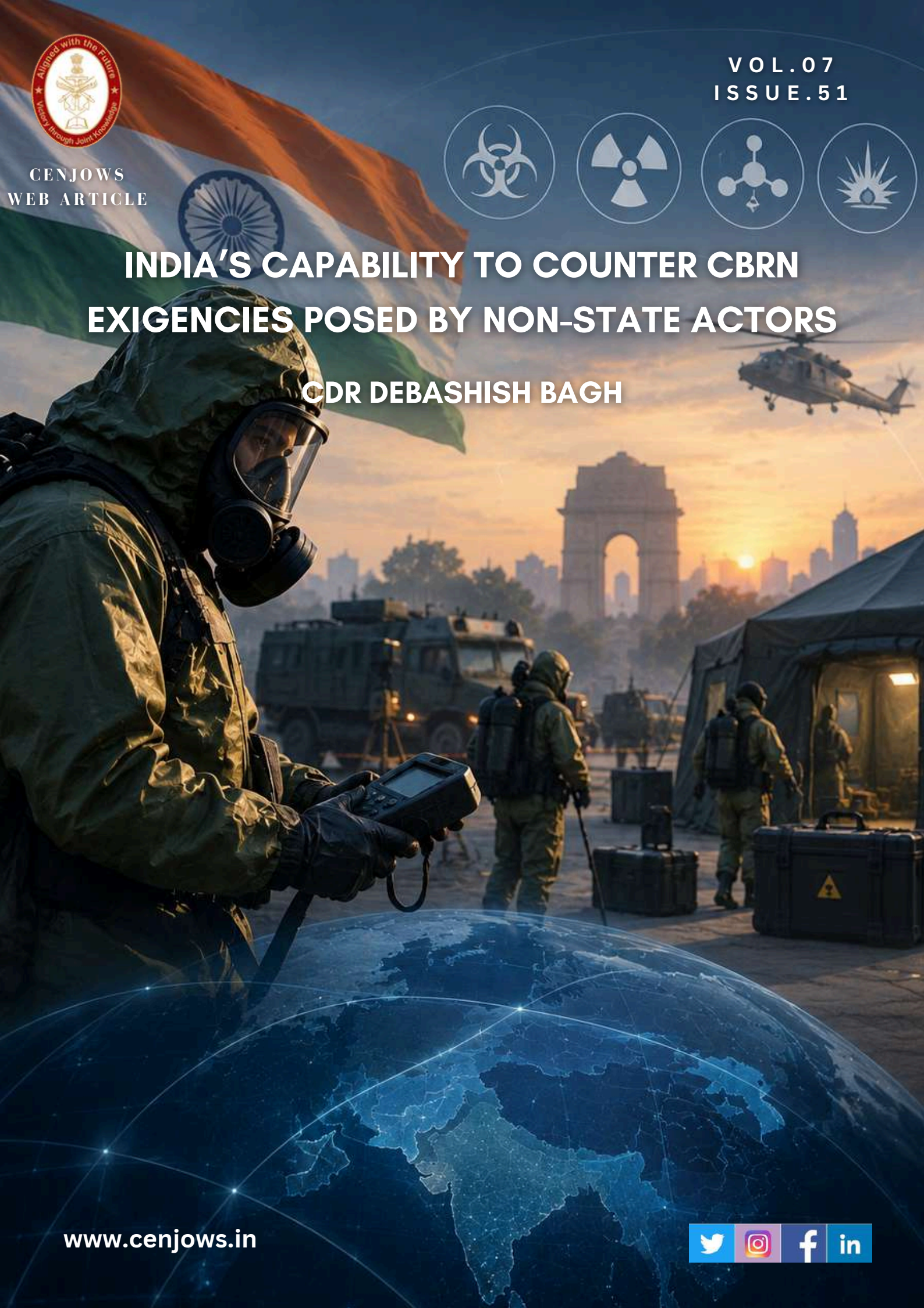
VOL.07
ISSUE.51

CENJOWS
WEB ARTICLE

INDIA'S CAPABILITY TO COUNTER CBRN EXIGENCIES POSED BY NON-STATE ACTORS

CDR DEBASHISH BAGH



www.cenjows.in

CENJOWS WEB ARTICLE

Volume 07 Issue 51 SEP 2026

CENJOWS
(Established: 2007)

Room No 301, B-2 Wing, 3rd Floor
Pt Deendayal Antyodaya Bhawan,
CGO Complex, Lodhi Road
New Delhi –110003 (INDIA)
Telephone Nos: 011-24364881, 24366485
Fax: 011-24366484
Website: www.cenjows.in
E-mail: cenjows@cenjows.in

ABOUT US

CENJOWS was raised in 2007 as an independent think tank, registered under the Societies Registration Act, 1860. This aims to promote Jointness as a synergistic enabler for the growth of Comprehensive National Power and provide alternatives in all dimensions of its applications through focused research and debate.

