Defence Life Science Journal, Vol. 6, No. 1, January 2021, pp. 37-42, DOI : 10.14429/dlsj.6.16667

Nuclear Security Architecture & Radiological Disaster Response in India: Progress and Challenges

Shivani Singh

Aberystwyth University, Penglais, Aberystwyth, SY23 3FE Wales, United Kingdom
E-mail: shs48@aber.ac.uk

ABSTRACT

The nuclear security architecture in India is three-fold: the infrastructure security including physical security of the nuclear plant; port and border security including training and capacity building to prevent any illicit trafficking of nuclear material into the country and; the inter-institutional coordination at the Centre and State level during radiological emergencies. However, there exist structural weaknesses that need to be accounted for in all these three areas. It is imperative to develop capacities not only for safe handling, transport and disposal of nuclear material but also instituting stringent cyber-security laws, border security measures and functional Centre-State coordination in crisis situation for the safety and security of the general population. The following paper seeks to address these challenges and provide recommendations for strengthening the nuclear security and disaster response framework in India. The paper draws recommendations from the 2019 IPCS workshop on Smuggling and Radiation Detection, on the illicit trafficking of radioactive materials supported by the Office of Nuclear Smuggling Detection and Deterrence (NSDD) of the United States Department of Energy (DOE).

Keywords: Nuclear security; Non-proliferation; Radiation detection; CBRN emergencies; Disaster management

1. INTRODUCTION

The Atomic Energy Regulatory Board (AERB) defines nuclear security as "*All* preventive measures taken to minimize the residual risk of unauthorised transfer of nuclear material and/or sabotage, which could lead to release of radioactivity and/or adverse impact on the safety of the plant, plant personnel, public and environment". According to the AERB safety guidelines of December 2009, information on nuclear security entails aspects such as "physical protection system, physical barrier and communication". The definition provided by the AERB falls in line with the broader rubric of nuclear security as agreed to by the International Atomic Energy Agency (IAEA).

The operative phrase in the definition provided by the AERB is "All preventive measures". The guidelines do provide for stringent physical security of nuclear facilities in India including the nuclear power plants, power projects, various fuel cycle facilities as well as other radiation facilities. According to the guidelines, the individual operators are responsible for the safety and security of the nuclear facility. The Central Industrial Reserve Force (CISF) is tasked with deploying trained first responders to the nuclear facility site. Each of these CISF teams is guided by a commandant and they are skilled and equipped to respond appropriately and proportionately in case of a nuclear emergency at the nuclear facility. Hence, the physical security parameters of a nuclear facility are clearly laid out.

However, there are not sufficient security measures in place for transit security of the nuclear material. As far as the security of the front-end of the fuel cycle is concerned, there remain certain loopholes which can inadvertently encourage illicit nuclear proliferation activities. The front-end of the nuclear fuel cycle would imply accounting for the Uranium Ore concentrate that is extracted from the mining of the Uranium Ore and its transport (by land, air and sea) to the Conversion Plant before it reaches the enrichment and fabrication stages. These loopholes in the physical security stage of the nuclear power plant need to be addressed in order to pave way for preventing and by extension facilitating better and more effective implementation of the other two aspects of nuclear security architecture in India, that is border security and inter-institutional coordination in case of a radiological emergency. The next section begins by laying out the current framework for physical security at nuclear power plants and the challenges that need to be addressed.

