans better, organises better, equips better, trains better and exercises better, resulting in improved national preparedness and resilience."

http://www.fema.gov/media-library-data/20130726-1923-25045-1176/lessons_learned_from_the_boston_marathon_bombings_preparing_for_and_responding_to_the_attack.pdf

Preparing For The Worst

The initial planning team must first look at local vulnerabilities in three categories: 1) Natural Disasters 2) Man-made Disasters and 3) Incidents of Violence. Once these potential disasters are identified the planning process should take a triage approach and establish plans for the most likely incidents first and work.

Disasters may be community-wide
A localised incident is defined as an occurrence that affects only a small part of a community
Major incident emergencies are potential threats that disrupt sizeable portions of the community
Major disaster emergency or critical crisis or imminent threat involves the entire city and community and can have multiple ground zeros

With all incidents of emergencies 'offshoots' must be taken into consideration such as fire leading to explosion, power outage, shortage of emergency responders or no means of communication.

London Bombings

For example during London bombings as there was no mobile radio communication system in the subway, emergency workers had to run back and forth between trains and platforms to communicate.

The bomb sites were four in total, one on a bus and three underground locations (train stations), near one of the bomb sites a 2-way antenna was damaged which is a system used by the train drivers to communicate. The city's emergency response relied on mobile phones and with mass panic and citizens trying to get in touch with their family and friends – all this led to communication problem with jammed networks. Situations like this are the offshoots that need to be pictured in the planning process.

Planning and training, with continuous drills are imperative to increase the response system effectiveness and raising the confidence of the first responders including the communities.

Major emergency management arrangements build on current strengths and make full use of the core competencies and organisation strengths of the principal response agencies as the basis for the response
Major emergency management arrangements should fit in with existing organisation and government structures, subject to appropriate coordination mechanisms being added
The response to emergencies builds from the basic level with capability to respond, that is from the local organisation units

Assessing Existing Resources

Once such vulnerabilities are identified then the planning team needs to determine what it will require to respond to such emergencies, identify the appropriate response services and the equipment needed.

Identification Of Stakeholders

We can all agree that traditional responders, Fire Police etc are the primary participants or stakeholders in the emergency response. But it is also very important to identify other stakeholders since the best laid plans can be rendered useless or interfered with if an unidentified stakeholder emerges prior to plan implementation or during the incident.

The initial process however must begin with resilient communities and prepared individuals and depend on the leadership and engagement of local government, NGOs and the private sector.

Unified Command

Failure to have a Unified Command Structure is the most common obstacle to effective emergency management. Not knowing who is in charge or even worse competing commands will create chaos and can cost lives because one team will not know what the other team is doing. It is therefore essential that after the primary stakeholders are identified, the planning team must establish a Unified Command Structure and designate an incident commander.

Unified Command Structure

<ul style="list-style-type: none"> Develop a single standard command structure for all types of emergencies. An integrated command structure avoids confusion
<ul style="list-style-type: none"> Functions should be assigned according to the divisions of labour that would apply during an emergency
<ul style="list-style-type: none"> As different types of emergency overlap it is best to establish standard training programmes that incorporate a spectrum of response skills

<ul style="list-style-type: none"> Emergency Operations Plan (EOP) should be straightforward and concise containing fundamental response procedures
<ul style="list-style-type: none"> One set of emergency personnel roster and one set of emergency response equipment should be chalked out appropriate for all required plans
<ul style="list-style-type: none"> As responders come to the scene, they should know how to identify their place in the command structure

The foundation of an integrated management system and national response plan is that the incidents should be managed at local level first; they form the first-line of emergency management and incident response.

A need is also prominent to build resilient communities.

Resilient communities begin with prepared individuals and depend on the leadership and engagement of local government, NGOs and the private sector

- The first to detect a threat:
- Community
 - Local Police
 - Local Fire Department
 - Local Emergency Medical Services
- And they are often the last to leave an incident site and have to cope with the effects of the incident longer than others
- The local appointed officials and their emergency managers are responsible for ensuring public safety and welfare of the residents giving timely and effective emergency response.

Integrated Training, Drills, Simulations

Through the use of training events we can examine all levels of the plan. There are three basic training components for plan evaluation: Training, Drills and Simulations. 1) Training refers to classroom training and not only includes learning the competencies necessary for team members, but also an overview of the plan and their team/individual role in it. 2) Drills take teams out of the classroom to practice components of the plan that must be conducted as a part of the operation. 3) Simulations are the highest level of emergency training and require a great deal of coordination and precautions. Simulations should include all components of the response team interacting in a manner that mimics a real emergency. Emergency planners should rely on all three methods of training to identify plan problems and ultimately strengthen the plan.

Integrated emergency response in the end must be evaluated through after-action reviews (AARs) to help leaders and officers with a feedback on mission and task performance, this will in turn assist planning preparedness for future incidents if they should occur.

Note: AARs can be conducted even during the operation so as to assess the current situation regarding what needs to be done and what new resources to call for to reach the operational objective.



LAW ENFORCEMENT PERSONNEL KEEPING PACE WITH DEVELOPMENTS AND TECHNOLOGIES

Technology has changed the manner we live our lives, but it has not until now transformed the system the police do their jobs. The lessons from the private sector – and the world of sport for that matter – are clear: It does not matter how excellent you are, you can all the time get better.

Europe is on the cusp of an unmatched scientific revolution. The writer calls it the Internet of the whole thing: The diffusion of the World Wide Web into the each-day aspects of our lives. Almost half a billion people in Europe use the Internet. It allows connections between individuals across a wide geographic area, bringing many socio-economic benefits. Wearable technology will notify us how healthy we are sleeping and whether we have to work out. Sensors in the road will assist us pass up traffic jams and find parking. Telemedicine applications will permit physicians to treat patients who are hundreds of miles away.

Crime On The Internet

There are many ways information and communication technologies are driving new and emerging crimes. Online criminal 'social networking' can provide forms

of criminal 'outreach' and links between criminal groups. A false impression of social acceptability of criminal acts such as child sexual exploitation can be created by online communities. Global incitement to violence and terrorism through social media has widened the reach and influence of previously localised radical and terrorist groups. Illicit drugs and other products can be bought online, paid for with anonymous virtual currencies.

New criminal trends in Europe have emerged with people committing crimes in cyberspace that they would not otherwise commit – the anonymity of the Internet and the possibility of adopting variable identities can be incentives for criminal behaviour. Criminals can gain access to large number of targets through online services such as banking, shopping and social networking.

Criminal groups operate in new ways, hiring specialists to perform tasks not covered by their

existing knowledge and skills. This trend of a more transient and less structured organisation may be how serious crime will be perpetrated in the future. The disproportionate impact of the economic crises in Europe faced by many young people in terms of poverty may increase youth vulnerability. In this context social media tools at their high-speed do not give space to doubt, critical thinking or self-criticism and attribute the entire responsibility for an individual's situation in particular real or perceived grievances to the 'others and the society at large'.

This substantial changeover will convert how general public interrelate with their governments, transfigure whole industries and revolutionise the way we connect with one another. In Europe, the Internet of Everything is up-and-coming as the only most capable way to revitalise a declining economy and undertake the continent's stubborn joblessness problem, with companies, cities and even countries positioning themselves as leaders in improvement, development and the creation of jobs.

Complicated Policing

In the present day, public safety is a bit more complicated and methods of communication much quicker. Law enforcement tools have evolved from wanted posters to police radio, patrol cars and social networks, such as Twitter, Facebook and YouTube. Even though the main beliefs of policing stay invariable, the world in which the police function has undergone remarkable shifts. Keeping the peace, protecting existence and property and enforcing the law are everyday jobs that are now challenged by increasing citizen expectations, the shifting nature and increasing complexity of crime and a need to tackle frequently harsh budgetary constraints.

To be able to tackle these future challenges, the police have to be capable of twisting information into actionable intelligence. In the terms of the maxim, 'prevention is better than cure', by adopting evidence-based policing strategies, the police can more successfully identify crime and adjust their services to meet the future requirements of policing. More police leaders believe that police services are ready to embrace operational, cultural, technological and organisational transformation. There is confirmation of investment that has translated into rising police officer numbers and a significant drop in crime rates.

Social Networking As Police Tool

Social networking speedily has turned out to be a precious intelligence gathering instrument for law enforcement agencies, as well as a resource of evidence for defence and prosecution personnel who investigate Facebook pages, Twitter feeds or YouTube videos in the hunt to question witnesses, set-up law enforcement bias, track down evidence or create associations between gang members.

Often, perpetrators brag about their crimes on social networks and child pornographers and sexual predators have been located and apprehended as a result of their online activities. Community policing today has also permeated social networking to trace missing children, alert neighbours of doubtful activity and even bring up to date the public concerning crimes committed in their area.

But social networking is an instrument that cuts mutually both ways. Flash mobs prearranged online in Philadelphia for example swarmed stores to shoplift and assault pedestrians; paedophile use social networking platforms to distribute photos and videos and terrorists conscript members and organise attacks via these tools. Twentyfirst century crime is progressively leaving more tracks on digital devices. As burdens on digital investigators and crime labs rise, so do the challenges of speedily acquiring and distributing of possible proofs from a persistently varying array of devices with other experts, field agents and prosecutor's offices.

Cybercrime

Cybercrime represents another area where there is a strong competition between the law enforcement and cyber criminals and without the support of new technologies law we could lose that battle. As practice has proved it, many cyber criminals use the Internet for political purposes or to conduct illegal activities. Unlike the other categories, they use information and communication systems to initiate or coordinate terrorist actions and to propagate ideas that incite racial hatred or hatred between certain organisations or to instigate masses to antisocial behaviour, such as the transmission of images of executions of 'opponents', paramilitary training, combat exposure techniques or ways of producing complete explosive devices etc.

And this is a battleground where the innovators – equally from police forces and the private sector – can go out and make available applications and software that give significance to the taxpayer, stop police officers from wasting their time and guarantee the public is protected and cybercrime is tackled.

New Appliances

Thrilling work has been in progress – applications are being developed to permit forms to be filled in by



Dorin Muresan

The writer is currently Head of Security and Regime Service at Dej Prison Hospital in Romania. In 2011 and 2012 he was Deputy Director General of the Romanian Prison Service. He coordinated projects like the evolution of e-learning project for prison staff; the development of telemedicine project in Romanian Prison Service and provision of expertise to post-conflict prison services (Libya, Iraq).

Social networking speedily has turned out to be a precious intelligence gathering instrument



Tough devices for those, who enforce the law.



design on the street, rather than in time-honoured (and time-consuming) pen and paper fashion at the police station. New technology requests need to be customised and governed by 'rules of the game'. We will do the boring bit by setting the scientific standards and ensuring data is collected in well matched formats and accessible to those who need it. And we'll make sure people be familiar with how to secure a superior range of devices for officers.

We need to see more examples like those in UK which allows officers on the highway patrol to access real time information concerning suspects or GPS-based information about the area they are working in. We need to see more forces operating body-worn cameras. Evidence shows up to 90 per cent of suspects plead guilty when they see the recorded evidence.

And we need to see more use of mobile fingerprint scanning devices like the ones West Midlands Police have used to identify more than 2,500 people without returning to the station. Emerging concepts like 'Mobile Predictive Policing' provide flexibility for the field officers. Predictions are delivered directly to officers on any Internet connected mobile device-like smartphones and tablets – or vehicle data terminals. Reports and predictions can be exported to PDF, KML or CSV formats for use in other programmes or printed on paper during daily patrol briefings. And every minute saved in unnecessary bureaucracy is another minute spent fighting crime.