Starting Year : 2020

Year of Publication : 2026

Frequency : Weekly

Language : English

Publisher : Maj Gen (Dr) Ashok Kumar, VSM (Retd) Director General, CENJOWS
301, B-2 Wing, 3rd Floor
Pt. Deendayal Antyodaya Bhawan CGO Complex,
Lodhi Road
New Delhi-110003

Editor : Maj Gen (Dr) Ashok Kumar, VSM (Retd) (dg@cenjows.in)

Deputy Editor : Dr Ulupi Borah, Distinguished Fellow
(distinguishedfellow1@cenjows.in)

Editorial Board :

Brig K Ranjeev Singh, VSM (ddg@cenjows.in)

Col Ajay Kumar Rajak, SM
(secy@cenjows.in)

Gp Capt Ashish Kumar Gupta (Retd)
(seniorfellow2@cenjows.in)

Dr Ulupi Borah, Distinguished Fellow
(distinguishedfellow1@cenjows.in)

301, B-2 Wing, 3rd Floor
Pt. Deendayal Antyodaya Bhawan
CGO Complex, Lodhi Road
New Delhi-110003

Dr Monojit Das, Senior Fellow, PRO
(monojit.das@cenjows.in)

Publication Head : Ms Vaibhavi Katal

All correspondence may be addressed to:
Editor
Centre for Joint Warfare Studies (CENJOWS) 301, B-2 Wing, 3rd Floor
Pt Deendayal Antyodaya Bhawan CGO Complex,
Lodhi Road
New Delhi-110003
Telephone: (91-11) 24366485/Telefax: (91-11) 24366484 e-mails:
cenjows@cenjows.in / cenjows@yahoo.com Website: http://cenjows.in

Price: Rs 150/- INR

INDIA'S CAPABILITY TO COUNTER CBRN EXIGENCIES POSED BY NON-STATE ACTORS

CONTENTS

CENTRE FOR JOINT WARFARE STUDIES

CENJOWS

India’s Capability to Counter CBRN Exigencies Posed by Non-State Actors

Cdr Debashish Bagh is an Engineer Officer who is a qualified ‘instructor’ in CBRN.

Abstract

Non-state actors have already crossed the chemical weapons threshold. The 1995 Tokyo sarin attack proved the same. Radiological and nuclear material has also proven to be vulnerable to diversion outside state control; India's own 2010 Mayapuri incident proves this to be true. This article looks at India's capability to counter CBRN (Chemical, Biological, Radiological, and Nuclear) exigencies posed by non-state actors and argues that the real vulnerability is not a shortage of capability. It is the absence of a system that reliably brings that capability together when it is actually needed. India's disaster management architecture, built under the Disaster Management Act, 2005, does not even name CBRN as a category in its founding legislation. The National Disaster Response Force (NDRF), the Defence Research and Development Organisation (DRDO), the Atomic Energy Regulatory Board (AERB) and the Armed Forces each bring real and growing capabilities; however, they sit fragmented across separate chains of command, with no standing protocol linking them together. It concludes that closing India's CBRN preparedness gap

needs a dedicated CBRN doctrine, a standing civil-military protocol, and CBRN preparedness pushed down to the state and district level**.**

Key Words: CBRN Preparedness, Non-State Actors, NDRF, Civil-Military Coordination, Tactical Nuclear Weapons.

"I don't believe it is a question of if it will happen. It is a question of when."
- Deborah A. Wilber, Director, Office of Emergency Response, U.S. National Nuclear Security Administration

The Contemporary CBRN Threat Landscape

For the majority of the time during the 20th century, militaries prepared for CBRN threats largely on the assumption that only states could pose them. Chemical and biological weapons development required industrial-grade infrastructure, scientific acumen, and state protection to thrive. However, that was the notion. That assumption has not aged well.