2. SECURITY OF THE NUCLEAR PLANT: TRANSIT, PHYSICAL AND CYBER DIMENSIONS

Depending on the level of radioactivity present, there are different levels of security-level 1, level 2 and level 3, that are in place for safe transport of Radioactive Material (RAM). The guidelines also provide for installation of hardware for

Received : 21 October 2019, Revised : 20 June 2020
Accepted : 22 June 2020, Online published : 23 February 2021

monitoring the movement of conveyances carrying RAM[1]. Currently the system employed for the accounting of the transit of nuclear material from the ore to the milling stage includes a Unique Identification Number (UID) allotted to the drums carrying the material, which is linked to the production lot number[2]. These drums are then transported to the conversion or fabrication plants. In case of any discrepancy in terms of the amount (weight) of material inside the drums, independent auditors are called in to conduct a review. The whole process of tracking the material leaving the mine is mostly done manually which increases the room for human error or complacency. The lack of a credible security infrastructure in the front-end phase of the nuclear cycle can give terror outfits an open space for theft of such material. Further, this material can then be sold by illegal intermediaries in black market, making the RAM readily available to whomsoever is willing to offer the right price.

To avoid these errors, blockchain technology can come handy for governing the transport of nuclear material, especially in the front-end phase of the fuel cycle which is currently not extensively covered by the national or international (IAEA) guidelines. A blockchain is essentially an online, peer-to-peer, distributed ledger used for maintaining an account of different material/data set depending on the type of blockchain. Although, the most common usage of this technology was seen in context of Bitcoins (virtual currency), blockchain technology can be used in various other fields owing to the high degree of technological sophistication, precision and security that the system entails.

Each container/drum carrying RAM from the ore can be marked with a microchip which will give that container a unique digital identity containing all information like the nature of material inside the container, the weight, level of radioactivity, names of persons allotted to oversee smooth transportation of the container, the route to be taken for transporting the container from the place of origin to place of destination and so on. All the personnel having access to this digital identity will be able to track the movement of the container in real-time. Hence, any changes, like a diversion in the route of transportation or any discrepancies in weight etc can be tracked as it happens, hence not losing any time in taking appropriate action[2].

Similarly, a consortium of blockchains for nuclear material accounting can be created with the unique digital identity of each, drawing from the previous one so that any small, malicious activity aimed at breaking into the system will be caught in real-time.

This is not an entirely new concept as the AERB, in its guidelines, has suggested that an "automated and real time tracking methods should be deployed in order to permit the transport control centre to remotely monitor the movement of radioactive material conveyances and packages and their status"[1].

Similarly, physical sabotage or accidents aren't the only threat scenarios that exist. Another facet of physical security of the nuclear facility which is often ignored is a stringent cyber security infrastructure. It is possible for hackers to introduce a malware into the functioning systems inside the nuclear facility and make the instruments or reactors malfunction or shut them down entirely. This was observed during a cyber-attack at a petrochemical plant in Saudi Arabia wherein a malware called 'Triton' was introduced into the critical systems of the industrial infrastructure of the plant in 2017.

Another instance of using cyberspace to target security systems at a nuclear facility was in 2010 when a malware called 'Stuxnet' caused hundreds of centrifuges at an Iranian nuclear plant to function out of control and destroy themselves[3]. Specifically, in India's case, certain reports surfaced some time back, concerning the Uranium enrichment plant at Rattehalli near Mysore being compromised due to its critical infrastructure being exposed to the 'Stuxnet' malware. More recently, India's Kudankulam Nuclear Power Plant (KKNPP) was attacked by a 'dtrack' malware in September 2019, that affected the plant's administrative network[4].

The seriousness of a cyber security attack can be gauged from the fact that since at nuclear plants, the nuclear generators, once installed with fuel, run for a couple of years at a stretch, any disruption can cause the reactor to shut down leading to melting of the reactor core. Although such errors could be a result of human complacency, operator errors or the system malfunction as was seen in the Three-Mile Island crisis, a malware can replicate the same errors with risks almost ten folds and cause a reactor to melt[5].

Currently, the point entity for handling cyber security at nuclear facilities in India is Computer and Information Security Advisory Group (CISAG) and the Task Force for Instrumentation and Control Security (TAFICS).

Despite having serious repercussions for the security of critical infrastructure like nuclear facilities, there is no mention of management of cybersecurity threats in the National Disaster Management Guidelines on 'Management of Nuclear and Radiological Emergencies'[6].

