

# National Security Challenges



***“ATMANIRBHAR BHARAT SE HI ATMANIRBHAYA BHARAT”***

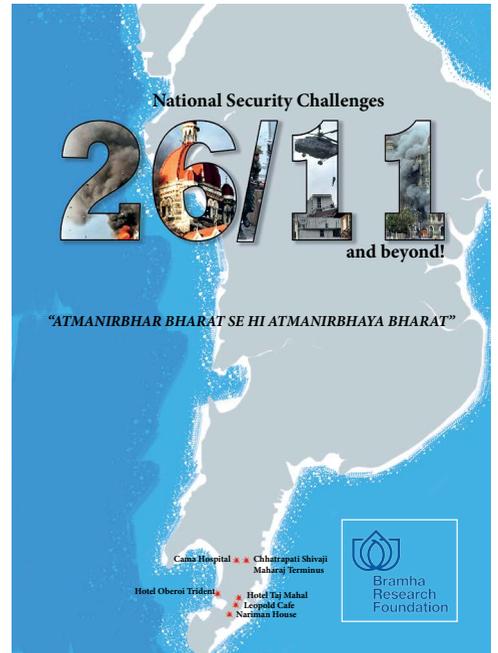
Cama Hospital \* \* Chhatrapati Shivaji  
Maharaj Terminus

Hotel Oberoi Trident \* \* Hotel Taj Mahal  
\* \* Leopold Cafe  
\* \* Nariman House



**Bramha  
Research  
Foundation**





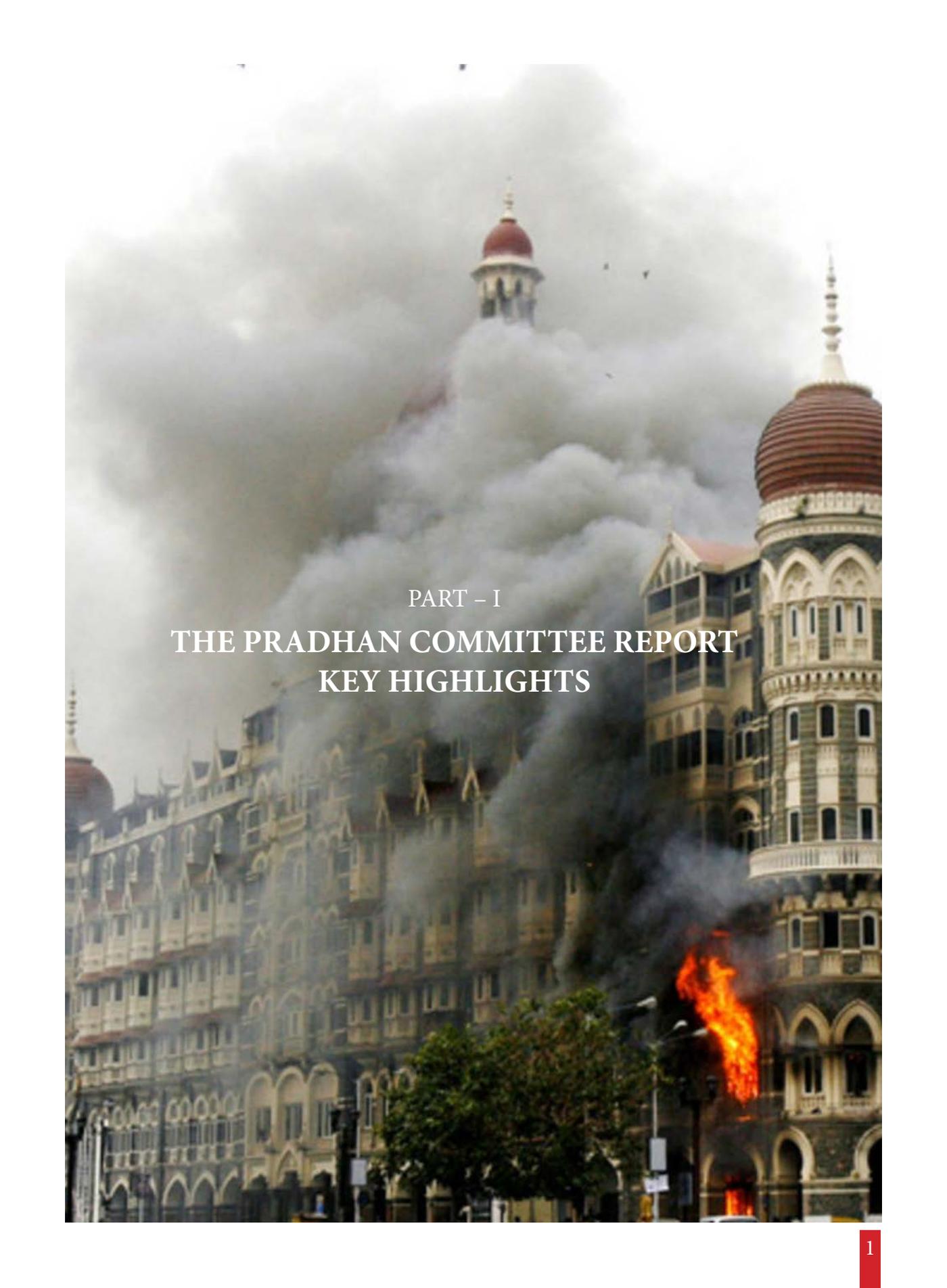
# National Security Challenges – 26/11 and beyond!

“ATMANIRBHAR BHARAT SE HI ATMANIRBHAYA BHARAT”

Published on : 26/11/2021

Presented by  
Bramha Research Foundation





PART – I  
THE PRADHAN COMMITTEE REPORT  
KEY HIGHLIGHTS

### PRELUDE

The 2008 Mumbai attacks that occurred on 26/11/2008 were a series of terrorist attacks that took place in November 2008, when 10 members of Lashkar-e-Taiba, an Islamist terrorist organization from Pakistan, carried out 12 coordinated shooting and bombing attacks lasting four days across Mumbai. The attacks, which drew widespread global condemnation, began on Wednesday, 26 November and lasted until Saturday, 29 November, 2008. A total of 175 people died, including nine attackers, and more than 300 were wounded.

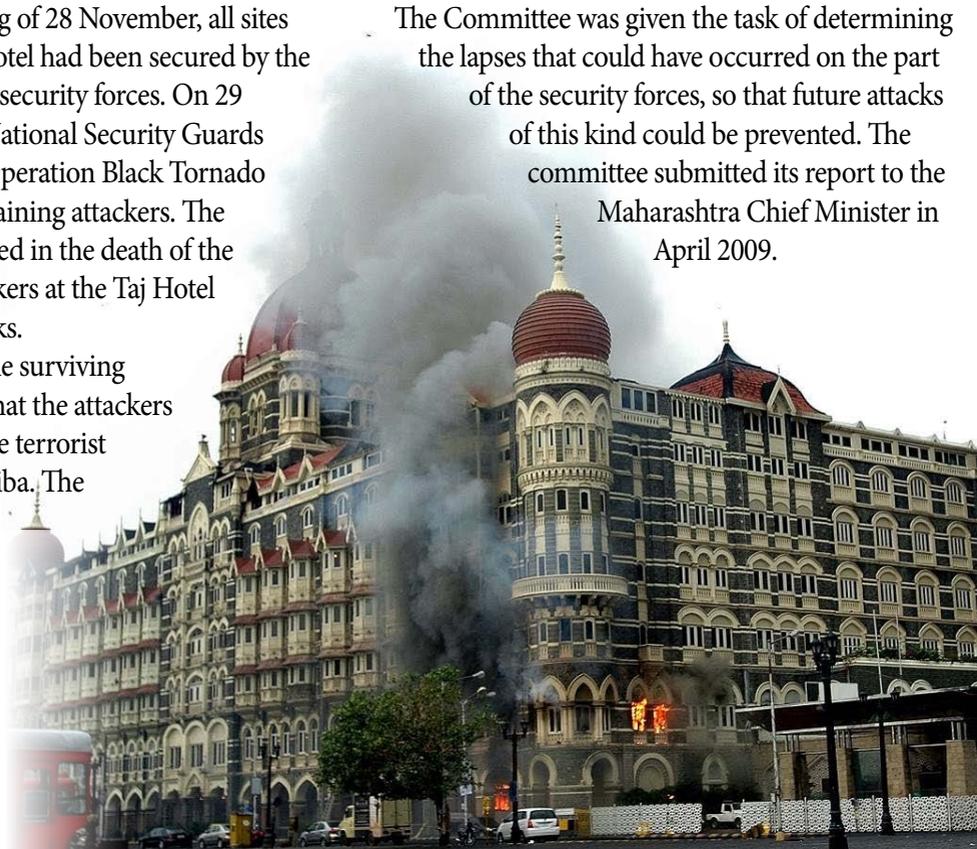
Eight of the attacks occurred in South Mumbai - Chhatrapati Shivaji Terminus, Oberoi Trident, Taj Palace & Tower, Leopold Cafe, Cama Hospital, Nariman House, Metro Cinema, and in a lane behind the Times of India building and St. Xavier's College. There was also an explosion at Mazgaon, in Mumbai's port area, and in a taxi at Vile Parle. By the early morning of 28 November, all sites except for the Taj Hotel had been secured by the Mumbai Police and security forces. On 29 November, India's National Security Guards (NSG) conducted Operation Black Tornado to flush out the remaining attackers. The Operation culminated in the death of the last remaining attackers at the Taj Hotel and ended the attacks.