The assumption ruptured on the morning of 20 Mar 1995, when members of the Japanese cult Aum Shinrikyo boarded three train lines of the Tokyo subway during rush hour and released Sarin, a military-grade nerve agent, killing 13 commuters and injuring roughly 5,500 more.[1] It was not the cult's first such attempt. Nine months earlier, the same group had killed eight people in a Sarin gas release in Matsumoto.[2] What made the Tokyo case different was the scale and intent, which was a non-state actor's execution of a coordinated chemical attack in a nation's capital, with no state sponsor behind it and no state protection to fall back on. A subsequent clinical review of the incident revealed that Japanese emergency services and hospitals, despite handling over 5,000 patients on that day, managed to handle the overwhelming casualty count because Tokyo had the hospital density and medical infrastructure to absorb a mass-casualty event of that kind.[3] Most cities, including most Indian ones, do not.

Aum Shinrikyo did not stop at chemical agents. The group also ran what remains the most ambitious biological weapons programme ever undertaken by a non-state

actor, pursuing both anthrax and botulinum toxin, though neither was deployed as effectively as Sarin.[4] The lesson to be drawn is not really about Aum Shinrikyo; it is about what the attacks proved was possible, that a non-state group with modest resources and no state backing could independently synthesise and use chemical weapons and come close to using the biological weapons.

That threshold of using Weapons of Mass Destruction (WMD) has been tested since, most visibly through ISIS's use of chlorine and mustard agents in Iraq and Syria between 2014 and 2017. The nuclear and radiological threshold has proven harder to breach outright, but Pakistan's own A.Q. Khan case showed why that threshold cannot be treated as a secure one. A.Q. Khan, the metallurgist who built Pakistan's uranium enrichment programme, spent the 1980s and '90s running a parallel black-market operation on the side, using the same private suppliers and manufacturing contacts to sell centrifuge designs and hardware to Iran, Libya, and North Korea, entirely without Pakistan's government's sanction.[5] Due to the shipment intercepted in 2003, which unravelled the network. What this proved was not that terrorists can build a bomb; it is still farfetched. However, once nuclear weapons technology/material gets inside a private supply chain, it can have catastrophic effects. That is a thinner wall than is assumed.

For India, sitting in a neighbourhood where terrorist networks and state fragility often intersect, which is the operating environment this article is written against.

India’s Doctrinal and Institutional Framework

Does India have a dedicated CBRN doctrine? The honest answer would be, No. What India has is a Disaster Management Framework that covers CBRN as one category among many, and it is not even named as such in the founding legislation. The Disaster Management Act of 2005, which created the entire institutional architecture described in this section, does not use the term CBRN anywhere in its text. Its provisions for the National Disaster Response Force speak only of a "specialist response" force for "threatening disaster situations" in the generic sense.[6] The NDRF's CBRN mandate does not even come from one instrument. NDMA has issued separate chemical, biological, and nuclear/radiological hazard guideline documents, each covering early warning, capacity-building, and response protocols

for its respective category, but no single CBRN framework. That's no small difference. In India, CBRN response is based on an administrative guidance sitting on top of a law that does not even mention the category. There is no specific primary legislation prescribing threat thresholds, escalation triggers, or who commands what in the event of a deliberate CBRN attack by a non-state actor, as opposed to an industrial accident or a natural-hazard-triggered release.

The gap between accident and attack is more significant than it looks at first glance. A chlorine leak by accident and a coordinated attack call for very different immediate responses. The gap is in treating identification, detection, and threat neutralization as disaster-management functions in the conventional sense.

On the ground, more organisations are taking part in the response to CBRN incidents than the law recognises. The NDRF is the first-responder agency designated for CBRN incidents in the civilian sector. DRDO, via organisations such as DRDE Gwalior and INMAS, supplies the technical and diagnostic support, detection equipment, decontaminants, and medical countermeasures. AERB has regulatory responsibility for the security of radioactive sources, a role whose practical boundaries were shown during the 2010 Mayapuri incident. The Indian Army, the Indian Navy and the Indian Air Force each have their own NBCD training facilities and response procedures, these having been tailored to ensure battlefield survivability rather than to deal with large-scale civilian casualties, even though in practice this difference is becoming less clear. There is, however, one structural connection between the civil and defence response agencies provided by the DM Act. The Chief of the Integrated Defence Staff is a member of the National Executive Committee (NEC) by right and serves on the committee which assists the NDMA,[7] a general coordination mechanism, but one with no CBRN-specific content of its own.