Another area of matching advanced technologies with daily activities of law enforcement structures is represented by the statistical programmes that analyse socio-geographic locations of criminal acts. These types of solutions are useful in applications related to space-time analysis of crime.

In principle, it is based on the introduction of the crime characteristics in a predefined database. Based on spatial coordinates, through GIS application this will outline the places where the criminal acts occurred; listing them on the geographical map. Their operation is relatively simple:

- Includes more than 100 analysis predefined routines
- Every incident is entered into the database together with a number of features selected from a predefined database
- Statistical analysis and incident characteristics are by algorithms
- Displays the results using a graphical interface algorithms to illustrate both in space and time incidents (geographic coordinates, dates and times, areas of a city etc) and by other parameters (offender nationality, residence, occupation, context etc)
- One of the sections of the application generates reports for certain predictive data characteristics (Examples of reports generated: Density of incidents in a certain area, zonal analysis of offenses, the relationship between the offender and incident-based spatial modelling regression models)

Technology has changed the manner we live our lives, but it has not until now transformed the system the police do their jobs. The lessons from the private sector – and the world of sport for that matter – are clear: It does not matter how excellent you are, you can all the time get better.

This IT transformation of law enforcement structures is about far more than reduction of a few Euros by 'getting a bit better on the computer'. It is about instituting a change in mindset, regarding persuading every police officer, no matter how knowledgeable they are, of the transformational power of technology. **DSA**

Every minute saved in unnecessary bureaucracy is another minute spent fighting crime

Panasonic Toughbooks & Toughpads are mission critical Mobile Data Terminals (MDT) best suitable for those who enforce the law.

People who enforce the law know how valuable it is to access the right information instantly, when needed the most. Imagine a site of suspicious activity that requires an immediate response from law enforcement. You can depend upon the headquarter to gain vital information on perpetrators or your location. All you need is a device that will allow you to run license plates, take / scan photographs, read up on an individual's gang activity and/or criminal record, scan crime graphs for the locale and more.

Loaded with the latest innovative technologies, Panasonic ToughBooks and ToughPads are extreme machines that are built to never fail you – come what may.



- Performance
- Ruggedness
- Mobility
- 3G Solution
- IP65
- Customisable

TOUHPAD

TOUHPBOOK



CBRN SECURITY FOR HIGH VISIBILITY EVENTS

India has made great technological advancement in the last two decades. Indian Industry is now capable of producing world-class CBRN equipment. Many such players are offering state-of-the-art CBRN PPE, detectors, decontamination equipment, collective protection equipment (fixed and inflatable quick deploy CBRN shelters) and medical equipment. All these will enhance the response of our CBRN response forces.

We must anticipate the next threat, not react to the last.

The threat of conventional and full-scale war has faded. Nuclear sabre-rattling may be used as mere tools for moral ascendancy and leveraging diplomatic advantage. Globalisation and revolution in Information Technology has caused a spurt in transnational terrorism or 'Revolution in Terrorist Affairs (RTA)'. Chemical, Biological, Radiological and Nuclear (CBRN) materials have proliferated widely and the expertise required to utilise these is actually within the grasp of terrorists.

Availability Of WMD Materials

Research shows that terrorists are constantly seeking new terror means. The Tokyo nerve gas attack by the Japanese cult group, Aum Shinrikyo, on 20 March 1995, had set

precedence in the use of WMDs. The Anthrax cases in the US and radiation scares across the EU are other examples. A lot of recent reports suggest that caches of Chemical Warfare Agents (CWAs) are still lying in rubble in Syria and Iraq. Reports also indicate continued use of Chlorine in Syria. Some reports also suggest that the ISIS is in possession of CWAs and is attempting to weaponise Ebola virus. It is but a matter of time, when India will be faced with a CBRN terrorist incident. Indian Police and paramilitary forces are not adequately trained and equipped for responding to CBRN incidents.

High visibility events like large sporting events (Olympic Games, Asian Games, IPL matches etc), political rallies and religious festivals are all potential yet highly complex targets for terrorist CBRN strikes. Police, paramilitary forces, Special Teams and

Intelligence agencies need to understand this threat and prepare for preventing and responding to these.

Emerging Threat

With proliferation of Industry, extensive open source Internet knowledge base and easy availability of dual-use technology, we are witnessing the emergence of 'techno'-terrorist, who is more likely to resort to CBRN terrorism. The chance of a significant CBRN incident occurring in India is heightened by several factors:

- Inexpensive availability of Chemical/Biological (C/B) agents, their precursors and easily obtainable production processes.
- Increased WMD stockpiles in the region, with the potential for theft or acquisition of the weapons by terrorist groups.
- Capability of inflicting mass casualties based on limited administrative and public ability to quickly identify and/or contain the effects of such substances.
- Potential for large-scale impact due to increased media coverage of the use of CBRN materials and high-level psychological, paranoid and panic reactions.

The Legislative Framework

It is, therefore, not a figment of imagination or misplaced paranoia to assume that CBRN threats loom large over India. CBRN security in India is still in its infancy. India is party to the Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on Their Destruction (BWC) and the Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on Their Destruction (CWC). Despite signing these international frameworks on CBRN, India's domestic laws and rules leave some gaps. UN Security Council Resolution 1540, adopted in 2004, indicates the heightened threat perception about CBRN terrorism.

While movement of CBRN materials across India's borders is closely monitored, the same is not true for their movement within India. India has enacted several laws which deal with CBRN matters viz The WMDs and Their Delivery Systems (Prohibition of Unlawful Activities) Act, 2005, The Factories Act, 1948 (amended 1987), Unlawful Activities (Prevention) Amendment Act, 2004, Manufacture, Storage and Import of Hazardous Chemicals Rules of 1989 (amended in 2000), Provisions under the Indian Penal Code and Prevention of Terrorism Act, 2002. There is however, no comprehensive legislation in India, which covers CBRN as a whole and addresses all related aspects. This is compounded by the gross administrative and public apathy and complacency towards CBRN threats.

Large Event CBRN Security

Large public events, being high population density venues with significant politico-social importance, are highly vulnerable to CBRN terrorism. To be successful, organisers of major events, security systems must be

treated as a major part of a larger, multifaceted planning process. The first stage is a clear understanding of how to match capability to a well thought through risk analysis that extends well beyond the traditional thinking of threats.

Peculiarities

Large public events like international and national level sporting events, sociocultural extravaganzas, public/political rallies and religious events, where people gather in huge numbers are high-priority targets for CBRN threats. Such events are characterised by the following peculiarities:

- Multiple locations – dispersal of assets
- Each venue may have multiple entry and exits
- Some venues may be open air or in buildings
- Crowd management – prior, during and after the event
- Traffic management – prior, during and after the event
- Euphoria vs Caution – Iconic branding
- Multi-agency security – issues of coordination and synergy

Threat Assessment

Awareness of CBRN threats and diligent planning is fundamental to effective counter-terrorism protection of the event. Hence, CBRN threats should be properly emphasised in the terrorist threat assessment, risk analysis and counter-terrorism strategy for the event.

Guidelines and formulas for conducting threat and risk assessments are available from NDMA and take into account the intention and capability of an adversary, as well as vulnerabilities (eg building characteristics, security practices). The Ministry of Home Affairs has also developed threat assessment tools, primarily regarding protection of targets. However, our Police and paramilitary forces are grossly ill-equipped and inadequately trained to respond to CBRN incidents. Basic awareness of CBRN threats and training on CBRN response need serious and immediate attention.

Information Collection

The information collection phase tasks are to:

- Assign responsibility to experienced, qualified assessors
- Review available information (floor plans, utility



Col (Dr) Ram Athavale (Retd)

The writer is a Veteran Army officer. Alumnus of the Defence Services Staff College and Army War College, he has extensive operational and senior staff experience. He has been a Key Adviser to the Government of India on CBRN Security (critical Infrastructure protection and CBRN Incident Management). A prolific writer and a CBRN subject panellist in international seminars and conferences, he holds a Fellowship and has been awarded PhD for his Doctoral Research on "CBRN Terrorism: A Crisis & Consequence Management Model for India" from University of Pune, India. He is also a Visiting Faculty at Symbiosis International University, India and Senior Adviser CBRN & Homeland Security to some Industries.



layouts, maps, aerial photos, evacuation plans, fire inspection reports etc)

- Interview event planners in the governing jurisdiction and the event promoters
- Obtain threat intelligence information from internal and external sources
- Conduct extensive site observations and surveys
- Develop detailed participant profiles
- Assess the security plans of key event hotels
- Examine all forms of transportation that participants will use to travel to the event – airports, trains, buses, subways and metro systems

Crisis And Consequence Management

While many nations of the world began working on Consequence Management mechanisms of CBRN events during and after the Cold War, real impetus has been acquired post the 9/11 attacks. The USA has put into place a credible Homeland Security apparatus. International initiatives to combat CBRN terrorism under the UN, NATO, EU, SAARC and other global initiatives for combating CBRN terror have been formalised and are in place.

A Crisis and Consequence Management plan should be based on the following focus areas, with each area integrating training and research:

- **Crisis Prevention**
 - Preparedness
 - Prevention
- **Crisis Management**
 - Surveillance and Detection
 - Immediate response and escalation prevention
- **Consequence Management**
 - Response
 - Mitigation

Our Police and paramilitary forces are grossly ill-equipped and inadequately trained to respond to CBRN incidents

Incident Management

The government has put in place a very comprehensive and detailed structure, primarily to deal with disaster incidents (including terrorism). The Disaster Management Act 2005 is a comprehensive legislation. A lot of thought has been given by the Indian Government to CBRN disaster management. The WMD Act was passed in June 2005. In addition, the government has instituted the following measures to deal with CBRN incidents:

- Devised SOPs to deal with terrorist attacks involving use of CBRN weapons
- Earmarked twelve paramilitary battalions like the NDRF, trained and equipped for CBRN disaster /terrorist strikes
- Atomic Emergency Response Centres (AERCs) /Mobile Radiation Detection Systems (MRDS) in 1,000 Police Stations covering 35 Cities
- Established the National Intelligence Grid (NATGRID) and set-up the Crime and Criminal Tracking Network & Systems (CCTNS)
- Radiation monitors being installed at seaports (12), airports and border posts for container /cargo scanning

- Pre-positioning of QRTs & QRMTs in all districts having nuclear facilities

CBRN Security Paradigm

Response and protective actions for law enforcement in the event of a hazmat (hazardous material) incident. Ministry of Home Affairs has worked out protocols for CBRN threats at major special events. To beat the CBRN Security conundrum, it would be prudent to follow a proven model. Over the years guidance, standards and policies have changed, but the universally valid paradigm is as enumerated below:

Threat Analysis and Vulnerability Assessment (TAVA).

This would begin with an on-site reconnaissance to generate a realistic threat analysis. This will lead to maximising value of networked threat detection, existing infrastructure operations, security systems and personnel resources.

Developing a CBRN Security Concept and Plan.

A comprehensive CBRN Security Plan would include crisis prevention, threat detection, immediate response and mitigation. Based on this evaluation, incident strategies, objectives and response tactics are developed in the incident action plan. This will include availability of Subject Matter Experts (SMEs) for rapid risk assessment of received threats, procedures for venue protection from hazmat and deployment of response and assessment teams for reported hazmat incidents in and around the venues.

Incident Command Centre (ICC), Site Preparedness and On-site Teams. The ICC will synergise efforts and optimally control personnel and resources, preparation of the venue and help provide initial responders a quick guide for traffic management and structured response. Optimally equipped and trained On-site Teams for prevention and immediate response to an incident are a dire need.