Ajmal Kasab, the sole surviving attacker, disclosed that the attackers were members of the terrorist group Lashkar-e-Taiba. The Government of India stated that the attackers came from

Pakistan, and their controllers were in Pakistan. Later, Pakistan confirmed that the sole surviving perpetrator of the attacks was a Pakistani citizen. On 9 April 2015, the foremost ringleader of the attacks, Zakiur Rehman Lakhvi, was released on bail and went off the radar. He was arrested again in Lahore on January 2, 2021. In 2018, former Pakistani Prime Minister, Nawaz Sharif suggested that the Pakistani government played a key role in the 2008 Mumbai attack.

On December 30, 2008, the Maharashtra government appointed a two-member High-Level Enquiry Committee, also known as the Pradhan Inquiry Commission to probe the security forces' response to the 26/11 Mumbai terror attacks. The committee comprised former home secretary, Ram Pradhan and former IPS officer, Vappala Balachandran.

The Committee was given the task of determining the lapses that could have occurred on the part of the security forces, so that future attacks of this kind could be prevented. The committee submitted its report to the Maharashtra Chief Minister in April 2009.



## **Findings**

The Committee did not find any serious lapses in the conduct of any individual officer. What they have found are instances of lack of: intelligent appreciation of threats, handling of intelligence, maintaining high degree of efficiency in instruments specifically set up to deal with terrorist attacks and certainly lack of overt and visible leadership in carrying out operations to face multi-targeted attacks. In fact the last factor has led to public anger and resentment, both against the political as well as the administrative establishments.

## **Intelligence**

There were several intelligence reports beginning 7th August, 2006 indicating that LeT was making preparations to infiltrate Fidayeen (Commando terrorists) into India by sea route. There was however no specific intelligence that sea-borne terrorists would hit Hotel Taj or Oberoi.

## **Nodal Officer needed**

The Committee was told that under the “Desk Officer” system, even intelligence alerts received from Ministry of Home Affairs (MHA) are directly received and processed by the concerned Desk officer instead of the Addl. Chief Secretary (Home) directly receiving and handling these sensitive communications. For the Committee, this was a shocking revelation! The Committee recommended that an experienced officer has to be designated as a Nodal Officer by the Home Department for Maharashtra State to handle intelligence connected with terrorism. The Committee recommends that Commissioner, State Intelligence Department (SID) should be the nodal point, since he is in charge of all intelligence.

## **Clothing and Equipment**

Many of the police mobile vehicles were equipped with only riot gear of lathis, gas guns and .303 rifles which were no match to the superior fire power of the terrorists who

carried AK-47 assault rifles, pistols, hand grenades, bags of 8 kg of RDX, sophisticated cell phone with headphone, commando wear clothing etc.

The police lacked stealth tactics of commandos to counter terrorists. The terrorists were not only well trained but fully equipped to undertake war-like operations. They were adopting the usual commando tactics of “area clearing” by throwing grenades. Also, the Mumbai Police did not have adequate protective gear like bulletproof vests or anything that could withstand grenade attacks.

## **Inadequate training**

No actual simulated training in facing terrorist attacks and hostage rescue was given at Manesar. Since September 27, 2007 no firing practice was done due to shortage of practice ammunition.

## **Lack of Leadership**

According to the Committee, Quick Reaction Team (QRT) without on-the-spot leadership cannot be an effective instrument. Present ATS chief (Addl. DGP, Railways) who took charge after Shri Karkare’s death told the Committee that he had individually questioned QRT men on what went wrong? They told him that there was no one who could lead them in Taj and also at Oberoi where they had gone up to the ninth floor.

## **Poor tactics**

Like in the case of Heritage Taj, the terrorists positioned themselves on higher floor of the “Atrium” so as to cause maximum damage to the police. And this made it impossible for the police to cross the vast “Atrium”. Moreover, the RDX bomb placed adjacent to Oberoi lobby exploded at 22:30 hours and caused much damage, igniting fires and making it impossible for anyone to carry out any assault.

Since the police were no match to the terrorists in fire power, they had to retreat.

### **Lack in flow of information**

From then on, the officers in the Control Room (C/R) could not closely track the movements of the terrorists or police teams in their pursuit, because the attack was taking place in sequence and senior officers present on the spot could not keep the C/ R informed of their tactical plans.

### **Lack of training and casual response to attacks by Police**

The Committee enquiries also showed that the Mumbai Police were not given regular firing practices. It appears to the Committee that in general, the Mumbai Police initially responded to multi-targeted attacks efficiently, but in a manner that they usually respond to in a law and order situation.

### **Performance of QRT teams below par**

According to Shri A. N. Roy, ex-DGP, Maharashtra, initially one QRT team could have been marshalled in 10 minutes, while others could have been brought in within 40 minutes. However, he felt that QRTs were not used for the purpose they were created for and were split into small groups/ units. The organizational structure and training curriculum of QRT was totally inadequate. To begin with, it was wrong to split QRT units into 1-12 which is too big for such type of assaults. An ideal assault unit should not be more than 1-5.

The Committee after a study of the control room logs found out that QRT teams were summoned at different locations as an emergency strike force (based on situations assessed by local commanders). That is how they got themselves divided into various small groups which went against the basic principle of commando teams which work

as composite units with their own command and control. QRT lost its punch because of this.

### **Lack of centralized Command Centre**

The Committee is of the view that during such a crisis, such as the one Mumbai faced, the Commissioner of Police should have been at the Command Centre in the Control Room which might have helped in preventing duplication of efforts by different police units. If each top officer, such as the CP or the DGP treats SOPs in cavalier manner, then there is no point in setting SOPs. In fact, the Committee with long standing experience of its members finds that in our administrative system, individual officers have increasingly taken liberty with established procedures.

### **Lack of collaboration between Civil and Police authorities**

The Taj and Oberoi management did not implement certain important security advice given by DCP Zone-1 during the security audit visits.

### **No Joint action with Coast Guards**

Despite receiving as many as six alerts about the sea route likely to be used by terrorists, no significant steps had been taken by the State Government to beef up coastal security by having regular interaction with the Coast Guards. It was well known that the patch work joint patrolling that started from 1993 had not worked. Nothing other than convening meetings seems to have been achieved as evident from the information given by the DGP Maharashtra.

### **Shortage of Ammunition and Equipment**

Availability of arms and ammunition for Maharashtra Police is a serious problem. It was already mentioned that QRT could not

do any firing since September 2007 due to shortage of ammunition, although they are subject to firing practice every fourth day, according to DGP Sri A N Roy. “We were shown a bullet proof jacket of 1993 vintage, weighing about 10/12 kg. How can anyone resist terrorists with such heavy weight on one’s shoulders?” Agility with which the terrorists moved about and operated their weapons holds many lessons. Mumbai/ Maharashtra Police must be provided equipment and means to challenge any attacks in future.

### **ACTION AREAS**

1. Continual awareness and sensitizing the public on the threat perception to the city and soft targets in particular. This is because people have a tendency to forget and get lulled into complacency.
2. Improved coordination between the Police, Civil Administration and Security Forces (when called for) during the conduct of Operations. Command Centre to be created and situation to be monitored by a high ranking Officer at all times.
3. Intelligence needs to be kept at very high level at all times, and the agencies need to be alert 24x7 so as to thwart ingress of any anti-national elements into the city and its environs.
4. Flow of information to be continuous and clear for smooth conduct of Operations.
5. Continuous training of Police and Security forces at all times. Special QRT Teams to be kept earmarked trained and provided adequate weapons and equipment to allow them to carry out their tasks effectively.
6. The procurement of weapons and equipment should not have any bottlenecks

as they are vital for security of our country.

7. The media should not be allowed to be involved too much into conduct of operations as it may result in intelligence falling into the hands of the enemy and also might create panic among the general public.