What this demonstrates, if anything, is the absence of a capability. India's capacity to respond to CBRN incidents is being developed, if slowly, through inter-service training as well as the acquisition of state-of-the-art equipment. At the same time, responsibility for such tasks is not formally established, being based on a legal framework not explicitly addressing CBRN issues. There is no overarching authority tasked with responding to CBRN incidents, covering the entire spectrum of

response, from threat recognition and decontamination to consequence management.

The Radiological Dirty Bomb Scenario

If one wants to know how a dirty bomb scenario plays out on Indian soil without any terrorist ever being involved, Mayapuri poses the perfect example. In Feb 2010, a Gammacell 220 irradiator containing Cobalt-60, sitting unused in a Delhi University chemistry lab since 1985, was auctioned off as scrap without anyone flagging what it actually was.[8] It ended up dismantled by hand in a scrap market, its radioactive parts cut into pieces and passed between dealers who had no idea what they were handling. One dealer kept a fragment of the radioactive material in his wallet for days. Eight people had to be hospitalised with Acute Radiation Syndrome and out of them, one later died from multi-organ failure.[9] The Atomic Energy Regulatory Board (AERB) eventually recovered ten sources, however only after the exposure had occurred. There was no system along the source's path that captured the source, and therefore it was not recovered during transit.

What Mayapuri showed was not a first and only case of a system failure. It showed the loss of sources remains a clear systemic problem in India. Radioactive material from old medical, industrial and research equipment is known to enter the informal scrap market. This happens when regulatory oversight is lost when the sources leave their institutions.[10] A later study of the scrap dealers in Delhi showed most of the dealers still lack the required knowledge of the safety concerns posed by radioactive waste. These individuals are most likely to discover the lost sources. This is a structural problem and not a lack of awareness.[11]

This pertains to RDD threats. A Radiological Dispersal Device (RDD) needs a radioactive source and only a way to disperse it. It doesn't need sophisticated technology or materials. Mayapuri demonstrates how these sources may pass through Indian scrap networks with very little traceability. The distinction between an exposure caused by radioactive material that was released by accident and an exposure caused by a Radiological Dispersal Device does not depend on whether or not the materials were available. It depends on whether or not there was an intent to do so. Given the existing terrorist groups in India, especially those supported by

Pakistan, this article will not assume that if orphan sources exist, our country will not be vulnerable to what orphan sources have to offer against our interests.

The delivery mechanism for an RDD has also changed in ways that Mayapuri would have little reason to have anticipated in 2010. Commercial drones enable a non-state actor to deliver radioactive material without requiring him to get anywhere near his intended target, a consideration that would previously not have figured in CBRN threat assessments for decades prior to their ubiquity. The danger is not merely theoretical, as the very real attempt by a group to land a drone carrying radioactive sand on the Japanese Prime Minister's office building demonstrates, and analysts have noted that such attacks are likely to become ever more common.[12] Analysts tracking CBRN threats have since flagged that commercially available drones, cheap, easy to modify, and requiring no specialised piloting skill, lower the barrier for a non-state actor to disperse a radiological source over a crowded area from a standoff distance, without ever needing to breach physical security around the target.[13] For India, this adds a dimension the Mayapuri case did not have to contend with. Even if source security at the point of origin is tightened, an actor who has already acquired material, whether through the scrap economy or otherwise, no longer needs to deliver it by hand.

There is also a second, related dimension to this problem that the Mayapuri case does not display. India's civil nuclear fleet is expanding fast, from 24 reactors today toward a targeted 100 GW by 2047. Every additional reactor adds another facility holding radioactive material, a set of contractors and vendors and another point of potential compromise. This is not a hypothetical concern. In 2019, at the Nuclear Power Plant at Kudankulam, there was a breach reported at the administrative network by malware, which was later linked to North Korea's Lazarus Group.[14] NPCIL initially denied the attack before admitting it within 24 hours. Another breach has been reported in Jul 26, wherein close to 19,000 sensitive documents regarding Kudankulam's newer units have been leaked on the dark web including engineering drawings, infrastructure layouts and vendor details, etc.[15] NPCIL has maintained that reactor control systems remain air-gapped and unaffected in both cases. However, security researchers observed that an air gap defeats untargeted intrusions, not determined, targeted ones and that data of exactly this kind can be used to map a facility's vulnerabilities for a future physical or cyber-enabled attack.[16] A larger

reactor fleet will accompany a wider, harder-to-secure attack surface that a non-state / state proxy actor need not physically breach akin to Mayapuri's scrap dealer's case. This makes us look deeper into the requirement of having better CBRN countermeasures.