The AERB D-25[7] and D-10[8] safety guide released in 2003 and 2005 respectively provide a manual for computer-based safety systems of PHWR. The guide mentions the security requirements to be met by instrumentation and control systems (I&C) at nuclear power plants, like tamper-proof event logs, sanitisation of pre-developed software and so on. However, these guidelines need to be updated to account for the new kinds of cyber security threats that have emerged ever since. To address this very issue, BARC, in 2010, came out with a special issue on I&C security for nuclear power plants where based on the AERB and international I&C security guidelines, the article featured a system specific plan for evading I&C related threats[9].

One of the more recent 2014 BARC special issue gave a detailed view on secure network access systems (SNAS), India's only integrated network security solution[10]. More recently, a 2017 query raised in Rajya Sabha on possible cyber security threats to nuclear facilities attracted response from the government on how safe and secure the nuclear facilities are in India[11]. However, there was no detailed mention on how the new kinds/nature of cyber security threats emerging in present times is being dealt with by the government.

Adopting new measures like the upcoming Shared Ledger-SAFKA[12] "informed by Finland's nuclear material database (SAFKA) and co-developed with Stimson Centre for the safety of nuclear material in the front and back-end phase

of the nuclear cycle is absolutely imperative especially when, India ranks 19th in the "theft rankings' out of 22 countries with weapons-usable nuclear material[13]. Although India is party to the Convention for the Physical Protection of Nuclear Material (CPPNM) and has ratified the 2005 amendment as well[14], there is still scope for improvement.

3. TRAINING OF PERSONNEL AND ACCESS TO RADIATION DETECTION EQUIPMENT

The second most important aspect of preventing illicit trafficking of nuclear material is a stringent radiation detection law enforcement which includes proper training of personnel deployed not only at the nuclear facilities but also at ports and borders as well as capacity building in terms of providing appropriate instruments for radiation detection.

The IPCS workshop on Smuggling and Radiation Detection held in June 2019 highlighted all the major instances of nuclear smuggling witnessed in India including- a uranium smuggling racket in 1992 which was busted by Kolkata police, seizure of 100 kg of uranium in 1998 by the West Bengal police, theft of a container in 2006 from a research facility in Eastern India which was never found and the 2016 arrests made by Thane police for possession of radioactive uranium.

There exist systemic vulnerabilities which have been exploited several times in the past and continue to expose nuclear facilities to acts of nuclear terrorism. For example, the Central Industrial Security Force (CISF), which is mainly tasked with guarding the nuclear facilities is not sufficiently equipped with spotting instances of smuggling of nuclear material in and out of the facility. This is because all nuclear facilities have different security systems. While some facilities are solely guarded by the CISF, there are others like the Heavy Water Plant in Hazira which is guarded by security personnel of Krishak Bharti Cooperative Ltd (KRIBHCO) in collaboration with the state Police personnel, and Institute of Plasma Research (IPR) at Gandhi Nagar which is guarded by private security personnel. Therefore, there is an absence of a unified and standardised security apparatus across the country[15].

Similarly, India's porous borders with countries like Nepal, Bangladesh and so on further allow for free movement of material of any nature across the border. Almost all cargo entry points in India-be it air, water or land are supposed to be installed with radiation detection equipment. Additionally, all personnel are provided with and trained in using handheld mobile radiation detection systems. To further enhance airport security against illicit smuggling of nuclear material, a radiological mock drill was conducted at Rajiv Gandhi Hyderabad International Airport in 2017[16]. This was followed by a training programme conducted by NDMA in 2018 at the Indira Gandhi International Airport (IGI), New Delhi for preparedness for CBRN emergencies[17]. Similar training programme was conducted at the New Mangalore Port Trust, Mangaluru and a mock drill at a mall in Vijayawada in 2019 to enable Seaport Emergency Handlers (SEH) and the NDRF officials respectively to handle threats emanating from CBRN-related emergency[18]. However, there remains certain gaps in implementation and a lot more needs to be done for sensitisation and standardised training of personnel across the country tasked with prevention and mitigation of acts of nuclear terrorism.