### **Profile of Col Venkat Raman**



#### **(Retd.)**

25 years of service in the Indian Army as an Officer in the Corps of Engineers, Col Venkat Raman has served in various positions -

technical, supervisory and managerial. A well-educated and talented personality, with a high degree of administrative, analytical and technical knowledge as well as excellent communication skills, who has the ability to lead and administer efficiently almost any team to perfection. Having a Master’s Degree in Business Administration (MBA) from Anna University Chennai in 2001, he went on to get a Master’s Degree in Psychology from the University of Madras (ICE) in 1998. Col Raman was also awarded the Army Commander Eastern Command (Army commander’s) Commendation Card in 1983 for exemplary service beyond the call of duty while constructing fortifications in high altitude areas in Sikkim while on active service. He has also written several articles for technical journals like Indian Road Congress Seminar proceedings in 1996, Institution of Engineers (India) Seminar proceedings 1998 and Indian Road Congress Seminar Proceedings in 2003 on Civil Engineering subjects.

## References

1. Article in the Wire (online version); <https://thewire.in/security/26-11-mumbai-terror-attack-inquiry-committee>
2. Article in The Hindu dated 21 December 2019 <https://www.thehindu.com/news/national/other-states/Pradhan-Committee-finds-serious-lapses-on-Gafoorrsquos-part/article16854533.ece>
3. ORF Special Report December 2018 [file:///D:/d%20%20data/BACKUP19042016/Strategic%20think%20tank/ORF\\_Special\\_Report\\_77.pdf](file:///D:/d%20%20data/BACKUP19042016/Strategic%20think%20tank/ORF_Special_Report_77.pdf)
4. Article in Hindustan Times dated 22 November 2021 <https://www.hindustantimes.com/india-news/26-11-attacks-anniversary-need-to-assume-that-it-can-happen-again-says-former-home-secretary/story-DTVIvZk-fX7hao0cUTTmHAO.html>



PART – II  
**TRANSFORMING MUMBAI POLICE TO  
MEET FUTURE CHALLENGES**





## TRANSFORMING MUMBAI POLICE TO MEET FUTURE CHALLENGES

While preparing a megapolis like Mumbai for a war like 26/11/2008 one has to undertake a 360-degree view and look for multiple angles from where the attack could emerge. The danger could be from land, air or water... Mumbai has all such openings and this makes the task of the CP much more difficult.

1 Firstly, I wanted to boost the morale of the police force who had lost 16 brave hearts, including ATS chief Shri. Hemant Karkare, Addl. CP Ashok Kamte, inspector Vijay Salaskar and 13 others who showed exemplary courage and made the supreme sacrifice of laying down their lives for the protection of our motherland.

2 Second and important task was to get the bulletproof (BP) jackets for the policemen in case there was another attack... I requested the MCHI to buy a specific quality of BP jackets and donate to Mumbai police! We got 500 pieces of BP jackets for the commandos.

3 We had to train the commandos and then newly formed QRT men. We selected 1500 brave men and trained them with the help of Israeli commando trainers. I personally met the Israel police chief who readily agreed to spare the trainers free of cost. These 1500 men equipped with all the newly purchased arms and ammunition were made available in five different regional control rooms in the city to tackle multiple incidents (in case the need arises).

4 We bought 40 fully bulletproof marksman vehicles and parked them in 40 vantage points in the city. So, they could reach any

area in the city within minutes. The vehicle was equipped with commandos and all other necessary equipment to tackle any given situation.

5 All modern firearms were purchased from US, Germany and Israel to equip the commandos. Thirteen sets of bomb disposal squad equipment was also added to our capacity.

6 We bought seven firearms simulators for the policemen to do firing practice as to sharpen their skills.

7 We gave necessary land to the NSG unit to be located right in the middle of the city so that they could be deployed at short notice. During the Mumbai attack they took 26 hours to reach the city.

8 We created our own NSG equivalent force called "Force One". They have been fully trained and are as capable as the NSG commandos today.

9 We created 30 modern gymnasiums for the policemen. These gyms have state-of-the-art equipment and is funded by policemen itself.

10 The 110-year old police hospital was completely revamped with an investment of about Rs 3.5 crores.

11 The main police control room, which is the nerve centre of city police ops, was modernised at the cost of 4 crore.

12 Over 43000 men and women of Mumbai Police were medically examined free of

cost to categorise them as per their medical fitness.

The Central and State Government helped buy bulletproof boats for the marine police to patrol the sea coast. In fact, marine police stations were also built on the coastline.

We organised a number of training programs for the policemen and also built a Prerna Training Centre for the Mumbai police.

We organised couple of anti-terrorism seminars which were addressed by Shri Abdul Kalam, MK Narayanan, KPS Gill, Julio Ribeiro and various other experts. Each session was attended by over 1200 citizens and top policemen.

We created a Marathi in house magazine called “Samvad” for communicating effectively with the 50000 policemen and women. The magazine also covered separate sections for policemen on how to lead a healthy life and what to eat and what not!

A private magazine called “the Protector “was started to communicate with the people as to latest happenings in the police system.

We built a “Martyrs” memorial /monument for the 18 martyrs, including the NSG officers right on the marine drive. The whole project was funded by people of Mumbai.

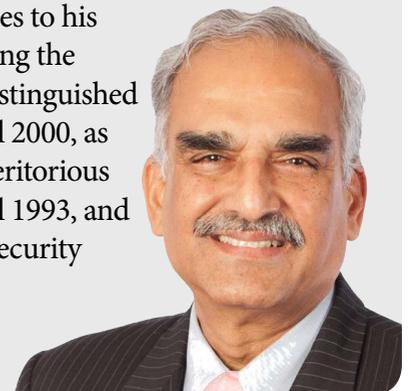
Many other govt initiatives were done to get the Mumbai city up and going. All these were done in 2009, and now I am sure many scientifically superior things have been deployed for the protection of Mumbaikars.

## **Profile of Mr. D. Sivanandhan**

One of the most highly regarded IPS officers in India, with an illustrious career spanning several postings during his 35 years of service, Mr. D. Sivanandhan has dedicated his life to the eradication of corruption and organised crime and is renowned for his use of strategy and intelligence to uphold the rule of law. During his tenure, he raised resources to upgrade the police force capabilities and welfare in the form of the latest law enforcement equipment, hospitals, gymnasiums, schools, and other facilities.

His professional career spans from being the Director General of Police, Maharashtra State in March 2011, to serving as Commissioner of Police, Mumbai after the 26/11 attacks and was responsible for building up a world-class anti-terrorism mechanism. Six years in the Mumbai Crime Branch as Additional Commissioner of Police – Crime and Joint Commissioner of Police – Crime (1993-1995 and 1998-2001), he is credited with having broken the back of the underworld that was at its peak. Most recently, he has been a member of the special task force in the National Security Council Secretariat (Prime Minister’s Office) for revamping India’s internal and external national security.

In his tenure, Mr. Sivanandhan has been many accolades to his name, including the President’s Distinguished Service Medal 2000, as well as the Meritorious Service Medal 1993, and the Internal Security Medal 1998.





**PART - III**  
**CBRN THREATS TO NATIONAL SECURITY**



Day One. Dawn of another bright day, week away from Diwali. Pune, the city of the retired and of the happening young professional is awakening to another busy day. Sweet stalls and shopping malls are all spruced up for the festival shopping. At mid-day, a team of plumbers are repairing a major water pipeline in the Kothrud area of Pune. At an eatery, a woman is quietly garnishing sweetmeats with an odd-looking liquid.

Day Seven. Today is Dhanteras, an auspicious shopping day for most Indians. An inconspicuous worker at a renowned hospital is spraying disinfectant in the lobby, corridors and OPD area. Another cleaner is going about disinfecting and mopping railings and door handles in a famous Mall.

Day Eight. OPD department of a hospital in Pune. Two patients reported complaining of fever, backache and nausea; symptoms of what initially appear to be a viral infection. By afternoon, they show early-stage smallpox (a strain of Variola Virus, a deadly contagious biological agent). Desperate doctors administer antidotes, but the patients begin to die. Pune Municipal Corporation (PMC), health services and other hospitals/clinics are alerted. Similar reports are received from some hospitals and private clinics from other localities. However, it is closing time and most staff and officials are already away on a long Diwali weekend.

Some shoppers are testing Deodorant spray cans at a mall. By evening, some shoppers are complaining nausea and vomiting. Doctors diagnose these as food poisoning and cracker pollution. Similar incidents are reported by a number of malls across

the city. At 8 PM, a smart doctor-on-duty at a hospital identifies Sarin [a lethal nerve agent which can be dispersed by aerosol] poisoning among these cases. He alerts the already sensitized administration which takes immediate actions to notify all.