Pakistan's Tactical Nuclear Weapons: Custody, Contamination and the Non-State Actor Risk

Pakistan did not build battlefield nuclear weapons on a whim. It was a direct response to India's own conventional doctrine. India began developing what came to be called the Cold Start doctrine, the idea of rapid, shallow conventional strikes that could answer Pakistan for a terrorist provocation before international pressure forced a halt. Islamabad's answer was to fill the gap at the tactical level. In 2011, Pakistan tested the Nasr (Hatf-IX), a short-range, nuclear-capable missile built explicitly for battlefield use, and folded it into a doctrine it now calls Full Spectrum Deterrence.[17] The logic on paper is straight forward, strategic, operational and tactical nuclear capability spread across the full range of India's territory, so as to close what Pakistani planners saw as a gap for conventional punishment below the nuclear threshold.[18]

For India, the operationally relevant question is what happens to Indian formations and the surrounding population if a low-yield battlefield weapon is actually used against advancing troops. This is a contamination and consequence-management problem as much as a military one. Radiological fallout does not respect a unit's forward line of troops, and decontamination of both personnel and terrain would need to happen while operations continue, not after they conclude.

There is another risk here that most observations on TNWs tend to overlook. Analysts examining Pakistan's tactical nuclear command and control have pointed out that battlefield deployment inherently means dispersing weapons closer to the front, under looser custodial arrangements than strategic warheads held in central storage and that this dispersal itself raises the risk of a non-state actor gaining access to a weapon, whether through theft, insider compromise or battlefield capture.[19] A TNW employed on the battlefield and a TNW that leaks into non-state

hands are, from India's consequence-management perspective, more or less the same contingencies.

The two contingencies converge further once delivery is considered rather than just acquisition. Fissile or radiological material recovered from a forward-deployed weapon, whether through battlefield capture, insider compromise or post-strike scavenging of a damaged system, would no longer require a non-state actor to be physically present at the intended target to disperse it. Commercially available drones, already flagged as an emerging RDD delivery vector,[20] means that material sourced from a compromised battlefield weapon could in principle be dispersed at a location distant from the original theatre of conflict, complicating both attribution and containment. This is what makes the TNW's custody, a question that is inseparable from the rest of this article's concerns. It is not only about what happens if Pakistan uses a battlefield weapon as intended, but also what happens to whatever residual material a poorly secured system leaves behind and how far that material could travel before anyone is in a position to stop it.

NDRF's Capability Assessment

On paper, NDRF's CBRN capability looks solid. Sixteen battalions are trained and equipped to handle chemical, biological, radiological and nuclear emergencies, organised into self-contained teams of 47 personnel each, built to operate independently for 72 hours.[21] NDRF's CBRN credentials were tested in April 2010, when NDRF teams handled the retrieval of Cobalt-60 material at Mayapuri.[22] NDRF has also run hundreds of CBRN mock exercises involving personnel from different agencies. Ahead of the G20 Summit in 2023, it added seven more HAZMAT vehicles for chemical and radiological threats alone. The Home Ministry even called 2024 its "Year of CBRN Preparedness."[23] This goes to show that CBRN has not been ignored in totality.

A deeper analysis beyond numerical data reveals significant gaps. A serving CBRN professional who wrote on India's readiness CBRN pointed out that apart from NDRF's own CBRN teams, no other civil agency in our country is truly trained to handle a CBRN incident.[24] This means that in case an incident requires a response which is beyond NDRF's capacity, there is no other agency to turn to. Alarmingly, the

article also mentions that awareness with respect to CBRN risk is quite poor among the responders, i.e., the police force. They are unaware of whom to contact and what actions to take in case of a CBRN threat[25] Another article reviewing the CBRN policy points to the same things. NDMA's CBRN guidelines look worked out properly on paper; however, they are practically suffering and have not been thoroughly thought out in detail for real-time use.[26]

Therefore, it is not about the NDRF being under-equipped. It has the latest equipment and developed training infrastructure. The issue is that only training personnel and developing/acquiring equipment is not a comprehensive answer. The focus on training has to percolate to SDRF/DDRF. Parallelly, hospitals have to be equipped for mass casualty CBRN patient handling. Further, there is no guideline which mandates the NDRF, the Armed Forces and civil administration to rehearse a response together.

Armed Force's CBRN Capabilities

If there is one place where India's CBRN capability is genuinely strong, it is the Armed Forces. That strength, however, was built for a different purpose than the one this article is concerned with, and the mismatch deserves before turning to what each service actually brings to the table.