Equipping for CBRN Security (type and quantity) and manpower for CBRN Security.

A comprehensive equipping policy depending on anticipated contingencies needs to be formulated and implemented. This includes Personal Protective Equipment (PPE), equipment for detection, identification, containment, decontamination and medical management of CBRN casualties are catered for to implement mitigation objectives. As of today only a handful of specialist teams are adequately equipped.

Effective Monitoring, Exit and Evacuation Plan.

A key component in post event management is the controlled and structured exit and evacuation plan from the affected area. Secure exits, pre-identified holding spaces, transportation logistics and isolation /segregation of victims call for meticulous planning and effective crowd control measures. A plethora of

state-of-the-art equipment and resources like CBRN detectors; decontamination equipment; screening and checking procedures; canine corps are available and must be used. Plain clothes CBRN specialists should mix with the crowds whilst undertaking their work without arising suspicion or panic behaviours.

Information Management and Resource Coordination.

Timely and accurate information flow to all stakeholders is of paramount importance for optimal response. Appropriate data management systems working to develop a Common Operating Picture are required.

Decontamination and Clean Up Operations.

Neutralisation of toxic threat is critical to resilience. An important area is Emergency and Technical Decontamination for responders and Mass Decontamination for victims, depending on the specifics of incident. Casualty decontamination is an often neglected area.

Training Philosophy and Responder Curriculum.

CBRN Training philosophy and comprehensive curricula based on user profile and requirements should be developed. Adequate emphasis on key skill development should be ensured while focusing on real time response and use of appropriate equipment. This can be further honed by conduct of mock exercises and tabletop exercises to provide realistic training to stakeholders.

CBRN Security Audit.

CBRN Security plans need to be dynamic in nature and flexible enough to meet new threats scenarios. It is necessary to conduct comprehensive and periodic CBRN Security Audits to keep CBRN Security updated and CBRN Incident Management plans in order.

Awareness Generation.

A key component in prevention and post-incident mitigation is public awareness. It is imperative to enhance awareness about CBRN Threats, response and mitigation measures to a wide stratum of stakeholders.

Long-term mitigation, Resilience building and Learning from Lessons.

Post an incident it is imperative to mitigate the effects to enhance resilience and return to normalcy.

The Way Forward

The CBRN field is governed by a variety of national regulatory agencies, as well as state and district law enforcement agencies – Ministry of Home Affairs, emergency management agencies, public health agencies and others. Response to CBRN/hazmat situations is also covered in the guidelines issued by the NDMA. Salient aspects for modernisation of our Police and paramilitary forces to effectively deal with CBRN incidents include:

Policy. Realistic threat assessment to develop a comprehensive National CBRN Security policy. Similar efforts need to be made at every state level for integration of CBRN Security policies to affect synergised and optimal response at all cities, critical infrastructure, transportation hubs, key venues and prominent public places.

Equipping. Procurement of state-of-the-art CBRN equipment for CBRN Response Teams at all states and district levels and coordination with partners, such as Armed Forces and NDRF, who can provide support for training and maintenance of such equipment and provide other assistance. Similarly, critical venues and infrastructures need CBRN detection equipment and on-site decontamination means which all response personnel must be made aware of.

Training. Provision of optimal hazmat training to Police Officers and personnel, especially of the Quick Reaction Teams and Quick Response Medical Teams. Synergising of training protocols across the spectrum of responders like local Civil Police, Firefighters, Special Police teams, Civil Defence and others is called for. Such training should include procedures for use of CBRN equipment, detection technologies, donning of PPE, decontamination and medical management of casualties.

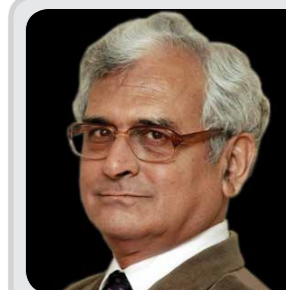
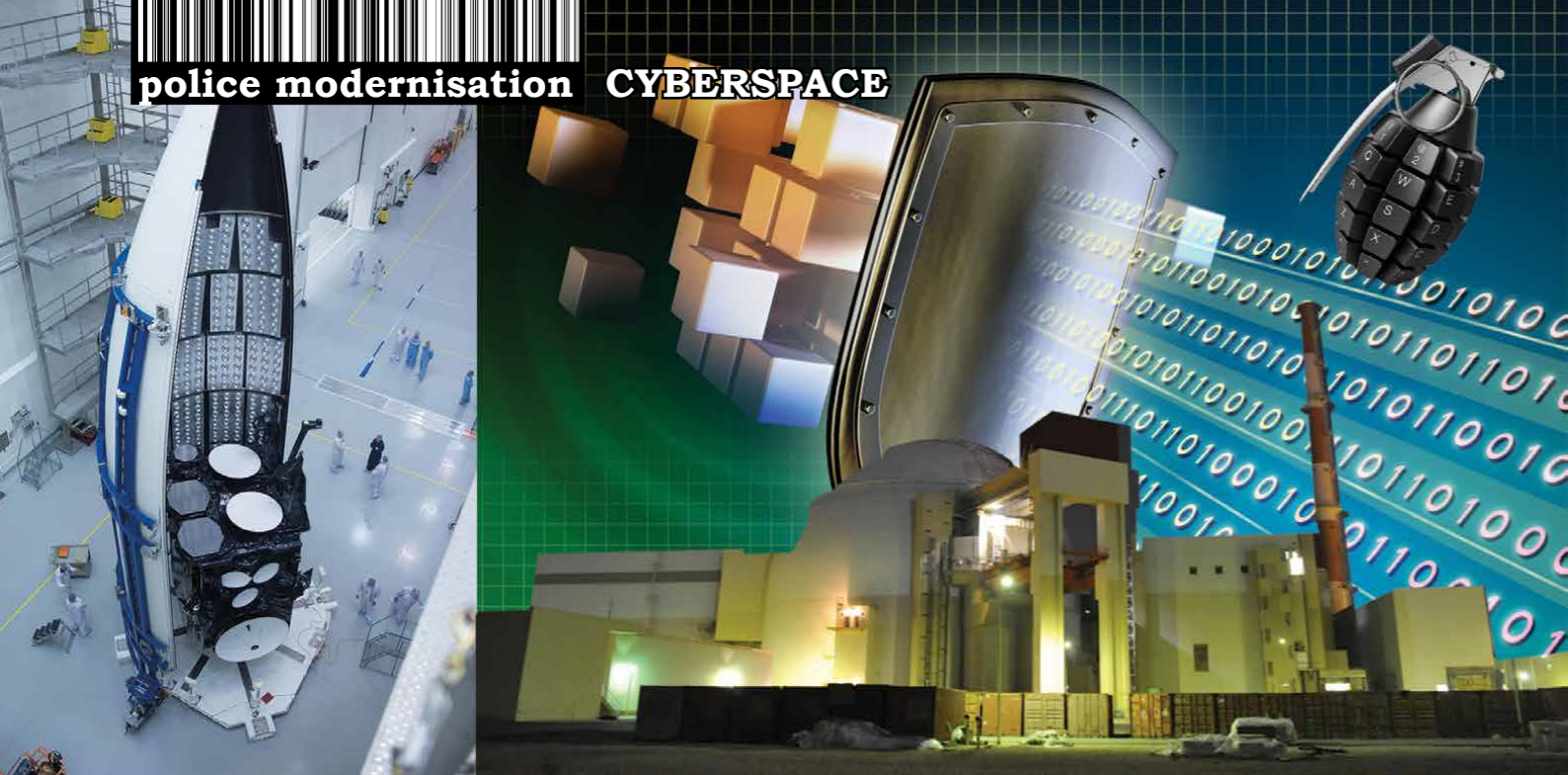
Dynamic Updating. Regular conduct of seminars, workshops, tabletop exercises and mock drills to keep abreast of latest technologies, techniques and procedures. Seminars and workshops must make full use of domain specialists and national and international subject matter experts. Such workshops and mock drills should be extended to districts and cities where CBRN threats are likely to manifest.

Technology. India has made great technological advancement in the last two decades. Indian Industry is now capable of producing world-class CBRN equipment. Many such players are offering state-of-the-art CBRN PPE, detectors, decontamination equipment, collective protection equipment (fixed and inflatable quick deploy CBRN shelters) and medical equipment. All these will enhance the response of our CBRN response forces.

Greater Awareness

India has secure borders but insecure citizens. Terrorists can slip into our societies and exploit our openness to inflict massive attacks. Analyses clearly indicate the possibility of CBRN terrorism in the Indian subcontinent. Large events are a security nightmare. India hosts numerous large events at varied venues, having huge socio-political importance. Ensuring security, especially from CBRN threats is a major concern. We need to be extra vigilant and fully prepared to prevent and deter and if faced with, react to CBRN terrorism incidents.

A key component in prevention and post-incident mitigation is public awareness



Dr Kamlesh Bajaj
The writer is Mentor Professor, NIIT University. He is a Distinguished Fellow at EastWest Institute, New York. He was the Founder CEO, DSCI; and Founder Director, CERT-In. Views are personal.

CYBER WEAPONISATION AND CYBER DETERRENCE

China, Russia, Tajikistan and Uzbekistan proposed an ‘international Code of Conduct for Information Security’ in the UN in September 2011, for non-proliferation of “information weapons”, obligating nation states ‘not to use information and communication technologies, including networks, to carry out hostile activities or acts of aggression, pose threats to international peace and security or proliferate information weapons or related technologies’. Note the proposed involvement of UN in cyberspace, which the United States and its allies are resisting in a global campaign involving industry, NGOs and academia.

Nuclear deterrence kept the United States and the Soviet Union in check during the Cold War. That is the analogy that has been invoked the most to conclude that some kind of cyber deterrence is essential in the information age to prevent a cyber war. But while the nuclear attacks would have a fallout in a localised region albeit a large one, cyber attacks, because of their global reach could target multiple sites and geographic regions, with devastating physical outcomes. The weapons, which are in the form of malicious code – the same code that can be used for financial frauds, identity theft, denial of service attacks – are easily available on the Internet for free or at a small price. Even if these are used to launch targeted attacks, it may not be possible to confine them, since sooner or later the attack vectors reach the ‘wild’ causing widespread unintended damage. Stuxnet was targeted at the Iranian nuclear reactors, but soon got into the entire cyberspace. This is unlike nuclear weapons that take large concerted programmes to develop or acquire clandestinely by nations. So, is there something as cyber deterrence?

Nuclear Deterrence Analogy
Cyber war has long been predicted, though in recent times more analysts have discounted its possibility. Analogy with a possible Pearl Harbour was drawn by Leon Panetta – the CIA Director in 2011 – while briefing the House Permanent Select Committee on Intelligence. Over the last few years the view that cyberspace is a ‘global commons’, similar to sea, land, air and outer space has gained currency. The global commons are for the good of mankind and should be used for the economic growth of all nations. But the United States chose to define it as the fifth domain as part of its military doctrine in its “Department of Defense Strategy for Operating in Cyberspace” that was announced in July 2011 – the US military’s first comprehensive blueprint for cyber security and cyber warfare. According to William Lynn (DOD) the United States reserves the right to respond to serious cyber attacks, even on private infrastructure, with “a proportional and justified military response”, because “the centrality of information technology to military operations” has made the US vulnerable to cyber

attacks. This worldview assumes that the cyberspace is primarily under the jurisdiction of military authorities – both defence and counterterrorism. The latter may include global surveillance and espionage, as is the case in the United States. Retaliation to achieve deterrence as a policy reflects the Cold War mindset of cyber security – the ideology of militarism that converts the problem to that of an existential issue requiring proportional response akin to that of nuclear first use by the adversary.