Day Nine. The city is awakening to a bright Diwali morning. Reports of the previous day's incidents have received small coverage on City page of some dailies; however, Diwali advertisements have gobbled up print space. The District Commissioner of Pune chairs an emergency meeting of health officials, emergency services, Police, Paramilitary and select NGOs. Key officials out of Pune for the long weekend have been recalled. All hospitals, health centers and clinics have been put on high alert. Appeals for mass immunizations are being announced on Radio and TV. Who cares? Its Diwali!

The above scenario (applicable to any city in India) is merely fictional but illustrative to highlight public lack of understanding and dearth of trained and aware staff and officials at various Government departments and other institutions, especially during festival holidays.

### Introduction

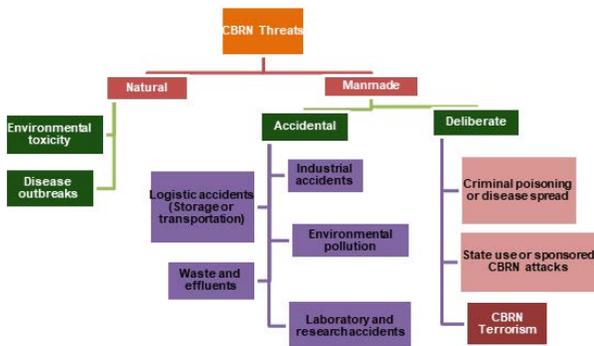
The Mumbai terror attacks of November 26, 2008, have left a deep scar not just on the residents of Mumbai but also on the security fraternity in India as a whole. The multi-pronged attacks were well synchronized and aimed for causing maximum destruction and casualties. Yet in some ways they were pretty conventional. Imagine if these were coupled with a chemical or radiological release which would have caused huge losses

not just in human casualties but also in terms of business, economy, social fabric disruption and emotional degradation.

Chemical, Biological, Radiological and Nuclear (CBRN) security is a matter of grave concern for many nations today. CBRN security in India is still in its early stages. While the Armed Forces are well prepared for CBRN defence, it is the hinterland that is of concern. There is a need to look at CBRN threats from a broader perspective of internal and regional security challenges that manifest in many forms including CBRN terrorism. The current Covid19 global pandemic has highlighted many issues – procedural, healthcare, legal, economic, and social. The paranoia created and panic generated by a CBRN incident shall have many repercussions and leave many lessons.

### CBRN Threat Spectrum

CBRN emergencies occur as a result of occupational exposure, fire, explosion, release of toxicants, and warfare, and are caused either by ignorance, negligence, incompetence, accident, or malicious intention. Such incidents would result in a larger population in a state of panic and fear, affecting their health and morale. The impact is multipronged - physical, psychological, economic, and social. CBRN threats can be natural or manmade. It is the Manmade threats that are of concern and need to be addressed.



National CBRN security is still evolving in India. Issues like poverty, illiteracy, lack of adequate healthcare, ignorance of/disregard to safety measures and lax enforcement increase our vulnerability to looming CBRN threats. Covid19 was coming at us since Nov 2019. Our efforts in keeping low death count and being proactively ahead of the possible spike in casualties, have been essentially responsive to evolving crisis. While we were lauded for the strict lockdown and management of early Covid19 effects, it highlighted many shortcomings in long term sustainable mitigation measures. It has been seen as a health issue and not a National security one. It is time India woke up to the idea of National CBRN security and prepared for the same.

The recent drone attacks in Jammu with conventional explosives and drone weapon drops should be a wakeup call of dire portents. Toxic chemical sprays or aerosolised dissemination of lethal pathogen by such drones can wreak havoc in our border areas and hinterland. Are we to wait for such an occurrence to ‘react’ and take counter measures? Can we not foresee or anticipate the emerging threat patterns and prepare ourselves in advance to prevent or counter them?

### Recent CBRN Incidents

Apart from the ongoing Covid19 pandemic, one of the largest CBRN incidents, there have been many incidents that seek attention. The gruesome Bhopal gas tragedy of 02-03 December 1984 had shaken the world. There are numerous instances of CBRN incidents in India and abroad. Some recent examples are as under:

- 1) Styrene Gas Leak at LG Polymers Vizag on 07 May 2020. The sudden release of Styrene in the early hours of the morning led to many people getting affected. The incident resulted in eleven dead and hundreds affected by the toxic gas. All

within the first hour or so.

b) Boiler explosion at UPL Plant Bharuch on 23 Feb 2021. A massive fire/explosion in the solvent that led to two workers dead and 28 injured.

c) A laboratory conducting unauthorized research on Nipah Virus was closed by the Government in February 2020. The US CDC appeared to have helped an under-qualified Indian laboratory to work on the Nipah virus, a pathogen that is considered a potential bio-weapon.

d) In May and Jul 2020, there have been boiler blasts at thermal power station in Neyveli, Tamil Nadu, claiming at least 14 lives and injuring many more.

e) The Mayapuri, New Delhi radiation (Cobalt 60) leak on 08 Apr 2010 is a stark reminder of careless disposal of radiation sources.

f) There have been instances of Radioactive material seized from scrap yards and persons with dubious distinctions, albeit in small quantities, in various parts of the country.

g) In Nov 2020, a tanker carrying 50 tons of Sulphuric acid met with an accident and overturned on the NH48 near Vadodara, spilling nearly four tons of the acid. Fumes from the acid made rescue and recovery difficult.

h) Ten people died and many injured when a gas tanker carrying highly inflammable gas Butadiene had an accident with a bus and exploded near Jaipur-Delhi Highway at Beelpur village in Jaipur district in Dec 2014.

In a survey carried out by the IndustriALL Global Union, in about 116 industrial accidents in chemical and mining industries across the country, about 231 workers were killed and many more injured between May 2020 and June 2021. Financially, State Bank of India research estimated a contraction of over 40% in the GDP in Q1 FY21. For the states, the total loss due to COVID-19 is estimated at 13.5% of the total Gross state domestic product. Socially, huge

loss of lives, livelihood, family structures and an overall disruption of social fabric was the result of one, just one virus spread.

### **CBRN Terrorism**

Terrorists may resort to the use of CBRN agents to generate widespread panic, which could bring down a democratic government, or to establish a position of strength from which to negotiate their demands. The Tokyo nerve gas attack by the Japanese cult group, Aum Shinrikyo, on 20 March 1995, had set a precedent in the use of CBRN weapons by terrorists. The Anthrax cases in the US, the use of Mustard gas, Chlorine and Sarin in the Syrian conflict, and radiation scare across the EU are other examples. It is but a matter of time when India will be faced with a CBRN terrorist incident.

With the empowerment of citizens, rising aspirations and easy availability of dual-use technology, we are witnessing the emergence of the 'techno'-terrorist, who may resort to CBRN Terrorism. Several incidents in 2017 and 2018 showed increasing use of sophisticated chemical agents to carry out assassinations or assassination attempts. In February 2017, Kim Jong Nam, the half-brother of North Korea's leader Kim Jong Un, was assassinated at the Kuala Lumpur airport with the nerve agent VX. On 4 March 2018, the Soviet era nerve agent Novichok was used in the poisoning of Sergey Skripal and his daughter Yulia in the UK. This was followed by yet another use of Novichok used by Russia against Alexie Navalny, the Russian opposition leader in 2020. It requires a frank and serious study about threats and their prevention, vulnerability assessment and how we are preparing to manage the consequences of such an incident in India.

As a result of the programme for de-nuclearisation in the former states of the Soviet Union, there are about 500 metric tons of

U-235 and 300 tons of Pu-239 from dismantled weapons that have to be disposed. To add to it are the “Suitcase Bombs” many of which are rumoured to be missing. A virtual ‘nuclear black market’ has come up in the Central Asian Republics (CAR) region raising fears of terrorists acquiring Improvised Nuclear Devices (IND). Technological partnerships may exist among rogue nations and groups with proliferation of weapons grade fissile material.

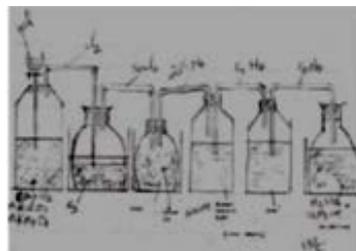
A radiological weapon, on the other hand, disperses radiological material by means of conventional explosions, causing radioactive contamination. Such weapons are called Radiological Dispersal Devices (RDD) or “Dirty Bombs”. These could be dispersible or just spreading radioactivity. The arrest of Dhiren Bharot for seeking to make an RDD in the UK, is an example. The deliberate use of radioactive isotopes to cause deaths (like the Litvenko Polonium poisoning case) or accidents (like the Mayapuri incident of Delhi, involving Cobalt-60), are wakeup calls for us, Indians. Cesium, Polonium, Cobalt and other radioactive isotopes, some common in medical equipment and industrial gauges, are potential weapon ingredients.