The Indian Army, Indian Navy and Indian Air Force each maintain their own CBRN training and response setup. The impetus for the CBRN preparedness was provided by Pokhran-II in 1998, which was shortly followed by Pakistan's nuclear tests, which signalled a belligerent, nuclear-armed neighbour.[27] Kargil, just a year later, demonstrated that Pakistan was ready and willing to fight a war, including a nuclear one, and so the need for systematic CBRN defence preparations was now a matter of urgency and not an academic exercise. The training at Armed Forces CBRN institutions is focused on the specific battlefield requirements and onboard ship response. Personnel trained at these institutions are better equipped to fight or keep a ship in operational condition in a chemical, biological or nuclear environment and have limited understanding of how to operate in a civilian environment in the case of a mass-casualty situation due to a CBRN attack.

The Indian Army's CBRN threat neutralisation approach is summarised in CBRN-trained units, detection of threat and decontamination of affected areas, retaining fighting capability and mobility of formations. It is undoubtedly the most mature land-based CBRN skill set available in the country. However, it has been built around protecting and triaging a fighting force and not for handling thousands of civilian casualties.

The Indian Navy works on a similar framework, however, at sea. A ship has room to manoeuvre around a CBRN fallout area, in case a mission allows it to do so. In case the mission requires passing through the fallout, or in case the ship is already under attack, there is no retreat from contamination. The ship has to pass through the contamination, keeping its crew safe. This requirement has developed a discipline around early detection, monitoring, containment and speedy decontamination onboard, for which personnel are trained at the Indian Navy's training institute. This expertise in close environments may also be well used in enclosed civilian spaces like metro stations; however, the skill is required to be practised and propagated to civil agencies.

The contribution of the Air Force is more of aerial surveillance for CBRN contamination/detection and rapid airlifting of specialist teams, materials and casualties. During the 2014 J&K floods, around 70 aircraft of the Indian Air Force managed to carry over 96,000 people and 3,500 tonnes of material within days.[28] The same capacity can be used to rapidly airlift casualties in case of a mass-casualty CBRN incident, although the joint training in this respect with civilian agencies needs to be looked into. The Armed Forces over the past years have developed immense capabilities in terms of advanced equipment through DRDO and iDEX challenges. Further, training of the three service personnel has grown exponentially post establishment of the CBRN Joint Services Training Institute.

The combined capability of the Armed Forces cannot be levelled with the civil agencies. The Armed Forces have time and again demonstrated capability to rapidly mobilise and deliver in inaccessible terrains whenever there has been a requirement. For instance, during the 2025 Myanmar earthquake, a 60-bed Indian Army field hospital provided inpatient care to more than 2,500 casualties within two weeks. Indian Naval ships and aircraft provided 750 tonnes of disaster relief supplies.[29] With

these kinds of capacities and readiness, the Services should be able to respond effectively to a domestic CBRN incident.

However, capability available in three separate services, developed for three different original purposes, is not the same as a single, ready civil-military CBRN response system. The Disaster Management Act just mentions deploying the armed forces, without spelling out how that deployment should actually work, who commands it or how it links to what NDRF is doing on the ground.[30] This is not a capability problem. It is a problem with connecting capabilities, and the next section tries to address it.

Civil-Military Jointness- The Way Forward

In all that has been brought out in the preceding paragraphs, there is one conclusion to be drawn. It is no lack of CBRN capability; the NDRF and armed forces are well equipped dealing with such scenarios. However, it lacks the systematic mechanism that will combine these individual capabilities when the situation demands. NDRF is under the Home Ministry and deals with any sort of disaster management, including CBRN, as one of its components, while the Armed Forces are under the Ministry of Defence responsible for battlefield management, which includes CBRN as well. Thus, there are two separate command and control structures in place which do not have a systematic way to combine their capabilities when an emergency arises.

It is under this context that the Disaster Management Act must be read wherein the Chief of the Integrated Defence Staff is an ex-officio member of the National Executive Committee that advises the NDMA.[31] This again shows a lack of command and control, as it does not mention who will be in charge if both the NDRF and the Armed Forces are involved in disaster response management. Thus, even though one man shows up in both the organisations, it does not define operational command and control.

It is through various exercises that jointness between NDRF, the NDMA and the Armed Forces has been developed. The Indian Navy's exercise Chakravat and the Indian Army's Sanyukt Vimochan involve joint drills with the other two entities, with Chakravat also including foreign participation.[32] Although these exercises provide a

forum for the agencies to meet each other in a joint environment, they are not specifically designed to tackle CBRN scenarios.