Concept Of Global Commons

However, there are other views of cyberspace that are being considered more seriously. For example, the governance of global commons of sea, air and space for access and stability has evolved internationally and rules of road have been created for them by the international community. History shows that dominating seaborne commerce and controlling sea routes enabled a country project its power capabilities. A State could become a military power through the control of routes – once again a militarist view. This led European thinkers to recognise the potential for international conflicts in the commons and hence, the need for international agreements to broad rules and regulations. Today some nations are trying to dominate the cyberspace by controlling it through transnational governance institutions that are under their control. Transnational mega corporations – the global monopolies that have emerged because of innovations that exploit the unique nature of cyberspace – control the lifeline of social media and search; all kinds of apps that impact human social, political, economic and cultural discourse. They exercise control over cyberspace by themselves and/or in partnership with their governments. So, it is the control of cyber commons that has dominated the thinking of policy makers – military or civilian.

Cyber deterrence is indeed necessary, if nations want to use the cyber commons

Cyber War

That the cyberspace is much more complex can be seen from its following characteristics:

- It is asymmetric – offense dominant, because the barrier to entry is too low.
- Attribution with certainty is a challenge – so how can response be targeted?
- Cyber incidents are largely carried out by criminals and hackers not necessarily sponsored by governments.
- Cyber espionage is a legitimate activity in which nations engage and likely will continue.
- Cyber weapons are made of the same malicious code – the malware used for crimes and espionage – but perhaps with higher degree of sophistication that may require intimate knowledge of engineering of targets, such as SCADA systems, for causing high levels of damage to the adversary.

But for cyber deterrence to take shape there must be spectre of cyber war. In ‘Cyber Security without Cyber

War’, Mary Ellen O’Connell states that though the “security concerns are as old as the Internet itself”, the world is probably “inventing a cyber war problem.”(Journal of Conflict & Security Law, 2012) Most intrusions are categorised as ‘computer network exploitation – CNE’, which target theft or espionage. Some of them such as attacks on Estonia, NATO’s response and Russia-Georgia conflict (during 2007 and 2008 respectively) could qualify as ‘computer network attacks – CNAs.’ But the Stuxnet worm was a CNA that destroyed the centrifuges of Iranian nuclear reactors. It was destructive but not enough to qualify as cyber war. Attribution beyond doubt is not possible in any of these three instances. While the first two are generally attributed to Russia, NATO concluded that, “there is no conclusive proof of who is behind the Distributed Denial of Services (DDoS) attacks (on Georgia) as was the case with Estonia.” Likewise, the third is generally attributed to the United States and Israel, but it can’t be said so categorically to invoke the US doctrine noted above. But one thing is clear that several governments are developing cyber weapons and testing waters and want to be ahead in the race. A McAfee report had put the number at over 130 countries.

Thomas Rid in The Journal of Strategic Studies, February 2012 writes that “Cyber War Will Not Take Place.” This view is just the opposite of the ideology of militarism of cyberspace. He discusses all of these cyber incidents and the policy pronouncements of William Lynn and Leon Panetta noted above. He also refers to Richard Clarke, former White House cyber czar, who presented several hypothetical scenarios of wars in South China Sea leading to critical infrastructure attacks resulting in calamities that will be of magnitude much higher than those of the 9/11 attacks. Rid invokes Carl von Clausewitz on the concept of war, who has said that a war has to meet all of the following three criteria: (1) an act has to be of violent character; (2) war has to have instrumental character – it must have ‘a means and an end’; (3) an act of war is always political.

Pros And Cons
Rid concludes that some of the cyber attacks meet one of the criteria, but not all three, including the Stuxnet worm unleashed on Iranian reactors. But perhaps this classic definition of war is dated, since modern wars use technology that is invisible – only the impact is felt. Cyber attacks are non-violent though the outcomes maybe devastating. Attribution to nation states is not possible. Even a writer like

Jeffrey Carr who was quick to point to China for any attacks (even Stuxnet) has revised his views. He has echoed NATO findings. In the recent cyber attack on Sony Studio, even though President Obama attributed it to North Korea, Carr has refuted the claim based on his team's detailed analysis. It should be noted that criminals, terrorists and non-state actors can successfully hide their identities. Between them they can cover the entire spectrum of crimes to war; former being mostly apolitical, while the latter is always political. According to Rid, political crime is somewhere between these two extremes and these can be described as three types of offenses: subversion, espionage and sabotage. Sabotage is technical in nature and aims to weaken or destroy an economic or military system. For example, a 'kill-switch' embedded in Syria's air-defence system rendered it useless in 2007 and could not detect Israeli squadron of *F-151* and *F-161* warplanes entering the Syrian airspace. Stuxnet is, of course the more well known sabotage attack on Iran. Espionage does not violate any explicit provisions of international law, though the scale in cyberspace has caused alarms worldwide. Subversion is to overthrow governments – like the Arab Spring – and undermine the established authority in a country.

Why Cyber Weaponisation?

So, if we follow this classic definition of war, there is no cyber incident that signifies cyber war, nor there is any likelihood of cyber war. Then what is cyber weaponisation for. Countries are indeed developing malicious codes for launching attacks on adversaries – their critical infrastructures, infrastructure essential for military supplies and logistics, poisoning the ICT supply chains, installing backdoors in equipment being supplied to friendly and not-so-friendly nations (NSA surveillance makes no distinction between friends and foes). Weaponisation is for gaining supremacy in cyberspace. Deterrence is not in the nuclear war sense. It is more for retaliation to cause collateral damage, to show cyber power. Not necessarily to bring the adversary to accept the political will or subjugation of the attacker. But more like guerrilla warfare that is forever bleeding the enemy – inflicting thousand wounds.

Joseph Nye says that, "statements about power always depend on context and cyberspace is a new and important domain of power." He traces "three faces of power" as part of behaviour power and states that, "hard power behaviour rests on coercion and payment. Soft power behaviour rests on framing agendas, attraction or persuasion." But the challenge in cyberspace is that even the United States – strong in both of these powers – finds it difficult to control their borders in cyberspace, even though they very much want to do so, notwithstanding their views that the Westphalian state model in cyberspace has to give way to a networked state, subject to governance by transnational private institutions like the Internet Corporation of Assigned Names and Numbers (ICANN). No wonder the Chinese are trying to set the agenda too.

The next major conflict will start in cyberspace

How Do China And Russia View This?

China is trying to set the international agenda on cyber security – the soft power approach. Cai Mingzhao, Minister of the State Council Information Office proposed in the EWI Cyberspace Cooperation Summit in November 2013 at Stanford University that, "to maintain cyber security, we need to ... show respect for national sovereignty over cyberspace; ... build a robust legal system; ... strengthen international cooperation." He suggested the following: international rules for behaviour in cyberspace (transparent governance of cyberspace and UN as a discussion forum); defining effective means to tackle urgent problems (with role of UN Group of Government Experts in ICT); create communication channels to facilitate international cooperation. Note the proposed involvement of UN in cyberspace, which the United States and its allies are resisting in a global campaign involving industry, NGOs and academia.

China, Russia, Tajikistan and Uzbekistan proposed an 'international Code of Conduct for Information Security' in the UN in September 2011, for non-proliferation of 'information weapons', obligating nation-states 'not to use information and communication technologies, including networks, to carry out hostile activities or acts of aggression, pose threats to international peace and security or proliferate information weapons or related technologies'. In the same month, Russia introduced another proposal for an international agreement, which is more detailed than the 2009 Agreement

between the Governments of Member States of the Shanghai Cooperation Organisation on Cooperation in the Field of International Information Security. (Russian Federation, The Ministry of Foreign Affairs, Convention on International Information Security (Concept): <http://www.mid.ru/bdomp/ns-osndoc.nsf/1e50de28fe77fdcc32575d900298676/7b17ead7244e2064c3257925003bcbcc!OpenDocument>

Notice the focus on information security instead of cyber security. This is because Russia and China being worried about the threat posed by content and the need for 'Internet sovereignty' interpreted by the West as the ability to control over the information space. In the name of human rights, are the Western states demolishing the Westphalian state model? Is it a new cyber weapon?

But how is war being viewed by military strategists by the induction of ICT? Qiao Liang and Wang Xiangsui – two colonels – in *Unrestricted Warfare* published in February 1999 by the PLA Literature and Arts Publishing House, Beijing, said the Gulf War changed the world and that "... war itself has now been changed." Satellite communication, multiple ground stations across the earth, guided weapons deployed at many places are coordinated through C3I systems for targeted attacks. Now the scenario includes cyber weapons that can penetrate the enemy systems, even though they are of similar sophistication. Clearly there is more militarisation of cyberspace and more distrust among states.



Cyber deterrence is indeed necessary, if nations want to use the cyber commons for their economic growth.

Where Is India?

There is not much visibility in the public domain on Indian plans of cyber weaponisation, if any. The cyber security establishment – both defensive and offensive – and the military command do not discuss these in the open. Nor are there many papers on the subject. There is the National Cyber Security Policy of July 2013, but without any implementation details. It is an irony that while India is the global hub of IT services to the largest global customers, the industry gets little traction in the form of consultation or farmed out R&D contracts for development of weapon grade code, or defensive software to deploy resilient systems and deny the successful attacker access to any deep assets. The mindset has to change – trust in the private sector is the key.

More Cyber Weaponisation Trends

Let us look at the continued cyber weaponisation that the United States, arguably the most advanced in this, is engaged in. Snowden documents published in the German magazine *Der Spiegel* over the last few months give a glimpse that *People's Daily* has picked on – the NSA is "planning for wars of the future in which the Internet will play a critical role". A project code-named "Politerain" seeks interns as hackers to destroy adversary's ICT infrastructure remotely. It aims at destroying computers, routers, servers, network-controlled devices and even "erase the BIOS on a brand of servers that act as a backbone to many rival governments." The goal of the internship programme was "developing an attacker's mindset," according to *Der Spiegel*.

The surveillance of the Internet is merely said to be "Phase 0" in the US digital war strategy, in which vulnerabilities in adversary systems are discovered, followed by "stealthy implants" in them leading to "permanent access", culminating in achievement of "Phase 3", namely "dominate". Snowden documents are said to state that the NSA can control and destroy "at will through pre-positioned accesses" critical systems and networks such as energy, communications and transportation, with the power to engage in 'real-time controlled escalation'.

People's Daily quotes an NSA presentation, citing *Der Spiegel* that "the next major conflict will start in cyberspace," stating that atomic, biological and chemical weapons – widely referred to as the ABC

weapons – have been extended to D, namely digital weapons. It is the D weapons that the *People's Daily*, quoting the report, stresses: "For the 2013 secret intelligence budget, the NSA projected it would need around 1 billion dollars in order to increase the strength of its computer network attack operations. The budget included an increase of some 32 million dollars for 'unconventional solutions' alone." The NSA is said to aim "to use the Net to paralyse computer networks and, by doing so, potentially all the infrastructure they control, including power and water supplies, factories, airports or the flow of money," according to the *Der Spiegel* disclosure.

It should not come as a surprise that "plausible deniability" is the guiding principle of NSA while launching cyber-attacks, while making it impossible to trace the sources of the attackers. "This approach threatens to transform the Internet into a lawless zone in which super powers and their secret services operate according to their own whims with very few ways to hold them accountable for their actions," it added.