Biological agents like toxins (Botulinum, Ricin) or live pathogens (anthrax, cholera, plague) are more potent than chemical agents, since they attack cells and multiply in their victims. Apart from high toxicity and delayed detectability by traditional sensors, these agents can be made from lab samples and stolen material. COVID-19, SARS and Ebola are live examples of the dangers of a viral spread. A number of laboratories in the world are working on such lethal pathogen samples and cultures of deadly biological agents with a view to develop vaccines and drugs. Terror groups are said to have set up lab facilities to work on and weaponize such pathogens.

The availability of Chemical agents or their ingredients is widespread. They are easy to produce even in a home lab by trained chemists, especially in a country having a vast industrial base like India, China or even Pakistan. The availability of toxic dual-purpose Chemical like Chlorine, Phosgene Hydrogen Cyanide, Ammonium Nitrate and many other Toxic Industrial Chemicals (TICs), makes the task of a Chemical terrorist easy.



*Terrorist groups have experimented with using agricultural spray by aircraft for dissemination of Biological agents like Anthrax*



*Documents found in Afghanistan indicate Al Qaeda's interest in production of Chemical agents like Sulphur Mustard, Sarin and VX*

Right from the days of the Sarin attack by Aum Shinrikyo in Japan (1995) or the Novichok poisoning of Navalny (2020), CBRN terror has been in our midst. While there have been innumerable hoaxes and mere threats of use of CBRN material, the number of actual cases is frightening. Research shows that likelihood of Chemical agents being used by terrorists is the highest. A comparative likelihood matrix of CBRN weapons used by terrorists is given below:

	Chemical	Biological	Radiological	Nuclear
Production	Easily available precursors	Agent seed stocks accessible	Costly. Not easily acquired. Unaccounted Fissile / radioactive material	Very difficult. Cost prohibitive. Large infrastructure
Weaponization	Simple	Met sensitive	Unsafe	Highly technical
Control/Contagious	Controlled	Not Controlled	Not Controlled	Not Controlled
Delivery	Liquid, Aerosol, Gas	Food, Water, Air	Multiple means, IEDs	Missiles, Aircraft, Artillery
Time to effect	Immediate	Incubation or manifestation period	Prolonged	Immediate and highly prolonged
Likelihood	Most likely	Likely	Less Likely	Least likely

## The Motivation

A review of the potential implications of CBRN and past incidents would indicate why such means appeal to terrorists.

- a) Sophisticated CBRN agents are potentially highly lethal while being silent killers, and therefore, harder to detect and contain – deniability/responsibility.
- b) Capability of inflicting mass casualties based on limited ability to quickly identify and/or contain the effects of such substances.
- c) Any attack using CBRN material would attract attention and receive prime-time coverage in the mass media - provoke terror, paranoia and panic among civilians and administrators.



*May-August 2016: Intern Doctors of Al Shabaab cadre converting animal Anthrax into transportable spore cultures at County hospitals – Kenya, Uganda & Ethiopia*

d) CBRN materials have the potential to inflict serious consequences and collateral economic damage (e.g. by contaminating the environment, disrupting normal life and businesses and affecting animal and human health).

e) CBRN materials offer the means to blackmail governments or at least pressurise them.

f) Possession and use of CBRN means would place the perpetrator in a position of perceived power vis-à-vis national authorities (at least temporarily).

## Terrorist Capabilities

Terrorist technological capabilities are rapidly increasing. They are no longer the illiterate cannon fodder. The risk factors of these dangerous weapons falling into indiscriminate hands include access to CBRN materials outside of government control in conflict zones, abuse of poor inventory systems in troubled territories and the threat of insiders' access in sensitive facilities, perhaps facilitated by corruption. The fragmentation of terrorist groups, the loss of authority, the creation of disparate cells or the facilitation of dangerous individuals could inspire lone wolf terrorists using alternate means of violence. Societal changes can increase vulnerabilities and facilitate enhancement of terrorist capabilities



*The assassination of Kim Jong-nam with VX nerve agent at Kuala Lumpur airport*



*The Tokyo Sarin attacks by Aum Shinrikyo 20 Mar 1995*

in the following areas:

- a) Organizational Capabilities
- b) Logistical Resources
- c) Financial Resources
- d) Knowledge/Skill Acquisition
- e) Materials and Technology Acquisition
- f) Initial Production and Weaponization of Agent

Communications technologies and the growing use of e-commerce also facilitate access to relevant scientific information and newer technologies, which allows for higher damage at lower costs with fewer knowledge prerequisites. In the future, CBRN agents may be more attractive to radicalised individuals.

### **Threat Manifestation**

CBRN Terrorist threats may manifest in any of the following forms. It just takes an innovative mind to think up many more possibilities.

- a) Attacks on / or sabotage of critical infrastructure, nuclear plant, chemical factory or biological research establishment with a view to cause large-scale damage, release of toxic material and increasing fatalities.
- b) Dirty Bombs using radiological / chemical material.
- c) Covert exposure / release of Radiological sources or toxic Chemicals (vapours and spills) in sensitive urban areas / heavily populated areas.
- d) Create widespread fear by use by poisoning induced through food, water, letters and other routinely handled equipment.
- e) Deliberate inappropriate disposal of toxic waste to cause casualties

Use of CBRN materials by terrorists is no longer just a storyline from fiction novels. They are a horrifying possibility and reality. Underlying this challenge is the fact, that few professed doctrine or strategies exist to guide the administration and other agencies

about how to control the health, water, shelter and other consequences of the use of CBRN weapons on large civilian populations in various parts of the country.

Incident Management Paradigm Essentials  
Domestic crisis prevention and response is the responsibility of the Government; in particular the Min of Home Affairs. Consequence management, by contrast, describes ways and means to alleviate the short- and long-term physical, socio-economic, and psychological effects of a CBRN attack. It describes the coordination of international, national, regional, and local assets to deal with the effects of such an attack. The term includes preparatory work in response to a CBRN threat that would include site surveys; securing critical infrastructure; strengthening border controls and domestic proliferation prevention measures; assessment of the ability of Local Hospitals/ Primary Health Clinics/Private Clinics to treat or decontaminate victims; the industrial capability to maintain supply of essentials in spite of surge demands, and the status of various antidotes.

Thereafter, should intelligence and police agencies be unable to prevent the incident, immediate crisis management must hit the road running. Counter terror agencies, special teams, industrial onsite response all need to focus on escalation prevention and casualty minimisation. All stakeholders need to be suitable trained and equipped for CBRN incidents.

Consequence management would include isolation/quarantine of the affected group/community/locality, treatment of victims within a contaminated zone, their decontamination and evacuation, and local clean-up. It would also involve psychological

treatment and other efforts to restore confidence in the social and economic well-being of the affected area and of the country itself. The essence of the issue being immediate response.

There is a stark contrast between nuclear, radiological, chemical and biological scenarios. While nuclear weapons cause untold deaths and devastation, their use by terrorists is not as yet a possibility. Radiological weapons (Dirty Bombs) however are. Nevertheless, size and explosion impact may keep the contamination largely localized. Chemical and Biological agents, the poor man's atom bomb, can be delivered covertly through various means like aerosol sprays, contaminated food or water and by contact infections.

After a chemical attack, there is a "golden hour" within which is the maximum effect. Beyond that hour, those who are going to survive, do and those who are not, do not. Once decontaminated, administered immediate first aid and removed from the incident site/"Ground Zero"/"Hot Zone," victims can be evacuated to different hospitals. These are essentially non contagious and spread can thus be contained. It is the other way round in the case of Biological agent victims. There is an incubation period of a week or so after transmission of infection. After onset and discovery, the victims must be immediately isolated in order to prevent the agent from spreading. Potential victims need to be isolated from the definitely uncontaminated public; they also should be isolated from others afflicted with the illness until each individual's degree of contamination can be established. But this type of mass quarantine is presently difficult. Given today's detection capabilities and the incubation period of

biological agents, we'll never know that we've been contaminated till symptoms emerge. Hence the diabolical genius of a biological agent attack: "we become the (unknowing) vector of our own death."

It is no secret that we are not adequately prepared. However, much planning is underway, funds are being made available, and the Government is beginning to study the threat and its consequences. There are many areas of concern. Detection capabilities are limited, integrated analytical and planning efforts are proclaimed but not fully understood, especially by administrative hierarchy, various stakeholder agencies and departments. Most importantly, there is need for clarity of how all related response agencies in any part of India function post the attack in relation to the requirement and to one another. Sadly, in keeping with the American experience of 9/11, it may take an incident to focus assets and responsibility for effective planning and preparation.