In addition to that, the disaster response mechanism for CBRN-related emergencies needs to be strengthened many folds. There is a wide scope for updating the training modules and frequency of training of stakeholders including the National Disaster Management Authority (NDMA) and National Disaster Response Force (NDRF) team along with training of Border Security Forces (BSF), Central Reserve Police Force (CRPF), CISF and Indo-Tibetan Border Policy (ITBP), especially in cases of Chemical, Biological, Radiological and Nuclear (CBRN) emergencies. For instance, between 2006 to 2015, out of 291 mock exercises, the NDMA conduced only 7 mock exercises for off-site Nuclear and Radiological Disaster where 6 exercises took place in 2011 and 1 mock exercise in 2013[19]. Similarly, from 2015 to 2016, only one mock exercise on CBRN disaster was conducted while the mock drills from 2016 to 2018 have no mention on the nature of mock exercises that were conducted[20]. There is no specific mention of the 2019 calendar for mock drills by the NDMA. Additionally, although large number of hospitals across India have been prepared to treat CBRN casualties, according to latest updates by BARC, there are no hospitals exclusively designated for handling CBRN disasters[21]. The slow pace of development in the area is evident from the fact that there has only been a marginal increase in number of Emergency Response Centres (ERC) in India from 18 in 2009 to 25 in 2019[22].

There is definitely a growing awareness for the need of training workshops for tackling CBRN-related emergencies. For example, in 2015-2016, specialised training and advanced courses and workshops were conducted for the NDRF battalion personnel in CBRN operations at the North Eastern Police Academy (NEPA) and Bhabha Atomic Research Centre (BARC)[23]. Similarly, in 2017, workshop on medical management of CBRN casualties for medical officers was held in New Delhi and BARC, Mumbai[16]. The recently proposed 2019 annual training calendar by the NDRF mentions refresher courses CBRN emergencies for the NDRF battalion including First Responders[24].

Management, prevention, mitigation and preparedness for CBRN disasters has been incorporated into the training curriculum on capacity building by NDMA for not only NDRF personnel but also the Indian Police and Army personnel as they are equal stakeholders during a radiological emergency[25]. Apart from the NDMA, the Ministry of Defense also runs a CBRN training curriculum which is especially designed to "assist the Armed Forces Medical Services (AFMS), an inter-services organisation, to improve its emergency preparedness"[26]. According to reports, these trainings are supposed to be conducted periodically at the command, corps and division level. However, the course details on capacity building have not been updated online. Relevant and up-to-date information on such training modules is necessary to suggest measures that can be taken to improve upon such courses to tackle the new kinds of threats that are emerging within the CBRN domain.

Therefore, measures like effective coordination and integration of civil and military training for CBRN disasters, standardised (and customised where needed) training manual for

concerned personnel to deal with such emergencies, modelling national emergency response mechanisms after international standards and increasing the frequency and quality of training and simulation exercises, with sufficient access to radiation detection equipment for handling radiological emergencies at the border as well as at major public events (MPE) can substantially enhance India's level of preparedness.

4. EFFECTIVE CENTRE-STATE COORDINATION

Last but not the least, the third essential element of strengthening the nuclear security and disaster management circuit includes strong, credible and effective coordination mechanism between the centre and state authorities responsible for dealing with a possible radiological disaster.

The Department of Atomic Energy is the nodal technical agency for handling a nuclear/radiological disaster especially in the public domain like a major public event. While the NDMA and NDRF work on the centre level to mitigate the risks, state and district authorities like State Disaster Management Authority (SDMA) and District Disaster Management Authority (DDMA) work in close coordination with the central authorities and various other stakeholders in a nuclear crisis.

However, there is a need to institute and most importantly, implement clear Standard Operation Procedures (SOP) in case of a radiological emergency. Lack of proper SOPs to handle a nuclear crisis in major public events like a cricket match was pointed out in the 2019 IPCS workshop on Smuggling and Radiation Detection as well. According to the findings, radiation detection for MPE only began roughly two years ago, that too for VIPs.