Cyber Arms Race Is On

Cyber weaponisation continues, while nations are talking cyber deterrence at various forums – bilaterals, think tanks, multilaterals and the UN. But the cyber arms race is on. Glimpses get revealed now and then. Asymmetric nature of cyberspace has enabled smaller nations like North Korea take on bigger powers like the United States. Non-state actors are powerful in cyberspace because of low barriers to entry and are also being used by nation states to take advantage of non-attribution. But development of next generation cyber weapons requires heavy investments by nation states, continued R&D involving industry and academia. Stuxnet is only the harbinger of that. Hence, it is the nation states which will have to negotiate any cyber arms control framework – rules of the road for state behaviour or a treaty. But because smaller countries too have a chance, it is worth recalling Joseph Nye's conclusion that, "The largest powers are unlikely to be able to dominate this domain as much as they have others like sea or air. But cyberspace also illustrates the point that diffusion of power does not mean equality of power or the replacement of governments as the most powerful actors in world politics." **DSA**

ADVANCED TECHNOLOGY SOLUTIONS



POLICING FOR MEGA CITIES

Securing the Indian mega cities will require much more than just the physical presence of police. It will certainly require the advanced technology/equipment that can diffuse demonstrations, decrease criminal activities/curb terrorism and also enhance the peaceful unity of the citizens living in the mega cities/throughout India.

The ever-increasing terrorism threats, economic recessions, anti-government demonstrations and crimes around the world have changed all police services and have also changed/increased the daily risk factors for the brave policemen/policewomen by several notches. Technology has removed borders and barriers; changes in society have opened up new opportunities and challenges; increasing investment in public services and a growing consumer culture has led to rising expectations of customer service. The core role of the police service is and will remain prevention, detection and reduction of crime and protecting the public.

Personnel Behind Machines

Like all public services, the police service cannot be immune from further change and continuous improvement. Indeed the service has shown itself prepared and willing to embrace change and meet new challenges, whilst maintaining the enduring values of the Indian police. Technical upgradation is a key factor in enhancing the efficiency of the police. At the same time, it is not to underplay the key importance of the human factor, ie the manpower, which is manning the police system and also needs to be upgraded in terms of capacity by imparting relevant and regular training modules /real time risk drills in the specific city/town

to analyse the response times in relation to the particular threats posed.

The modernisation of Indian police forces for the mega cities (and throughout India) will need a new real time systematic approach with professional training modules that are already active as the best former/current police officers/military professionals from around the world share their knowledge/experience factors thus reducing the costs for the new Indian policing systems that can be installed/activated by the **DSA** WHS Group which already has the software/technology as well as the elite specialists on-board to serve the Indian police/military forces and Indian Government. It includes the new 'India Nationals Intel Module Software' which facilitates the facial recognition software, biometrics, travel tracker and financial forensics data representing best practice in the use of intelligence to fight crime/terrorism groups. The key intelligence products are strategic assessments, tactical assessments, target profiles and problem profiles to assist in:

- Better detection of crime/terrorism acts.
- Increased conviction rates with the effective use of information/intelligence and the highest standards of detective work.
- A strategic approach to science and technology that is activated in a timely manner.
- Tougher action on persistent offenders.
- Better support for repeat victims.
- More timely effective action against organised crime/terrorists.

Intelligence-led Policing

This sets out a focused approach to gathering and using intelligence. Indian security forces in the new mega cities need to determine the issues on which they need intelligence, to gather it and then to have the ability (training) to analyse the results. Properly applied, the model greatly improves the information flows within a police force, providing a better basis for decisions and allowing resources to be targeted to where they will have most effect. The software and module can be applied at different levels of activity and underpins the concept of intelligence-led policing. India mega city policing modernisation should/will include the following technological and non-technological components.

Technological Components

CCTV Surveillance: The mega cities or any other city in India for that matter should be completely covered by a sophisticated network of CCTVs and must have analytics. It must be ensured that the vital public places and critical/sensitive infrastructure is covered by the CCTV network. Special care may be taken to cover such areas which are more densely populated or prone to crimes.

The CCTV network should be based on wireless system to the extent possible except places which are important from national security point of view wherein it may not be advisable to share data openly. Apart from installation of CCTV by government agencies/police, it is equally important that private sector is also encouraged to play an important role on equal footing. Accordingly, the private sector industries and business houses may be exhorted to install similar and compatible CCTV network from where data generated could be transmitted to the C4I unit base. The storage capacity in the servers should be for at least 60 days.

The C4I Unit Base: The C4I (Command Control Communications Computers and Intelligence) Unit Base

would be the heart of the entire mega cities project. The Unit Base, which would be a large hall, may have three or four sections within it. The C4I Unit Base should have a network of computer systems, which would enable collection of feeds (data-video, video, text) from CCTVs and other devices and should have the capacity to store, analyse and disseminate it, wherever required. There would be video walls, where live feed from the CCTV installed in the city would be received continuously with flexibility to focus (zero in) on a particular CCTV camera. It should also have the facility of GIS (Geographical Information System) to know the exact location of the source from where the data is coming to the C4I Unit base. This C4I Unit Base would be something like ATC (Air Traffic Control) at airports, which will control and direct the functioning of policemen/policewomen, police cars etc for timely action.

A part of the C4I Unit Base can be dedicated for storing and handling segregated data, which comes to the C4I Unit Base for proper analysis. This can be called data centre (smaller version of Fusion centre). The data centre should have 1-5 data analysts, depending on the size of the Indian city. They shall be responsible for generating vital information for taking preventive action or helping the investigation process in case of crimes and other emergencies. The data centre can also have the facility of face recognition and other analytic facilities.

Fusion/Data Centre: Fusion/Data Centre has been partly mentioned in the details of the C4I



Jo S Birring
The writer is the Chairman and Group President of The World Homeland Security (WHS) Group of Companies that focuses on World Intelligence Meta Tactics, Anti-terrorism training modules, software solutions and corporate asset risk investigations. He is **DSA** representative for Europe and the Americas.

The C4I Unit Base would be the heart of the entire mega cities project

Unit Base as above, where focus has been laid on the data centre. The Fusion centre is a much bigger concept and this facility, if at all necessary, may be created at the state level or national level only to collect, analyse and disseminate various data inputs having bearing on safety and security. The State governments should also have one at the state level. This Fusion/Data Centre would be playing a crucial role in prevention and detection as also investigation of crime or security related challenges. It will, however be necessary to have up-to-date and comprehensive databases from various fields, for example, vehicle registration numbers, Unique ID numbers (Digi Card activation) of the citizens, residential addresses, PAN card details, crime records related details etc.

Highway Patrol Cars: Modern highway patrol cars have a very vital role in the maintenance of law and order/control of crime by the police. These cars should be of high-speed with capacity to chase and overtake the criminals. These cars should be well equipped with surveillance equipment like ALPR (Automated License Plate Reader), intelligent cameras, computer system (ruggedised laptop interconnected to the C4I Unit Base and other security equipment also including laser tasers. These vehicles should be both mobile as well as stationary according to the city/location.

Aerial Surveillance (UAV /Helicopters etc): It is very essential to have surveillance from air with regard to law and order and other crime/possible terrorist-related activities in the cities. The air surveillance can be obtained by positioning various equipment ie balloons, UAVs and helicopters etc which should have gadgets like cameras, sensors etc to cater to the specialised requirements on the occasion. The data (video, audio, text) collected from these devices should be fed to the C4I Unit Base for necessary action for both preventative and post incidence operations. This element can also serve as a very effective means to check incidence of law and order as also check on the activities of criminal/terrorist elements as a deterrent factor.

Non-technological Components

Community Policing: The involvement of community in controlling law and order situations and crimes in the cities is of paramount importance. One of the ways to enlist the support of community is to have a regular schedule of interaction at the police stations. For this, the police stations should have room/conference hall having bold marking on the front of it as 'Police Community Centre'. It should have the capacity of say 100 people where face-to-face interaction with community leaders and police personnel could take place. These meetings could be organised at

least once every week on fixed days in a week. The community leaders would in this way work as agents of police to spread necessary message in the society. The creation of room/conference hall in the police stations could be made integral part of design of a police station and could be funded through the local politician/political party whose responsibility it is to safeguard the people who voted for him/her at election time and they can fund it under the Plan Budget.

Safety And Security Education: The involvement of schools/colleges and children from initial stages regarding education on the safety and security of the community is extremely important as it happens in the Western countries. The children in their schooldays should be imparted lessons on community safety and security as also responsibility and duties of citizens towards society. It would be ideal, if different Boards of Education at the Centre and State level could be impressed upon to include a chapter on the basic concept of community safety and security, community policing, response on emergency situations etc in the curriculum of the school textbooks. This step will ensure that the safety and security aspect of community is to be taken care of by all including the school children, who later grow as responsible citizens of the country.

Soft Skilling: The training of policemen should include components on soft skill, attitudinal change etc along with their operational training. The physical fitness of the policemen needs to be strictly maintained so that they can perform their duty efficiently. The overall look including the uniform and the gadgets that the policemen use need to be made smart and friendly.

More Police Women: Women in police at all levels in police hierarchy (30 per cent) of the force, will go a long way in building trust between the society and the police as also for control of crime against women in the society. Necessary legislation, if necessary, needs to be undertaken by the different State governments in this behalf. Women presently need to be treated at par with their men colleagues so that they can work with equal confidence and efficiency.

Securing the Indian mega cities will require much more than just the physical presence of police. It will certainly require the advanced technology/equipment that can diffuse demonstrations, decrease criminal activities /curb terrorism and also enhance the peaceful unity of the citizens living in the mega cities /throughout India with the new **DSA** WHS Group neighbourhood watch tactical software, C4I Units and RFID Monitoring Modules that once activated enhance ethical balanced cognitive fusion thus preventing crimes/loss of lives. **DSA**

CCTV network should cover areas which are more densely populated or prone to crimes

WOMEN IN POLICE



It was in April 1978 that I got the news about my selection in the civil services. I was on top of the world. A dream to join the coveted IPS fulfilled. When I joined the national police academy for training I found myself as the only lady officer in the batch.

If we look at the scenario today we find that there are 10-15 lady officers in a batch of about 130-150 officers. It only shows that there is a trend towards more women joining the IPS. But it is still far from equality in the gender ratio.

Appalling Figures

If we look at the number of Women in Police at the National level the figures do not show an encouraging trend. As per the BPR&D figures as on 1 January 2014, the lowest per cent of women in police is in Assam followed by Nagaland, Meghalaya and J&K. The best ratio we find is in Chandigarh followed by Tamil Nadu, Andaman & Nicobar Islands and Himachal Pradesh. Maharashtra is showing progress with 10.48 per cent women. Surprisingly Kerala has only 6.42 per cent women in their force. Delhi Police has only 7.15 per cent women. Figures as on April show 9.8 per cent women in Delhi Police. If we look at the numbers we find that UP has 7,238 women out of the total 1,68,851 force. Maharashtra has 17,957 women as against total force of 1,71,359 in Police.

The all India figures about the ranks and number of women in police are equally appalling. 60 women as DG/IG, 20 DIGs, 1,234 Inspectors, 9,221 SIs/ASIs and 85,696 constables constitute 1,06,325 of the total women police strength. The all India per cent of Women Police to total police is merely 6.11. This shows the extent of minority status of Women in the Police even today.

In CAPFs there are only 77 women officers at the gazetted level and 18,394 women in other ranks as on 1 January 2014.

In 1972 the first Lady IPS officer to join the police was Ms Kiran Bedi. Only 1 or 2 women officers joined every year (1976 and 1977 were the exceptions) till 1989. 1990 was the first batch to have 9 women officers followed by 7 women officers in 1991. In 1992 again

only 2 women IPS officers joined. The encouraging trend started only with 2006 when around 20 women officers joined. 2008 batch had the maximum number, when 24 lady officers joined.