The government's interest lies in educating the public and encouraging citizen involvement. A paradigm shift in the outlook of the Government to such threats is essential. This has to be pre-event. Any government official who thinks he can adequately inform or educate the public during a CBRN incident will be preaching to the morgue.

### **International Initiatives**

The world is seized of the threats posed by CBRN materials. The UN has passed the 1540 and 1673 Security Council resolutions against CBRN Terrorism. The UNODA and UNICRI have a CBRN Prevention programme. Then there are the Biological Weapons Convention (BWC 1972) and the Chemical Weapons Convention (CWC 1993).

There are many agreements and conventions for prevention of nuclear and radiological proliferation. The International Atomic Energy Agency (IAEA), the INTERPOL, WHO and the World Customs Organisation (WCO) have their own CBRN programmes. The WCO especially has the Container Control Programme to monitor strategic trade and dual use goods trade. In addition, there are many regional (EU, AU, ASEAN, among others) and bilateral groupings controlling environmental hazards (Rotterdam, Stockholm and Basel conventions) and the proliferation of dual use goods.

**Indian CBRN Security Paradigm: Need for Comprehensive National CBRN Security**  
India needs an effective strategy to mitigate CBRN risks of criminal, accidental or natural origin that requires a very high level of co-operation and co-ordination both between different national agencies as well as among Countries and International and Regional Organizations. Lack of harmonization of national preparedness and fragmentation of responsibilities can reduce effectiveness of prevention strategies and cause delay in response during a crisis. The aim of a National CBRN Security Strategy is to protect India (and Indians) by taking all possible measures to prevent, mitigate and respond effectively to a potential CBRN incident.

Existing international and national security strategies acknowledge the importance of developing a comprehensive approach but, tend to have an isolated approach perpetuated by the divisional structuring of chemical, biological, nuclear or radiological sectors. The CBRN issue is often fragmented – with each sector studied in isolation. It is more pronounced in India due to the size of the country, climate differences,

decentralized security structure, varied technological development, massive industrialization, cultural diversity and population variance. Such fragmentation is potentially counterproductive because no single organization possesses all necessary resources, expertise and statutory power to address all possible aspects of the CBRN problem.

The importance of a CBRN incident gets diluted as none of the agencies presently mandated to look at CBRN issues see it from a National Security perspective. It is necessary to develop a comprehensive National CBRN Security Strategy to be able to adequately address all aspects of prevention, protection and response.

#### Present Structure and Mechanism

On 23 December 2005, the Government of India enacted the Disaster Management Act 2005 (DM Act), which established the National Disaster Management Authority (NDMA), headed by the Prime Minister, and the State Disaster Management Authorities (SDMAs) supervised by respective Chief Ministers, to spearhead and implement a holistic and integrated approach to Disaster Management.

The NDMA is mandated to deal with all types of disasters, natural and man-made (including CBRN disasters). Whereas, other such emergencies including those requiring close involvement of the security forces and/or intelligence agencies such as terrorism, insurgency, law and order situation, serial bomb blasts, hijacking, air accidents, mine disasters, ports and harbour emergencies, forest fires, oil field fires, and oil spills will continue to be handled by the extant mechanism i.e., National Crisis Management Committee. The Government of India has

earmarked nodal ministries for CBRN disasters and incidents as under:

- (a) Biological Disasters - Ministry of Health and Family Welfare
- (b) Chemical Disasters - Ministry of Environment, Forests & Climate Change
- (c) Radiological and Nuclear Disasters - Atomic Energy Commission

CBRN as a domain has remained with the DRDO and the Armed Forces till late nineties. While the expertise of both these are world class in CBRN defence, it has not percolated in the desired extent to internal security agencies. Research and development in private sector are not encouraged as the DRDO is keen to retain these critical and sensitive technologies. A new CBRN product by a private industry needs DRDO backing/approval to be accepted even for internal security. While I agree testing of CBRN products is done by the DRDO, new technologies or items different from DRDO's homegrown technologies should be acceptable so long as they meet the stringent qualitative requirements of the users.

### **Government Initiatives for Responding to CBRN Incidents**

The Indian Government has given reasonable thought to disaster management aspects relating to CBRN threats and instituted a number of measures: -

- (a) Enunciated standard operating procedures (SOPs) to deal with terrorist attacks involving CBRN Weapons right down to District and Municipal levels.
- (b) Earmarked twelve battalions of the Police (CRPF, CISF, BSF, ITBP and SSB) as the National Disaster Response Force (NDRF). Four more have been sanctioned by the Government. NDRF Battalions

are nominated first responders for CBRN disaster/terrorist strikes. One team of 45 personnel from each Battalion is to be specifically trained and equipped for response during CBRN emergencies. (Presently four teams are trained and equipped).

(c) States have been asked to raise their own State Disaster Response Force (SDRF) to be the First Responders at State level and augment the NDRF when so required.

(d) Set up 23 Radiation Emergency Response Centres (RERCs) in different parts of the country to deal with any nuclear and radiation emergencies.

(e) Established the Integrated Disease Surveillance Project (IDSP) in all districts under MoHFW.

(f) Radiation monitors are being installed at sea ports, air ports and border posts

Core trainers of these NDRF CBRN teams have been specially trained by the Indian Army at Faculty of CBRN Protection, College of Military Engineering (CME), Pune and various other CBRN establishments in India and abroad. Presently, most of the CBRN Training for Central Police Organisations (CPO) is conducted at National Industrial Security Academy (NISA) Hyderabad.

The NDMA has issued 22 Guidelines for various types of disasters (natural and manmade) and their management. These include CBRN related guidelines as under:

- (a) Guidelines for Nuclear attack disaster.
- (b) Guidelines on Chemical Disaster (Industrial)
- (c) Guidelines for Chemical Disaster (Terrorism)
- (d) Guidelines on Medical Preparedness and Mass Casualty Management

- (e) Guidelines for Biological Disaster
- (f) Guidelines for Psycho-Social Support
- (g) Guidelines for Incident Response System

### **CBRN Related Acts and Laws**

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 (BTWC 1972). Also, to the Convention on Prohibition of Development, Production, Stockpiling and Use of Chemical Weapons and on their Destruction (CWC 1993). India has also joined many protocols and agreements towards effective non-proliferation, CBRN counter terrorism, strategic trade control of dual use goods and hazardous waste management.

While there is no overarching law which covers CBRN as a whole and addresses all related aspects, there is a gamut of administrative, regulatory and legal arrangements obtaining in India which aid CBRN risk mitigation. These acts and laws complement the DM Act 2005, Weapons of Mass Destruction and their Delivery Systems (Prohibition of Unlawful Activities) Act, 2005 (The WMD Act 2005) and the Chemical Weapons Act 2000 towards effective CBRN Incident Management in India. In fact, India has a very elaborate coverage of legal instruments for all aspects of CBRN incident prevention, control, response and mitigation. I agree that some of these laws or acts may be archaic and need revision as per current situation and evolving technologies. Primary ministries and agencies that control these acts are:

- (a) Ministry of Environment, Forests and Climate Change (MoEF & CC)
- (b) Ministry of Health and Welfare

- (c) Ministry of Commerce and Industry
- (d) Ministry of Earth Sciences
- (e) Ministry of Mines
- (f) Ministry of Science and Technology
- (g) Ministry of Chemicals and Fertilizers
- (h) Department of Atomic Energy (DAE) & Atomic Energy Regulatory Board (AERB)
- (i) Department of Biotechnology (DBT)
- (j) Department of Revenue and Customs

Much work has been done in the field of Radiological and Nuclear safety and security. Even disease control is quite effective in India, given its size and population. However, India does not yet have a National Registry of Chemicals and has not completely implemented the Global Harmonised System (GHS) of Classification and Labelling of Chemicals. Chemical management is a grey area presently.

### **Recommendations for Comprehensive National CBRN Security**

The first question that is asked when we mention CBRN National security and risk mitigation is: Are we prepared? Listed below are the main areas that need attention towards optimal National CBRN security.

- (a) **Acceptance and Awareness** - The fundamental weakness is the lack of understanding (and belief) about the likely occurrence of CBRN incidents by policy makers and administrators. Municipal officials turn a blind eye to CBRN situations and a very cursory interest is shown by District and State administration, primarily due to lack of awareness. Awareness in private sector is dismal. Very few companies really follow best practices for CBRN material (Hazmat). Public awareness of CBRN threats, despite a year plus of Covid19, is superficial.

Civic CBRN risk mitigation awareness should be enhanced. Use of social media and street plays, mock drills and awareness campaigns by the NDRF are called for.