The experience of other countries seems to be partially useful. A case in point, the US has a well-defined division of responsibility between the National Guard and the Department of Defence for CBRN-related tasks, with clearly defined triggers for the involvement of the Department of Defence. Although this does not exactly fit India's federal structure, this experience can be helpful, and it is necessary to find solutions that would connect all elements together into a system so that there is no need to rush to think of something in the moment of an immediate threat or actual crisis.

NDRF's teams, the Services' CBRN/NBCD expertise, DRDO's technical backbone, and AERB's regulatory reach have all grown over the past decade. The missing link is not the capability; it is the link itself. The legal and doctrinal framework was never written with a deliberate non-state CBRN attack in mind. The Disaster Management Act does not use the word CBRN. Mayapuri showed that even an accidental exposure can expose deep gaps in terms of source security; a deliberate one could cause worse. Pakistan's tactical nuclear posture adds a scenario that requires urgent cognisance.

Recommendations

As per this article's findings, three doable and achievable recommendations should suffice to reduce the gap.

First, to design a separate CBRN-related doctrine, not as a part of additional instructions or appendices but as a standalone document that would clearly define the differences between an incident that involves an intentional attack and a civilian accident. It has to detail the course of action in each case and outline the responsible parties that should be involved in rescue and relief operations.

Second, to create a Standard Operating Procedure for civil-military coordination specific to CBRN incidents. India already has a procedure known as 'Aid to Civil Authority' under the Disaster Management Act that allows civil authorities to request the Armed Force's support in case of any disaster response.[33] However, it is a generic act, and there is no specific regulation on how CBRN-related incidents

should be managed when the National Disaster Response Force (NDRF) and the Armed Forces are on the scene. This gap in the regulatory framework should be filled with a procedure that would outline the roles of the NDRF and the Armed Forces, specify when the latter should be involved to assist the former and designate the command-and-control authority once the military intervention has started.

Third, CBRN preparedness needs to be most emphasised at the state and district level, where an incident is most likely to first be reported. Although NDRF battalions and armed forces establishments carry out cross-service visits to understand each other's capabilities, dedicated and designated facilities at lower levels towards thorough training of SDRF and DDRF personnel are the need of the hour.

Conclusion

India's CBRN readiness has grown steadily; however, growth in capability is not the same as readiness for the moment it is actually tested. What remains unfinished is not capability; it is coordination. The difference between individually strong institutions and a single system that functions as one the moment it actually matters. That difference is not a matter of new equipment or bigger budgets. It is a matter of deciding, in advance, who does what, so that decision does not have to be made for the first time in the middle of a crisis.

Declaration

I declare that this manuscript is being submitted exclusively to CENJOWS for publication consideration, is original, and has not been published or submitted elsewhere. I further certify that it contains no classified, restricted, or sensitive information and is based entirely on open-source material suitable for publication in the public domain.