Level Playing Field

Although in acute minority, women police can be seen at all levels. There is no indication of equal status though.

It is generally sideline roles or essential duties that only women can perform that are assigned to women police. Women are generally used for security duties, frisking etc, welfare tasks, to deal with women complainants, as investigating officers for crime relating to women. There is total lack of mainstreaming. Although we see some exceptions here and there.

The latest trend to create Women Police stations is an example where we try to create exclusive areas of responsibility for women rather than integrate them into the mainstream. This is leading to strengthening the sidelining and stereotyping of women. The need in the 21st century is for inclusive police. Women and men should work together as partners in social change rather than divide them into different compartments.

Acceptability

Continued minority of women is the result of non-acceptance of women in the police. Recent furor over crime against women has made the leadership of police and the government to realise that it is imperative to bring in more women in the police not only for meeting the increasing demand for essential duties but also to fulfill the rising aspirations of women for equality in society. More women in the police will surely empower women, make the police force gender sensitive and will lead to better status of women in society. Voice of women has hitherto gone unheard and they must join the police in good numbers to make their voice heard.

It is no longer possible for the government to deny the right to dignified and empowered status to women and provide an atmosphere of freedom and equality to women in society at large. And this is possible with more women representation and mainstreaming of women in the police at all levels, in all duties. **DSA**



Vimla Mehra IPS

The writer is a distinguished police officer with qualities of Leadership with Social Responsibility. She is MA in Sociology and MPhil in International Relations and joined the National Police Academy in 1978. The cause that is closest to her heart is the empowerment of women and her two stints at the Crime against Women Cell, first as Deputy Commissioner of Police and then as Joint Commissioner has given her unique insights into women's issues and the vulnerabilities of women. She introduced the **1091** helpline and Post Box No **5353** to provide immediate and effective help to women in distress. Now, working as Special Commissioner of Police, Administration, Delhi Police she is devoting her wholehearted efforts for the betterment of Delhi Police. She has received President's Police Medal for Meritorious Service in 1995 and President's Police Medal for Distinguished Service in 2003.



CRIMINOGENIC FACTORS



While many factors put together do provide an excellent medium to cultivate the virus of crime, no individual factor can be said to be solely or in isolation responsible for crime. At one time it was widely believed that poverty gives rise to crime. But modern studies have brought out that there is no strong correlation between them.

In the international context, a mega city is an urban conglomeration in excess of 10 million population and few of these may be approaching the vicinity of 20 million population. One common factor in all mega cities is the very high population density and the spread of city over a large area, sometimes terming the spread to a *region* rather than to a *city*. In the Indian context, the term mega city refers to those cities which have population of 10 lakh (1 million) or more. As per last census, held in 2011, there are 53 such cities (urban conglomerates) in India. The population of these 53 mega cities constitutes nearly 13.3 per cent of the country's total population. As per information published by National Crime Records Bureau, a Government of India agency, while All India Rate of Crime for the year 2013 stands at 215.5 (absolute figure at 26,47,722 cognizable crimes under Indian Penal Code) per 1,00,000 of population, the mega cities crime rate is 345.9 (absolute figure at

5,56,024). Thus the mega cities have much more crime per thousand population as compared to the All India rate. In fact these 53 cities have accounted for 41.1 per cent (68,024 out of 1,65,690 cases) of the total auto theft cases, 28.0 per cent of total cheating cases (30,085 out of 1,07,330 cases) and 29.4 per cent of total counterfeiting cases (691 out of 2,349 cases) in the country. It is obvious that we have to look deeper for special criminogenic factors in mega cities which contribute to crime generation than that provided by the bare theories of sociology. Interestingly, a workshop held at the 12th UN Congress on Crime Prevention and Criminal Justice, Salvador, Brazil, April 12-19, 2010 by International Centre for the Prevention of Crime in collaboration with United Nations Office on Drugs and Crime (UNODC) observed (published 2011) that urbanisation is not inherently criminogenic, nor is the city size necessarily a key factor. It is the *inequality* that urbanisation fosters, in terms

of the living conditions and relationships, which help to generate crime and victimisation in the urban setting. Let us therefore examine the underlying issues in detail.

Skewed Distribution Of Resources: The distribution of social bounties in a mega city is skewed in favour of the rich. The poor normally reside in concentrated pockets in the peripheral areas of the mega cities. These areas are characterised by absence or weakness of basic urban infrastructure, basic social services and community organisations. Open spaces are limited. Supply of potable water is either not there or is scant. Fear of eviction is always lurking. There is every day quarrel over sharing of these items. Children watch their parents fighting among themselves or with neighbours. Drunken brawls are common. Very few educational institutions would even think to open their school branches in such areas. Neglected children in these poverty stricken pockets are vulnerable to be sucked into criminal streams due to multiple causes.

Migrants And Crime: For the population in smaller cities, the mega city signifies better quality of life in terms of education, health, transport and also better job opportunities. Their steady migration puts pressure on scarce resources in the mega city. Some adopt criminal route to corner the resources. Mega cities are also the destination of choice for the rural poor migrating in search of worthwhile employment. Few of those who are not lucky enough to get gainful employment may get drawn towards committing crime. While in their native place they would not commit crime even if in financial difficulty, for fear of getting bad name for the entire family if caught, there is no such fear in a big city where anonymity is the order. A large male population in cities is living alone leaving their families behind in village or in another city. This generates demand for sexual gratification and consequential network of prostitution. They operate in organised fashion as massage boys/girls, escorts, Net-friends, call girls, pimps and regular business in city red-light area.

Slum Population And Crime: Many mega cities include a significant slum population. It has been brought out by Indian census figures 2011, available at www.censusindia.in that more than 40 per cent of households in Greater Mumbai were in slums. By their very nature of establishment, slum tenements offer a tiny piece of space per family. They are highly congested, constructed in vast continuity leaving no space between them and they are invariably crowded. Many of the inhabitants reside there, males only, leaving their families behind in villages. Few, who bring families, cannot take care of them when they are out for the entire day to earn their livelihood. Young boys and girls

left in jhuggis in a slum area are vulnerable to the temptations thrown by the sex predators. The situation is conducive to sex related crimes. These areas also feed the organised sex markets of the mega city.

Criminal Route For Shortcut To Success: As is obvious, the resources in these mega cities are limited and there is stiff competition for them. For example electricity may be available at a price in most of the areas in a mega city, but many would still try to steal it. While a poor in the slum would place a hook on the nearest electric pole and steal it to light his one room tenement, there could be a rich businessman laying a concealed cable to steal the electricity for his factory, so that his cost of production is kept low as compared to his competitors. Both have committed the same crime. Take another example. Normally it takes time to establish a business and start making profit. But there are those running ponzi schemes in such places. They promise very high return on Capital invested in a short time. After collecting investment from a large number of gullible populations they would close their office and quietly vanish, only to reappear in another mega city under another banner. Manipulating property records and fraudulent selling of property, grabbing land and house of others specially old and infirm who have no one to take care is also common in these places. Trying to maintain extravagant lifestyle without having means also generates crime in mega cities.

Information Explosion And Crime: The television is a great source of spreading information and knowledge. But there are some with criminal bent of mind, who learn new techniques of committing crime from TV serials. They also try to learn methods by which they could wipe out crime trail and avoid getting caught by police. A mega city offers enough opportunities to commit crime and they make attempts after complete planning as per their understanding. Some get caught while few succeed and in due course become hardened criminals. Low arrest rate, lengthy court proceedings, easy bail and very poor conviction rate emboldens them.

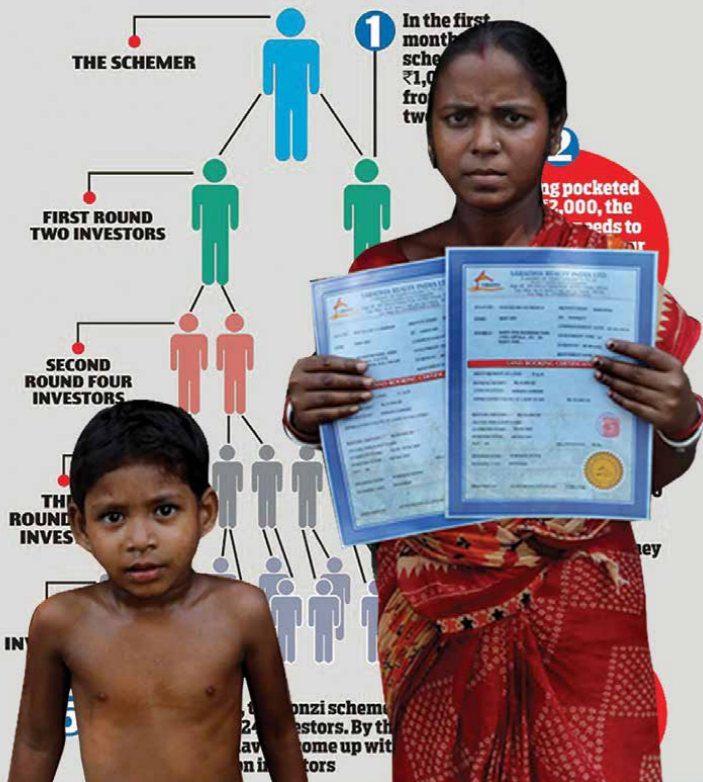
It is the inequality that urbanisation fosters, which helps to generate crime



Sharda Prasad IPS

The writer is a Postgraduate in Physics (1971) from Allahabad University, with specialisation in Electronics. He also has a Bachelor's degree in Law from Delhi University. He joined the Indian Police Service in 1973 and superannuated from the high rank of Director General in 2010. Earlier, he worked as Director, National Institute of Criminology and Forensic Science in 2002-2004 and Director National Crime Records Bureau in 1998-2000. He was the Chairman of the Committee on Technology introduction in Police and had conceptualised the present project of Crime & Criminal Tracking Network (CCTNS), being implemented throughout the country. He has been awarded Indian Police Medal for Meritorious Services in 1994 and President's Police Medal for Distinguished Services in the year 2006.

THE PONZI PYRAMID



Showing Off And Crime: Who does not need money? But some in the mega city need it to show off. To please their boy/girl friends and entertain them in costly restaurants/bars and take them out on long drives in costly cars they need money. Such persons, mostly young, do not hesitate to commit crime like stealing vehicles, looting and highway robbery. Once successful, they become bold and commit more serious crimes. Some may even commit murder just to rob a person and eliminate the crime trail. The existing measures to rehabilitate juveniles are woefully inadequate. In most of the cases they learn quickly from other offenders and graduate to a regular crime life.

Young boys and girls left in jhuggis in a slum area are vulnerable to the temptations

Inadequate Policing: The policing in mega cities does not measure up to the desired level. To begin with, their numbers (141 police persons per 100,000 of population as per figures from NCRB for year 2013) are not adequate. Over the years, there has been large scale addition to the numbers of paramilitary battalions. The situation is such that in some States, the Armed Police Battalion strength is more than that of Civil Police. While the Armed Police are indispensable in containing law and order situation and *bandobast* duties as in case of elections, they are of little use in day-to-day policing. There is no emphasis on adding to the number of policemen in existing police stations. Many times, new police stations and police posts are announced without sanctioning manpower for them. The head of Police Force does not have powers to create posts for these new establishments. As a result, wherever the population density is very high as in case of mega cities, the policing is spread thinly on the

ground leading to inadequate and ineffective policing and security measures. The effective policing is then confined to smaller areas, euphemistically called 'no tolerance zone', while larger areas remain practically un-policed. The problem is compounded when due to lack of adequate manpower, police tacitly avoid going to certain areas, leaving them to the *dadagiri* of local mafia. It is in such areas where illegal liquor distillation, drug peddling and prostitution flourish.