The NDMA, in its guidelines clearly mention the need the strengthen the formal linkages and coordination mechanisms between DAE, Crisis Management Groups (CMG), ERCs and the state and district level authorities in an event of a radiological emergency. This needs to be complemented with appropriate intra-state coordination between the SDMA, the DDMA and the nearest NDRF battalion deployed for dealing with such emergency situations[6].

While all states have a state disaster management plan in place, it is highly imperative that the State Disaster Response Force (SDRF) in every state is well equipped and trained in radiological emergency management. Currently, there is no such exclusive CBRN training included in the mock drills that is conducted by the SDMAs and hence it needs to be instituted for smooth and uninterrupted coordination between the district, state and centre authorities.

5. BEST PRACTICES

While there is still a long way to go before blockchain technology can be incorporated into the nuclear security architecture of countries, some major advancements have been made in key areas of nuclear security, addressing some of the challenges raised above. Australia is one such country which has performed consistently, ranking first in the Nuclear Threat Initiative (NTI) index on nuclear theft and security since 2012. This includes stringent on-site physical protection, comprehensive measures for prevention of insider threat, controlled oversight of nuclear material transport and its frequency and so on.

Regular training and simulation exercises form a core component of Australia's nuclear security strategy. In addition to conducting national-level exercises and training course on enhancing radiation emergency response capability, Australia has actively collaborated with international organisations such as IAEA, WHO and FNCA (Forum for Nuclear Cooperation in Asia) on operational, tactical and command level to enhance interoperability across all jurisdictions[28-29]. One of the noteworthy features of Australia's nuclear security regime is the robust inter-agency coordination between ARPANSA (Australian Radiation Protection and Nuclear Safety Agency) and Australian Customs and Border Protection Service for border control enhancements for import and export of radioactive material across the border[28].

Australia invited the IAEA International Physical Protection Advisory Service (IPPAS) in 2017 for a follow-up mission the progress on the country's nuclear security systems. In the final mission report, the IPPAS appreciated 5 best practices including periodic safety review process of research reactors, "no alone zone" function of the Electronic Access Control System to protect against insider threat, regular surveys across industries to update the information security manual for assessing new threat information and so on[30]. Australia has further improved its nuclear security with periodic updates of the Design Basis Threat (DBT) and instituting a "cyber-incident response plan" at nuclear sites[31].

As far as physical safety of the nuclear sites is concerned, UK has a special branch of police called Civil Nuclear Constabulary (CNC) to guard those nuclear material and facilities that do not fall under the jurisdiction of the armed forces[30] unlike India's CISF which is tasked with guarding industrial units and critical infrastructures across the board. Additionally, France has a Specialized Platoons Protection Police (PSPG) which is a "unified command and training structure to ensure high levels of interoperability between these forces in the time of a crisis"[32.]

6. CONCLUSIONS

The three-fold nuclear security architecture as mentioned in the paper highlights the progress that has been made so far as well as the lacuna in the current discourse on nuclear security in India. Incidentally, most of the areas of improvement as mentioned in the paper and underscored at the 2019 IPCS workshop on Smuggling and Radiation Detection are the same issues mentioned in the 2009 NDMA guidelines on "Management of Nuclear and Radiological Emergencies". This shows that in the last one decade, while steps have been taken by the government to improve upon the structural and technological weaknesses, there is still a wide scope of further improvement in the nuclear security domain. Selected practices of other countries in the domain could serve as a guiding path for further improvement. These practices would obviously have to be re-modelled to suit India's special security needs, socio-cultural environment and geostrategic concerns.