**(b) National CBRN Security Strategy and Plan** - CBRN issues are either looked as a military matter or a disaster issue and not as a National security concern. There is a need to have a clear National CBRN Security Strategy, aligned to and drawn from the National Security Strategy, to prevent, respond and mitigate CBRN threats. The National CBRN Security Strategy shall spell out desired objectives to be achieved by accountable stakeholders with broad timeframes. These objectives when matched with mapped existing capabilities and capacities shall draw out the gaps and shortcomings. Based on the same a multi stakeholder multi-faceted National CBRN plan can be developed.

**(c) CBRN Incident Management Structure** - The present mechanism is purely reactive with NDMA being the nodal agency for CBRN disaster management. CBRN issues must be looked at from a National Security perspective. NDMA is a Consequence Management agency. Crisis prevention is not in its focus. Further, its organization lacks a dedicated department to deal exclusively with CBRN incidents. The Covid19 crisis saw the Ministry of Health taking the lead with laboratories under the Ministry of Science and Technology assisting it. We are still talking of only Crisis Response and Consequence Management and not of Crisis Prevention, even for CBRN terrorism incidents. The present structure is grossly inadequate for effective CBRN prevention, preparedness and needs enhancement. Some recommendations are as under:

**(i) Crisis Prevention**

There needs to be clear understanding

of all aspects of CBRN crisis prevention. From international CBRN protocols, complimentary domestic legal provisions, border security (ports, airports and land borders), internal security to private enterprises. Proliferation control both international and domestic needs to be covered. In addition, sound CBRN intelligence is essential to allow timely intervention and crisis prevention. The job needs a federal control. It is recommended that the NIA under the Min of Home Affairs be restructured to take on this task. In fact, it should be beyond investigation. Ideally it should be restructured as National Internal Security Agency (NISA) aka Homeland Security.

**(ii) Immediate Crisis Management**

This would entail intervention to prevent escalation and minimize casualties. Counter terror agencies and special police forces form part of this. Also, agencies like customs, immigration, critical infrastructure security agencies (CISF and the like) would need to be grouped under this phase of operations. The NISA mentioned above is ideally suited to coordinate crisis prevention and immediate crisis management. All such stakeholders like special teams (NSG, Force One, Garuda, ATS and the like) local police, fire brigades, CISF, Civil Defence, medical rescue teams and onsite response teams at critical infrastructures must be adequately trained and equipped for immediate crisis response.

**(iii) Consequence Management**

This is already in place in the terms of the National Disaster Management Agency (NDMA). The NDMA presently lacks a dedicated section or branch for CBRN. This needs to be instituted with suitable trained staff. The NDRF Battalions have been earmarked for CBRN disaster management

and their equipping and training should be scaled up. Similarly, SDRF Battalions need to be equipped and trained for managing CBRN disasters.

**(d) Enforcement of Laws and Protocols**

- While we have some of the best laws, enforcement is weak and porous. India needs to strengthen its enforcement mechanism by strict oversight and rooting out of lax practices across ministries and agencies. Private Public partnership to enhance safety and imbibe global best practices is a must.

**(e) Proliferation Prevention and Border Control**

- We need to understand the role of Customs, Excise and Border security agencies in CBRN non-proliferation. These agencies have a major task of proliferation prevention and must be trained in detection, monitoring and interception of hazardous shipments, toxic threats, dual use goods and measures to respond to such threats. Across land, sea and air borders. It is recommended that due training and equipping of all stakeholders involved in this field be undertaken.

**(f) CBRN Security for Critical Infrastructure and High Visibility Events**

- This is an area of concern and needs to be carefully planned and executed. As of today, very little attention is paid to CBRN security of important Government buildings, critical infrastructure and also to high visibility events like sports extravaganzas, religious mega events and major public events. It is recommended that On-Site Response Teams be constituted for immediate CBRN response.

**(g) Zoning and Mapping** - Municipal areas, Industrial sectors and critical assets need to be risk mapped for CBRN threats. Toxic chemical hazards, laboratories, waste management and any other potential threat areas need to be mapped. Based on this

mapping, a vulnerability zone overlay needs to be added. Thereafter, a existing resource (response teams, police, fire brigade, hospitals, control HQs) map overlay be checked. This will enable us to know if our resources for response are optimally located in time and distance from the risk zones. Necessary relocation of resources may be undertaken.

**(h) Trade and Industry Oversight**

- Unrestricted trade in toxic materials, cost cutting measures, callous neglect of safety and security and corrupt practices lead to easy availability of large amounts of toxic materials and avoidable accidents. Ineffective implementation of legislations and regulations, pilferages and irresponsible dumping/disposal of toxic waste are serious concerns. Safety and security measures need to be imposed and regular practices and mock drills in liaison with District/Municipal authorities need to be planned. Organisations such as NACWC should be instituted for Biological & Toxin Weapons Convention. The R&N aspect is being adequately dealt by the DAE/AERB. The Indian Draft Chemicals (Management and Safety) Rules need to be enacted post haste and GHS be implemented strictly.

**(i) Response Mechanism** - Delayed execution of response protocols by various response agencies – Operational understanding, equipment woes (outdated and inadequate), grossly low footprint and transportation logistics. NDRF Battalions, the only ‘skilled CBRN responders’ also do not train for CBRN regularly and lack state of the art equipment. Other than the twelve teams of NDRF (actually four), very few agencies are trained to respond to a CBRN incident. SDRF Battalions are still a far cry from gaining counter CBRN

capability. All Critical Infrastructure, major SEZ and Industrial areas need to constitute on-site response mechanisms in terms of trained teams and appropriate equipping, sort of mutual-aid teams. There is a need to standardize such training so as to achieve right coordination and complementarity amongst various responders in a CBRN incident situation.

**(j) First Responder Training** - There is a dire need of basic CBRN training for the local Police and on-site response teams. Local police are a citizen's first responders for any crisis. Today the local police do not have even basic understanding of CBRN threats and immediate mitigation measures. Covid19 has been a stark reminder of this. Dr Manmohan Singh, then PM of India had said in Sep 2006, "Unless the beat constable is brought into the vortex of our counter-terrorist strategy, our capacity to pre-empt future attacks would be severely limited." More often than not, the local fire brigade may be called in for immediate CBRN response. It is imperative to train counter terror police teams, local police, CPOs and PMF and even private security agencies in CBRN threat understanding, prevention measures and immediate response/risk mitigation drills.

**(k) CBRN Security Culture** - The lack of awareness and complacency at Government and administration levels percolates to common citizen. There is a near zero understanding on basics of CBRN incident mitigation. The continued abysmal societal reaction to the current Covid19 crisis is a glaring example. In spite of a year and half of facing Covid19, even today, masks are not worn properly and there is disregard to vaccination and hygiene. The victims in a CBRN incident would be the society. The true first responders are the victims and people

immediately around them.

**(l) Community awareness programs, street plays, NGO initiatives to educate public awareness** - Interestingly, post 9/11, the Municipal Corporation of Greater Mumbai had issued a booklet on Dos and Don'ts during Chemical, Biological and Earthquake disasters. The booklet covers the threats expected and the simple means of mitigating these. Alas it never reached the administrators, leave alone the masses. Such booklets need to be prepared and widely disseminated much before a crisis erupts. The author has some experience in this regard.

**(m) Educate the population** - There is a dire need for the population at large to be educated on CBRN risks and threats and be ready to take small yet effective immediate mitigation steps. There is a serious need of developing a CBRN Security Culture amongst Government agencies and various stakeholder organisations. Medical Colleges do not teach CBRN casualty management. This needs a serious review. Basic CBRN risk mitigation should be included in High School and College curricula. A start has been made with a Post Graduate Diploma course on CBRN Protection and National Security at Department of Defence and Strategic Studies, Savitribai Phule Pune University (SPPU).

**(n) Embracing Emerging CBRN Technologies** - Emerging technologies are a force multiplier in preventing and effectively responding to a CBRN incident. The young generation needs to bring in newer technologies in the CBRN field to good use. Lack of indigenous testing kits and PPE during the early days of Covid19 crisis has raised concerns. Detection and protection are the basic requirements in a CBRN scenario. Use of robotics, drones,

unmanned ground vehicles and artificial intelligence need to be aptly integrated in existing prevention and response mechanics. There are some good CBRN industries making life saving equipment in India. We need to nurture these. FICCI, CII and Mahratta Chamber of Commerce, Industries and Agriculture (MCCIA) must encourage a Consortium of CBRN Industries to boost 'Make in India' CBRN products.