ENDNOTES

[1]"Tokyo Subway Attack of 1995," Britannica, https://www.britannica.com/event/Tokyo-subway-attack-of-1995.
[2]Ibid.
[3]"What Lessons Can We Learn from the Japanese Sarin Attacks?," PubMed, https://pubmed.ncbi.nlm.nih.gov/16225116/.
[4]"Chronology of Aum Shinrikyo's CBW Activities," Monterey Institute of International Studies, https://www.nonproliferation.org/wp-content/uploads/2016/06/aum_chrn.pdf.
[5]Christopher O. Clary, "The A.Q. Khan Network: Causes and Implications," Naval Postgraduate School (via Defense Technical Information Center), https://apps.dtic.mil/sti/tr/pdf/ADA443142.pdf.
[6]The Disaster Management Act, 2005, Act No. 53 of 2005 (India), §§ 44–45, https://www.indiacode.nic.in/bitstream/123456789/2045/1/aaa200553.pdf.
[7]The Disaster Management Act, 2005, § 8.
[8]Wm. Robert Johnston, "Mayapuri Orphaned Source, 2010," Johnston's Archive, https://www.johnstonsarchive.net/nuclear/radevents/2010INDA1.html.
[9]Ibid.
[10]Comptroller and Auditor General of India, Union Performance Audit: Activities of the Atomic Energy Regulatory Board, Report No. 9 of 2012, https://cag.gov.in/sites/default/files/audit_report_files/Union_Performance_Atomic_Energy_Regulatory_Board_Union_Government_Atomic_Energy_Department_9_2012.pdf; discussed in "CAG Appraisal of AERB: Some Misplaced Concerns," Centre for Air Power Studies, https://capssindia.org/wp-content/uploads/2021/10/ISSUE-BRIEF_59_CAG-APPRAISAL-OF-AERB-SOME-MISPLACED-CONCERNS_01-October-2012.pdf.
[11]"Evaluating Awareness and Practices Pertaining to Radioactive Waste Management among Scrap Dealers in Delhi, India," PMC/PLOS ONE, https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3951456/.
[12]"Unmanned Aerial Vehicles & AI: Policy Measures & Challenges," Vision of Humanity, https://www.visionofhumanity.org/preventing-terrorists-from-using-emerging-technologies/.
[13]Shravishtha Ajaykumar, "Emerging Technologies in the Development and Delivery of CBRN Threats," ORF Issue Brief No. 768, December 2024, https://www.orfonline.org/research/emerging-technologies-in-the-development-and-delivery-of-cbrn-threats.
[14]"Cyberattack Hits Indian Nuclear Plant," Arms Control Association, https://www.armscontrol.org/act/2019-12/news/cyberattack-hits-indian-nuclear-plant.
[15]"India's Largest Nuclear Plant Hit by Cyber Breach; Hackers Leak 19,000 Sensitive Documents on Dark Web," The Researchers, https://www.theresearchers.us/2026/07/15/cyber-breach-india-nuclear-plant/.
[16]"Throwback Attack: An Indian Nuclear Power Plant Falls Victim to Outdated Policies," Control Engineering, https://www.controleng.com/throwback-attack-an-indian-nuclear-power-plant-falls-victim-to-outdated-policies/.
[17]"Pakistan's Evolving Nuclear Doctrine," Arms Control Association, https://www.armscontrol.org/act/2023-10/features/pakistans-evolving-nuclear-doctrine.
[18]"Pakistan's Tactical Nuclear Weapons and Their Impact on Stability," Carnegie Endowment for International Peace, https://carnegieendowment.org/research/2016/06/pakistans-tactical-nuclear-weapons-and-their-impact-on-stability.
[19]"Pakistan's Nuclear Use Doctrine," Carnegie Endowment for International Peace, https://carnegieendowment.org/research/2016/06/pakistans-nuclear-use-doctrine?lang=en.
[20]Shravishtha Ajaykumar, "Emerging Technologies in the Development and Delivery of CBRN Threats," ORF Issue Brief No. 768, December 2024, https://www.orfonline.org/research/emerging-technologies-in-the-development-and-delivery-of-cbrn-threats.

[21]"About Us," National Disaster Response Force, https://ndrf.gov.in/en/about-us.
[22]Ibid.
[23]"NDRF to Observe 2024 as Year of CBRN Preparedness, Response," Business Standard, https://www.business-standard.com/india-news/ndrf-to-observe-2024-as-year-of-cbrn-preparedness-response-124011900209_1.html.
[24]"Lest We Perish: CBRN Incident Management," Defstrat, https://www.defstrat.com/magazine_articles/lest-we-perish-cbrn-incident-management/.
[25]Ibid.
[26]"CBRN Security: Assessing India's Preparedness," The Geostrata, https://www.thegeostrata.com/post/cbrn-security-assessing-india-s-preparedness.
[27]Mudit Sharma, "Chemical, Biological, Radiological and Nuclear Training Issues in India: A Fresh Perspective," Journal of Pharmacy and Bioallied Sciences 2, no. 2 (2010): 155–158, https://pmc.ncbi.nlm.nih.gov/articles/PMC3148632/.
[28]"Beyond Battlefield: Indian Armed Forces in Humanitarian Assistance and Disaster Relief," Press Information Bureau, https://www.pib.gov.in/PressReleasePage.aspx?PRID=2228319&reg=3&lang=1.
[29]Ibid.
[30]The Disaster Management Act, 2005, Act No. 53 of 2005 (India).
[31]The Disaster Management Act, 2005, § 8.
[32]"Beyond Battlefield: Indian Armed Forces in Humanitarian Assistance and Disaster Relief," Press Information Bureau.
[33]"Beyond Battlefield: Indian Armed Forces in Humanitarian Assistance and Disaster Relief," Press Information Bureau https://www.pib.gov.in/PressReleasePage.aspx?PRID=2228319&reg=3&lang=1