Mega Opportunity For Crime: Mega city setting provides better opportunity for committing crime. Inadequately guarded ATMs, unprotected cars and bikes, people moving with large cash on way to bank or coming out from bank, lonely morning jogger adorned in gold chain all provide good setting for committing theft or robbery and getting away without getting caught. Illegal arms are easily available for a modest price to help in committing crime. In every mega city gangs operate protection racket. They also fight amongst each other for turf supremacy or commit revenge killings. Some are in the business of contract killing. They may also have links in police and judiciary to help them in case of need. Due to large volume of crime in mega cities, such linkages escape notice of authorities. The gangs continue to operate without fear of getting caught or punished for crime. Their acquittal in broad daylight crimes, encourage those criminals who are fence-sitters in crime.

Drugs As Precursor To Crime: Easy availability of drugs in mega cities leads to early catching of drug habit among vulnerable children, say street children or children from broken families. Once they are addicted, they commit petty crime to earn their daily quota of drugs. They also take to drug peddling and acting as couriers for drugs. It takes not much time, before they start committing bigger crimes. Drug joints are well known in any mega city and any auto-rickshaw can take you to the nearest such joint or even to a pan-cigarette shop which on the sly peddles small doses of drugs as well. In another setting, some students in schools and colleges take to drugs under peer pressure and after some time when their financial means are not enough to meet their demand to satisfy increased craving for drugs, they take to crime to earn easy money.

No Nexus Between Poverty And Crime
While the above factors put together do provide an excellent medium to cultivate the virus of crime, no individual factor can be said to be solely or in isolation responsible for crime. At one time it was widely believed that poverty gives rise to crime. But modern studies have brought out that there is no strong correlation between them. On the other hand modern city planning where there is ample space between two neighbourhoods, combined with thin population density, vast park areas with lonely stretches, inadequately lit and deserted roads and bends, contribute to higher crime as they offer better opportunity to a criminal to commit crime. **DSA**

POLICE FORCES FOR CI AND CT

The Centre palming off responsibility of the Naxal problem to the States is apparently because the MHA failed to create a set-up, a unified operational command set-up and preferred to remain in the background. This could have been done in conjunction with the CAPFs but instead unaccountability was preferred. The negatives can be seen with the Home Minister's recent call to define a new counter-Naxal policy – what have we been doing all these years?

That the police versus population ratio in India is amongst the lowest in the world is an established fact. This apart, police forces have also been battling terror and insurgents over the years and there are large deployments in Naxal infected states. In the latter case Home Ministers and Chief Ministers have been saying that the issue will be resolved in next 2-3 years but these forecasts have not gone beyond media hype. There are also periodic announcements that police forces' modernisation is 'on track' but there appears to be little headway at ground level. The needless Centre versus State authority controversy has blocked national synergy in addressing serious threats to national security. In addition, are the internal Police versus Central Armed Police Forces (CAPFs) conflicts that though hidden from the media adversely affect smooth functioning. These then, along with the vote bank

politics, need to be reviewed in holistic fashion, which unfortunately remains largely unaddressed.

Centre Vs State

The chicken versus egg debate may well be applied to the law and order versus terrorism-insurgency debate in India. Take the case of the Naxal insurgency, which Prime Ministers have been describing as the biggest internal security threat to India. When the problem is spread over multiple states affecting some 40 per cent of the country's population, the wisdom of dealing with the problem at individual state level is highly debatable. This has happened despite the counter-insurgency models that we have on ground in J&K and in the Northeast – particularly with regard to single point operational control of counter-insurgency forces. The Centre has largely absolved itself of responsibility with the promise of additional CAPF units as required and routine IB warnings. When Chidambaram as





Home Minister had put forward the proposal for establishing the NCTC, he had also simultaneously proposed a separate Ministry of Internal Security. It needs no genius to discern that in its modern *avatar*, the MHA has such vast responsibilities that forces it to resort to daily firefighting. It is unthinkable why the MHA should be burdened with defending international borders, which should have been under the Ministry of Defence in-line with the 'One Border, One Force' concept. For example, can one visualise what difference it would make if the India-Bangladesh border was placed under GoC Bengal Area?

Andhra Paradigm

What has been the effect of say the States made responsible to deal with the Naxal insurgency? Under the previous government, the Integrated Action Plan (IAP) for Maoists affected states went retrograde once its responsibility was shifted to the States and the Centre ceased monitoring. Now the Special Infrastructure Scheme (SIS) for Naxal affected states is on the verge of closure because of devolution of central pool of taxes to the states. The SIS was a key security scheme meant for the four States of Chhattisgarh, Jharkhand, Odisha and Bihar to help them create Special Anti-Naxal Forces (SANFs) based on Andhra Pradesh's successful Greyhounds force. The SANFs were to be trained by special instructors trained at Greyhounds academy, each state getting some 40 special instructors, initial setback to the scheme already having been caused through creation of separate state of Telangana.

Politico-Police-Naxal Nexus

It appears that the decision to transfer more and more power to the States (42 per cent now and progressively more) the specifics of threats to national and internal security are being overlooked. The Centre cannot retract totally when the very basis of the Naxal issue is lack of governance at the state level. If States want lead role in everything how is it they are recalcitrant in implementing Schedules 5 and 9 of the Constitution seriously to ameliorate some of the grievances of the Naxalites? The undeniable truth is that the political-police-Naxal nexus at state level does exist, insurgency has become an industry and its continuation has obvious benefits. If a former Research and Analysis Wing officer says that the two foreigners abducted by Naxals was a stage-managed affair, the same is mentioned unofficially by police officers in the case of abduction of the DM of Malkangiri. How come none of the additional police stations sanctioned past so many years have not come up in areas devoid of rule of law? How come when the CAPFs went deep into unchartered Abujmarh forest, interacted with population and stayed there for one month, no move was made to establish posts or administrative units in even areas contiguous to existing posts? How come no illegal arms manufacturing unit has been discovered

in Bihar after the police caught 65 such facilities in only Munger District in December 2010?

The Centre palming off responsibility of the Naxal problem to the States is apparently because the MHA failed to create a set-up, a unified operational command set-up and preferred to remain in the background. This could have been done in conjunction with the CAPFs but instead unaccountability was preferred. The negatives can be seen with the Home Minister's recent call to define a new counter-Naxal policy – what have we been doing all these years? The CAPFs get thrown around like penny packets by the States. While the Naxals have well planned perception management policy, the MHA has no set-up to deal with this, leave aside a proactive policy to deal with such an important issue. Similarly, in a problem like this, it is a unified operational set-up under the MHA that should have evolved comprehensive intelligence acquisition plans, as well as psychological operations (psy-ops) plan, both of which need to be dynamic and reviewed periodically.

Police In Counter-terrorism

Force 1 was raised as a Special Police Force in Maharashtra within one year of the 26/11 Mumbai terrorist strike. It is well equipped with imported weaponry and it is manned by well-motivated locals. Yet, the unit is not permitted to generate their own intelligence even within Mumbai and surrounding areas, which they are quite capable of executing being located at Mumbai. The intelligence is supposed to come from the local police which is a rarity because the local police only go to the black and grey areas when the political masters so permit. Force 1 has hardly been used and never trained in conjunction with the NSG, leave aside MARCOS who too are located in Mumbai and may get employed in a future 26/11 type situation. Force 1 has no active operational experience and a system to send subunits by rotation to the Naxal belt to gain such experience does not exist. This is but one example.

CAPFs In Counter-insurgency

In a written reply to a question raised in *Rajya Sabha* recently, the MoS (Home) revealed that presently, a total number of 593 companies of CAPFs have been deployed in 10 Naxal affected states for assisting the State police in conducting anti-Naxal operations and that presently, there is no proposal with the government to reduce/decrease the number of battalions of CAPFs in the LWE affected states, thus reducing the expenditure on their deployment. Actually, the CRPF has the lead role for counter-insurgency operations with some 145 of the total 343 CRPF battalions deployed in the Naxal belt at any one time. Chhattisgarh has some 45 CAPF units at any time, 90 per cent CRPF, because of active Naxal movement in large areas. During the last elections in the state, the CAPFs strength was boosted to some 135 battalions.

Command And Control

Looking at the counter-insurgency models in the Northeast, J&K and Naxal affected states; all have Unified Headquarters at state level, as well as Unified Operational Command. The glaring difference, however, is that in the Naxal affected States, the operational command is headed by the DGP of the state (with the CRPF, BSF, ITBP and all other forces placed under him) who is subservient to the Chief Minister and takes clearance from the latter for every operation. The Chief Minister has his own constraints with his MLAs (some if not all) elected and in power because of Naxal support. So security of operations is suspect especially in case of the few proactive operations that require time for planning and execution. The recent call by the Home Minister to post DMs and SPs with zeal in the Naxal belt was perhaps in this context. Contrast this with the operational commands in the Northeast and J&K where operations are conducted without reference to, leave aside permission of, the political authority of the state though the Chief Minister can be kept informed periodically, as deemed fit. Interestingly, the MP from one of the Naxal affected states had disclosed that the DGP of the State was paying protection money to Naxals for his own safety. Even today this is happening at various levels, as mentioned by CAPF officers unofficially. The CAPFs, particularly the CRPF and BSF rue that they are being governed at the higher echelons by IPS officers who have little experience of counter-insurgency and yet they are planning operations for them, of which they have no clue. Take the largest massacre of 76 CRPF personnel that happened in April 2010 just because a senior though green IPS officer landed up as SP, Raipur and ordered the CRPF to just get out for 72 hours to dominate the area without any intelligence and without any objective in mind. The IPS lobby has ensured negligible Additional Director General level posts pan India for the CRPF, BSF and ITBP despite the very large strength of the CAPFs. Former CRPF officers cite this as a major reason for the poor state of manning, equipping and employment of the CRPF. This is an area that merits serious attention by the government. If the main counter-insurgency force is CRPF, they must have their own officers. More importantly, the single point unified command up the chain must have career specialists to plan and execute strategies and policies.

Organisation

When the CRPF has been chosen as the primary counter-insurgency police force, the focus should go beyond routine deployment of units for law and order in peace areas to the Naxal belt for counter-insurgency operations and vice versa. In the Naxal belt, the state must synergise operations – simultaneous operations – at the socio-political, moral and physical planes. Military operations are not the key, the centre of gravity is the population and hence population is the objective. Security forces need to fight at the moral and physical levels combining operations with development. The CRPF, BSF and ITBP deployed in the Naxal belt all have different organisation structures. However,

CRPF being the main counter-insurgency force has to take a call on reorganising itself. The decision has to be by the force itself but we have the successful counter-insurgency models in the Rashtriya Rifles and Assam Rifles to take a cue from. It would be prudent to at least reorganise 200 of the 343 CRPF battalions into a specialised counter-insurgency force. The new organisational structure must also cater for intelligence acquisition, psychological operations and capacity for surgical strikes, as also dog handling capacity.

Equipping

From the photographs appearing from time to time of the encounter sites, it appears that the modernisation of the CAPFs is far from what is desired. They do not even have adequate bulletproof jackets and helmets, leave aside weapons etc. It is imperative that the CAPFs be equipped with: adequate firepower including sniper rifles; day and night surveillance equipment; night fighting capability; modern communications; survival equipment for counter-insurgency environment; personal protection equipment; adequate mobility; IED and explosive handling equipment and; direction finding and interception equipment.