REFERENCES

1. Security of radioactive material during transport. Atomic Energy Regulatory Board. Aerb Safety Guide No. AERB/NRF-TS/SG-10. January 2008.
2. Bal, Meghna. Preventing proliferation: Tracking uranium on the blockchain. Observer Research Foundation. 12 April 2018 https://www.orfonline.org/research/preventing-proliferation-tracking-uranium-blockchain/. (Accessed on 28 September 2019).
3. Giles, Martin. Triton is the world's most murderous malware, and it's spreading. MIT Technology Review. https://www.technologyreview.com/s/613054/cybersecurity-critical-infrastructure-tritonmalware/?utm_medium=Social&utm_campaign=site_visitor.unpaid.engagement&utm_source=LinkedIn#Echobox=1564766972. (Accessed on 1 October 2019).
4. NPCIL admits malware attack at Kudankulam Nuclear Power Plant. The Hindu. 30 October 2019. https://www.thehindu.com/news/national/npcil-acknowledges-computer-breach-at-kudankulam-nuclear-power-plant/article29834644.ece. (Accessed on 14 January 2021).
5. Kesler, Brent. The vulnerability of nuclear facilities to cyber attack. Strategic insights. 2011. Volume 10(1) http://large.stanford.edu/courses/2015/ph241/holloway1/docs/SI-v10-I1_Kesler.pdf. (Accessed on 2 October 2019).
6. National disaster management guidelines: Management of nuclear and radiological emergencies. National Disaster Management Authority (NDMA). February 2009. ISBN: 978-81-906483-7-0.
7. Safety related instrumentation and control for pressurised heavy water reactor based nuclear power plants. Atomic Energy Regulatory Board. Aerb Safety Guide No. AERB/NPP-PHWR/SG/D-20. January 2003. https://www.aerb.gov.in/storage/images/PDF/CodesGuides/NuclearFacility/NPPDesign/11.PDF. (Accessed on 3 October 2019).
8. Safety systems for pressurised heavy water reactor. Atomic energy regulatory board. Aerb safety guide no. AERB/NPP-PHWR/SG/D-10. October 2005 https://www.aerb.gov.in/storage/images/PDF/CodesGuides/NuclearFacility/NPPDesign/7.PDF. (Accessed on 3 October 2019).
9. Babu, R.M Suresh, Mahapatra, U. & Srivastava, G.P. I&C security for nuclear power plants: A study. BARC Newsletter. September-October 2010. Issue No. 316.
10. Joseph, Gigi. Secure network access system. BARC News Letter. October 2014. Special Issue.
11. Threat on nuclear facilities. Rajya sabha unstarred question No. 483. 20 July 2017. Government of India.
12. Safeguards program attends SLAFKA project kick-off. Stimson organisation. https://www.stimson.org/content/safeguards-program-attends-slafka-project-kick?utm_source=Stimson+Center&utm_campaign=041fc335d7-Prog%2FNuclear%2FNuclear+Safeguards+Updates&utm_medium=email&utm_term=0_15c3e20f70-041fc335d7-46294693&mc_cid=041fc335d7&mc_eid=653f0883ec. (Accessed on 10 October 2019).
13. India ranks 19 in 'Theft Ranking' for countries with weapons usable nuclear materials. The Indian Express. 6 September 2018 https://indianexpress.com/article/india/india-ranks-19-in-theft-ranking-for-countries-with-weapons-usable-nuclear-materials-5342468/. (Accessed on 15 October 2019).
14. India's national progress report, Nuclear security summit 2016. Ministry of External Affairs, Government of India. 2 April 2016 https://mea.gov.in/bilateral-documents.htm?dtl/26590/Indias_National_Progress_Report_Nuclear_Security_Summit_2016. (Accessed on 15 October 2019).
15. Mishra, Sitakanta and Jacob, Happymon. Nuclear Security Governance in India: Institutions, Instruments, and Culture. Sandia Report. SAND2015-0233. January 2015.
16. NDRF Training data. 2017. http://www.ndrf.gov.in/sites/default/files/DATA_0.pdf. (Accessed on 10 October 2019).
17. NDMA conducts training programme for CBRN emergencies at New Delhi airport. Ministry of Home Affairs. Public Information Bureau. 10 December 2018. https://pib.gov.in/PressReleaseIframePage.aspx?PRID=1555409. (Accessed on 20 October 2019).
18. NDMA conducts training programme for CBRN emergencies at New Mangalore. Ministry of Home Affairs. Press Information Bureau. 11 February 2019. https://pib.gov.in/newsite/PrintRelease.aspx?relid=188366. (Accessed on 20 October 2019).
19. Mock drill at PVP Mall on CBRN emergencies. The New Indian Express. 28 March 2019 https://www.newindianexpress.com/cities/vijayawada/2019/mar/28/mock-drill-at-pvp-mall-on-cbrn-emergencies-1957051.html. (Accessed on 1 June 2019).
20. Mock exercises conducted by the NDMA from 6th October 2006 to 27 Mar, 2015. National Disaster Management Authority (NDMA). https://ndma.gov.in/images/pdf/Mock-Exercise.pdf. (Accessed on 20 October 2019).
21. Mock exercise conducted during the year 2015-2016. National Disaster Management Authority (NDMA) https://ndma.gov.in/images/pdf/MOCKEXERCISES-2015-17.pdf. (Accessed on 20 October 2019).
22. Management of nuclear / radiation disaster. Bhabha Atomic Research Centre (BARC). http://www.barc.gov.in/pubaware/gen_disaster.html. (Accessed on 20 October 2019).
23. Meet on prevention, preparedness & response to potential radiation threats / emergencies at Kalpakkam. Press Information Bureau. 17 May 2019. https://pib.gov.in/PressReleaseIframePage.aspx?PRID=1572178. (Accessed on 20 October 2019).
24. NDRF Training during 2015-2016. http://www.ndrf.gov.in/sites/default/files/Training.pdf. (Accessed on 20 October 2019).
25. Proposed NDRF annual training calendar for the year 2019. http://ndrf.gov.in/sites/default/files/NDRFTRGCALENDER%202019.pdf. (Accessed on 20 October 2019).
26. Bansal, J.K. & Ratan, C. Preparedness for CBRN