### **Conclusion**

The threat posed by CBRN terrorism is very relevant, driven by political, ideological, social, economic and technological factors. Preventing and countering CBRN attacks are particularly cumbersome and require considerable resources. To successfully discourage and punish such acts, the international cooperation framework must be strengthened and domestic capabilities, honed. Sound intelligence, focused proliferation prevention, punitive laws and regulations, and an effective sustainable response mechanism are the watchwords.

It is time we got serious about CBRN security. Growing industrialisation, increased imports of chemicals and machinery, coupled with lack of or non-stringent regulations on customs, safety and transportation of these leads to huge gaps in securing these assets. Waste management of toxic and hazardous substances is another key shortcoming. Awareness of CBRN threats and risk mitigation measures is necessary at all levels. There is an urgent need to educate and train all concerned stakeholders in CBRN risks and threats and the need to adopt risk mitigation measures.

It is imperative to develop an integrated CBRN approach that incorporates all international and national CBRN components

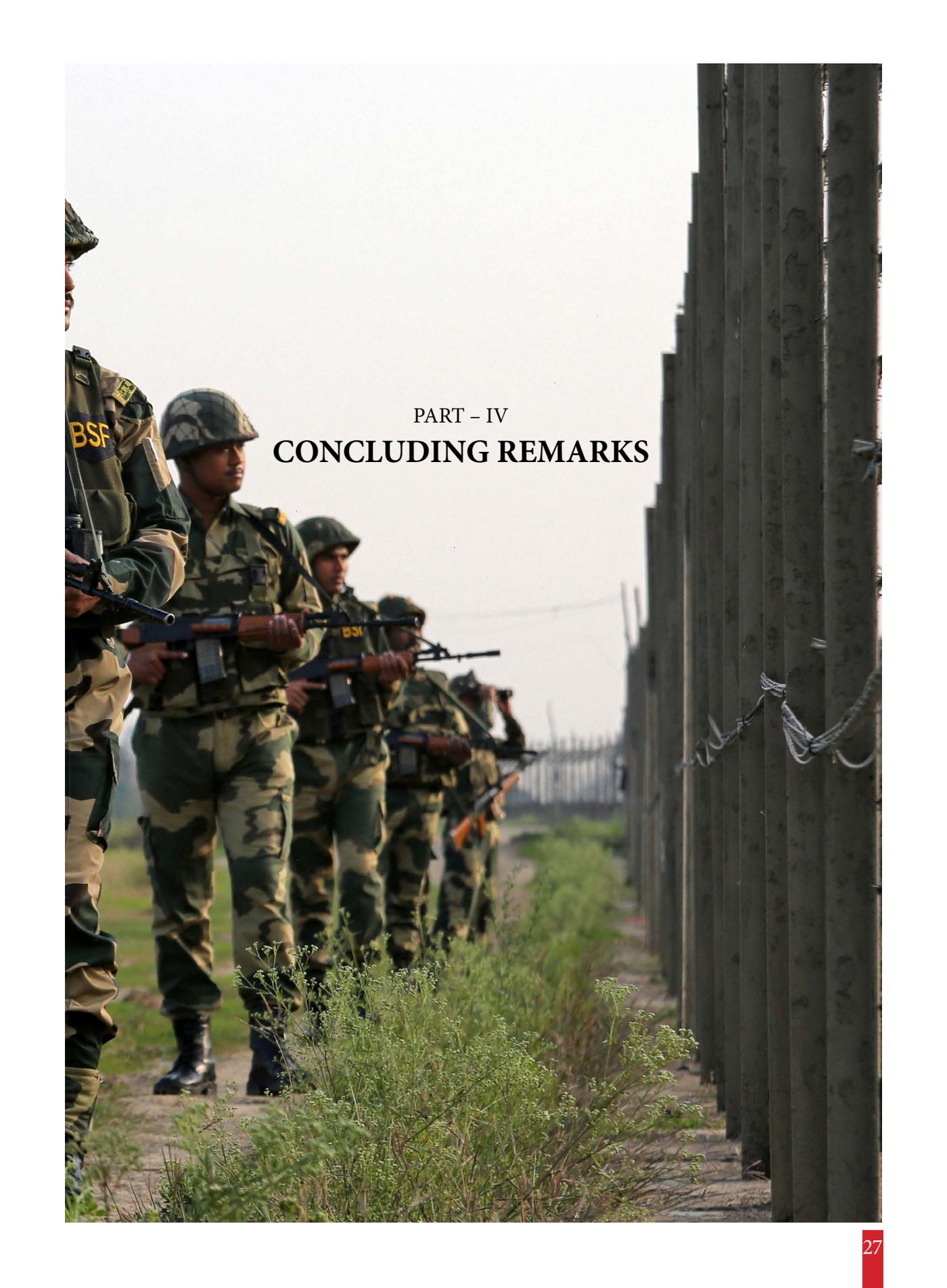
into a common CBRN Security strategy covering all aspects of Crisis Prevention, Crisis Response and Consequence Management. This entails the application of a holistic approach through which all stakeholders, while operating autonomously, can establish and realise common goals in a synergistic manner. Comprehensive CBRN Security while retaining domain specialisation can be achieved by the above approach and lead to optimal synergy in operationalising National CBRN Security.

*“Awareness and Preparedness is the Key to Survival.”*

### **Profile of Col Athavale**

Col Athavale has been a Key Adviser to the Government of India (MoD and MHA) on CBRN Security. He has been a key CBRN Expert for the EU CBRN Risk Mitigation Centres of Excellence initiative in Eastern and Central Africa. A visiting faculty at select Indian and overseas universities, prolific writer and a speaker in international seminars and conferences on CBRN subjects, he holds PhD in CBRN Security and Incident Management. He has authored a pioneering book titled “Toxic Portents” on ‘CBRN Incident Management in India’. Presently, he is a freelance CBRN Security and Risk Mitigation Consultant based at Pune, India.





PART - IV  
**CONCLUDING REMARKS**



## CONCLUDING REMARKS

“Man learns from history, that man doesn't learn anything from history.”

As we take a look back on the 13th anniversary of the 26/11 attack on the city of Mumbai, we have mixed feelings. On one hand, we have witnessed a substantial upgrading both in hardware and software critical for meeting internal and external security challenges both at the State and Central level. On the other hand, we find that the local Civil Administration and Police Machinery are better networked for handling crisis situations. Factors like housing the NSG sophisticated security establishments and substantial use and deployment of state-of-the-art digital technologies have given a sharper edge to the security apparatus to combat terror threats.

However, it is common experience that the crooked opportunistic enemies who surround us from all sides are always waiting to strike you when complacency steps in. Be it the LOC or LAC, despite sophisticated technologies deployed at the international borders intrusions and salami slicing are common phenomenon. Unfortunately, despite warnings and routine scenario building exercises, micro-gaps in the security set-ups are exploited by the enemies to our dis-advantage. Therefore it is critical to internalise the perpetual state of alertness seamlessly by the civilian, police as well as the masses. As stakeholders and guardians of the society one cannot underestimate Mazzini's call, “Eternal vigilance is the price of liberty.”

Translating this into the current scenario one feels that in terms of connectivity and multi-dimensional communication, we have 7x24 universal connectivity at our finger tips

and yet very often the corrective action and response are far too delayed to have any degree of control over the mishap. In the present times when conventional terror threats have been multiplied exponentially due to CRBN dimension, any such slippages could be suicidal and can have devastating impact on the society.

Summarily, one might say that at the national level with the Atmanirbhar Bharat initiative being forcefully launched is showing substantial impact in terms of high quality hardware and software tools, we have every reason to believe that now it is time for a paradigm shift from 'Atmanirbhar Bharat' to 'Atmanirbhaya Bharat' motivating and driving youth to positive results. What is crucial in this case is to ensure that while standard Police and Civil Defence routines are strictly adhered to, state of the art technologies like drones and CCTV camera networks are backed by highly efficient and responsive youthful teams deploying their AI/Robotic skills to achieve constant vigilance triggering appropriate and timely response. Apparently, there is no shortage of youth organisations both in the formal and informal sector. All that is required is to network and integrate these organisations seamlessly. And then, and then alone will the 'Atmanirbhar Bharat' Mission will help us achieve 'Atmanirbhaya Bharat'.

BRF gratefully acknowledges the kind help and guidance offered by Shri V.Balachandran IPS in person and in allowing references from his book “KEEPING INDIA SAFE – THE DILEMMA OF INTERNAL SECURITY”

**Prof. Vijay Page,**  
**Founder - Bramha Research Foundation**



**Bramha  
Research  
Foundation**

Bramha Research Foundation,  
Suite 501, S.G Raheja Auditorium, 24th and 32nd Road, Near  
Patwardhan Udyan, Off Linking Road, Bandra West, Mumbai. - 400050  
pagevijay@gmail.com Mob. 9324516410