Training

The syllabus laid down at the Counter-insurgency and Anti-terrorism (CIAT) Schools for the police forces is adequate where all units going to the Naxal belt are supposed to undergo three months of training. However, the bottom line is that no unit or subunit should be inducted without pre-induction training. This would also require maintaining adequate forces as reserves that have undergone such pre-induction training to meet emergent requirements of rushing additional CAPFs to the area when required.

Technology

It is ironic that we have still not commenced on the NCTC which we should have had in place a decade back. There is no reason why we cannot address reservations of the states on its possible misuse. If we do not start the process now, we are likely to land up with the NATGRID as an underutilised highway in absence of the NCTC. Our endeavour should be that we must simultaneously progress the NATGRID, NCTC and state level SCTCs in conjunction with Digital India. Additionally, as the Army is moving ahead to acquire the battlefield management system, we plan similarly for the security sector. An initiative taken now will still take some 10-15 years to fructify fully.

With the instability surrounding India, inimical forces out to destabilise and problems of unemployment and poverty, insurgencies and terrorism are unlikely to vanish in the foreseeable future. It is therefore essential that we focus more on the threats to internal security. The Police and the CAPFs are vital to dealing with such threats. We must reorganise, equip, train and employ these forces in the best possible manner. **DSA**

The IPS lobby has ensured negligible ADG level posts pan India for the CAPFs

Military operations are not the key, the centre of gravity is the population

VEHICLE THEFTS IN INDIA

HI-TECH APPROACH TO CUT DOWN THE MENACE

During evening patrolling or night rounds if police officers come across any person who is not carrying documents along with vehicle, they just make use of this app to know if the vehicle is stolen or not. It has resulted in recovery of number of stolen vehicles.

As per 2013 data, about 1.84 crore vehicles are sold in a year in India. For the same year National Crime Record Bureau data says that 1,67,838 vehicles were stolen in entire country. It comes to around one per cent. Only 23 per cent of stolen vehicles were recovered by police in year 2013. Remaining 77 per cent undetected vehicles land up in stolen vehicle market. Also there is no mechanism to monitor if the recovered vehicles from thieves have reached the owner or not. Mostly these recovered vehicles lie in police station premises for eternity. An article dated 28.09.2014 by the *Sunday Standard*, a publication of Indian Express group claims that vehicles worth Rs 400 crore are lying in police stations of New Delhi.

Unfortunately answer to all the above questions is "NO".

But it is no more applicable to Karnataka Police which has come up with a new approach to deal with menace of vehicle theft as well as menace of unclaimed vehicles lying in the police stations forever.

Unclaimed vehicles with lots of dust and rust on them are a common sight in police station premises throughout India. These vehicles can be classified into four groups:

1. Vehicles involved in crime and seized by police.
2. Vehicles involved in accident cases and seized by police.
3. Stolen vehicles recovered by police from thieves.
4. Vehicles abandoned by thieves or by drunkards.



Before the project



After the project

It can be good pointer to condition of remaining police stations in the country. This issue has been addressed by Karnataka Police with the help of a software and an android based application. This article shows a way how the databases of vehicles can be used to dispose the vehicles lying unclaimed in the police stations and also how on the spot police can check if the vehicle is stolen or not.

State Of Stolen Vehicles

- Is FIR registered in all vehicle theft cases?
- If all the stolen vehicles are recovered by police?
- Are all recovered stolen vehicles returned to the owners?
- Is there any mechanism to monitor that owners get back their vehicles?
- Can Indian Police tell on the spot if the vehicle is stolen or not?
- Can SHO of any police station in India tell how many vehicles are lying in the police station premises?

Many vehicles that are involved in crime and accident are not claimed back by owners because they do not have legitimate documents to prove their ownership. Often these vehicles are stolen vehicles which are purchased without any documentation and at very cheap rates.

Stolen vehicles that have been recovered by police from thieves also lie in police stations. After recovery of vehicles, officers often take less interest to know whether those vehicles are returned to the owner or not. Secondly the procedure to know the owner of vehicle is that one has to send the details of the vehicles to RTO and he in turn will send the RC book details. But often this process takes lots of time and many times the vehicle must have been brought and sold by three to four owners without updating the RC book. So it becomes difficult to track the last owner.

Mandya Experiment In Karnataka

A project was implemented in Mandya District of Karnataka for disposal of unclaimed vehicles in the

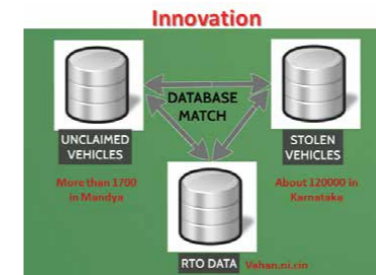
police stations. In 30 police stations of Mandya District there were more than 1,800 unclaimed vehicles. Three databases were used in this project to trace the unclaimed vehicle to its owner.

A) Data of Unclaimed Vehicles lying in police stations which includes information like registration number, engine number, chassis number, make and model of the vehicle.

B) Data of all the stolen vehicles of Karnataka State. This data was taken from a programme of National Crime Record Bureau called Motor Vehicle Verification Counter that is available in each district SP office of Karnataka.

C) Data of all registered vehicles in all RTOs across India. This data was accessed by getting username and password of the website: www.vahan.nic.in

A software was developed with the help of three students of Computer Engineering Department of PES Engineering College, Mandya. In this software first two databases were matched for common value and we got result in format showing that the XYZ vehicle



was stolen in which police station and it is lying unclaimed in which police station. For vehicles for which FIR could not be traced, the owner was traced with the help of website www.vahan.nic.in

Swachh Bharat Model

The results were an eye opener. Vehicle stolen in one of the Police station limits of Mandya District was lying unclaimed in another police station of same Mandya district for years. Similarly many vehicles stolen in neighbouring districts have been found lying unclaimed in Mandya District police stations.

Once the FIR is traced or the owner is traced the disposal of vehicles is done by returning the vehicle to the owner. If owner has claimed the vehicle insurance then the vehicle is returned to the insurance company and if both of them refuse to take the vehicle then it is auctioned. This way Mandya Police has disposed 786 vehicles and soon they will cross the mark of 1,000 vehicles. Thus owners get back their vehicle, police station premises get cleaner and police earn goodwill of the public. It is win-win situation for everybody. It can also be considered as honest contribution by police department to "Swachh Bharat Mission".

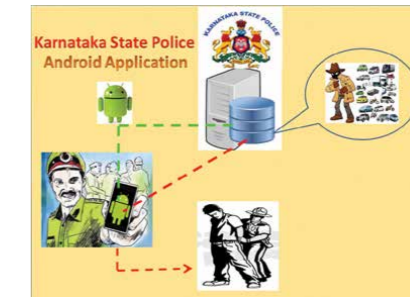
Mandya District Police won National Award for E-Governance on 30.01.2015 in Category of Best District Level Initiative in Citizen Centric Services through use of Information and communication Technology for this work.

Very soon this project is expected to be integrated with Karnataka Police Intranet called "Police IT". New addition will be that the owner will also get intimation through SMS as soon as the stolen vehicle is traced in any police station.

Insta-awareness

Taking the project ahead, Mysore District Police developed an Android based application in which

the stolen vehicle data of Karnataka state is stored in a server. Whenever an entry of any vehicle registration number, chassis number or engine number is made in this app, it checks in the server and reply is generated telling if the vehicle is stolen or not. This app is used by police officers of Mysore and Mandya districts. During evening patrolling or night rounds if these officers come across any person who is not carrying documents along with vehicle, they just make use of this app to know if the vehicle is stolen or not. It has resulted in recovery of number of stolen vehicles.



This app is expected to be used by Karnataka Police all over the state very soon. It has two advantages. It empowers the officer in the field to check on the spot if the vehicle is stolen or not. Once it gets a wide publicity, it will directly affect the demand supply equation of the stolen vehicles. If people know that police can check the vehicle on the spot, the demand for stolen vehicles will come down and thus it will result in less number of vehicle thefts.

Counter-tamper Tech

In case of above mentioned scenario, thieves may then try to tamper the chassis number and engine number of the vehicle. To tackle this problem Mandya Police in collaboration with PES Engineering College is in process of making an electronic device that can tell if the engine number or chassis number is genuine or not. This electronic device will have database of all the chassis number digits and engine number digits of all motor vehicles manufacturers in terms of digit size, shape, font and distance for comparison purpose.

Thus this project is a holistic approach to deal with menace of vehicle theft and the menace of unclaimed vehicles lying in the police stations. This project has full potential to be replicated in entire country. Let's do it.



Bijay Kumar Singh IPS

The writer is Inspector General of Police, Southern Range, Mysore.



Bhushan G Borase IPS

The co-writer is Superintendent of Police, Mandya District, Karnataka.



Abhinav A Khare IPS

The co-writer is Superintendent of Police, Mysore District, Karnataka.

new initiative

DSA DIALOGUE

IDEAS THAT UNITE!

An initiative of DSA

Mission: Vasudhaiva Kutumbakam: To endeavour to create "one world – one family"
Maha Upanishad Chapter 6, Verse 72

Vision: To offer a global interactive platform for dialogue, debate and discussion to avoid confusion, contention and conflict for a safe and secure world of peace, harmony and prosperity.

The appreciation and applause received from the readers of Defence and Security Alert magazine from around the world have inspired the conception of "DSA Dialogue", an online interactive platform with the objective to develop a community which influences change and is value packed with analyses on paradigm shifts in defence, security, safety, surveillance and international relations. We envision *DSA Dialogue* as the most sought after forum for the defence, police and paramilitary forces, coast guards, intelligence agencies, corporates, think tanks, defence and security industry, airlines, hotels, critical infrastructure and establishments in India and around the world. *DSA Dialogue* is a daily pulpit to share your knowledge by discussing topics which resonate with global scenarios in defence, security and international relations.

DSA DIALOGUE Focus Areas

- > Airlines
- > Banking and insurance
- > Border security
- > Corruption
- > Cyber terrorism
- > Cyber security
- > Defence budget
- > Defence forces
- > Defence industry
- > Defence policies
- > Drugs and human trafficking
- > Education
- > Environment
- > Entrepreneurship
- > Finance
- > Food
- > Fundamentalism and jihad
- > Future textiles
- > Geopolitics
- > Geostrategy
- > Healthcare
- > Hospitality industry
- > Intelligence
- > Insurgency
- > Internal security
- > Infrastructure
- > Plants and establishments
- > International relations
- > Innovation
- > Science and technology
- > Laws and policy
- > Maritime security
- > Military affairs
- > Migration
- > Money laundering
- > NATO
- > Naxalism
- > Politics
- > Police reforms
- > SCO
- > Security budget
- > Security and development
- > Security forces
- > Security industry
- > Social and political discord
- > Terrorism
- > Others

We invite experts and analysts from the entire spectrum of 'defence', 'security' and 'international relations' to initiate enthusiastic conversations and discussions that generate new ideas, unlock hidden insights, create an engrossing outlet of thoughts and make a difference for creating a more aware, safe and secure world for all of us and our coming generations. *DSA Dialogue* is a great way to get feedback on an idea that you want to develop further. Having a different view and some constructive criticism is invaluable in building a global recognition for your novel idea or unique perspective.

To know more please visit: www.dsalert.org and start the dialogue now!

get connected

DSA™

DEFENCE AND SECURITY ALERT

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



Subscribe Now!

You Pay

TENURE	COVER PRICE	DISCOUNTED PRICE	SHIPPING CHARGES			
			INDIA	DELHI / NCR	REST OF INDIA	DELHI / NCR
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**TM Online

www.dsalert.org

Online Subscription

One Year

US\$ 30

Two Years

US\$ 35

Three Years

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**



DSATM

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, adv@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