emergencies. Bharat Defence Kavach. 26 July 2018. http://www.bharatdefencekavach.com/news/expertopinion/preparedness-for-cbrn-emergencies/66017.html. (Accessed on 20 October 2019).
27. Basu, Nayanima. Armed forces undergoing nuclear, biological warfare training. Business Line. 9 January 2018. https://www.thehindubusinessline.com/news/national/armed-forces-undergoing-nuclear-biological-warfare-training/article9813830.ece. (Accessed on 20 October 2019).
28. 2014-15 Annual Report - Part 3.2 Radiological & nuclear safety & security. Australian radiation protection and nuclear safety agency. https://www.arpansa.gov.au/about-us/corporate-publications/annual-reports/annual-report-2014-15/part-3-2. (Accessed on 2 June 2020).
29. Australian national progress report 2016 Washington Nuclear Security Summit. Australian Government. https://static1.squarespace.com/static/568be36505f8e2af8023adf7/t/56fd674d59827e329bd8fbfb/1459447629669/National+Progress+Report+Australia.pdf. (Accessed on 2 June 2020).
30. Follow-up mission report: Australia. IPPAS. 10 November 2017. https://www.dfat.gov.au/sites/default/files/2017-ippas-follow-up-mission-report.pdf. (Accessed on 2 June 2020).
31. NTI nuclear security index: Sabotage fourth edition. Nuclear threat initiative (NTI). September 2018. https://ntiindex.org/wp-content/uploads/2018/08/NTI_2018-Index_FINAL.pdf. (Accessed on 1 June 2020).
32. Rajagopalan rajeswari. Nuclear Security in India. Observer Research Foundation (ORF). (Accessed on 1 June 2020).

CONTRIBUTORS

Ms. Shivani Singh received her MPhil in Diplomacy and Disarmament from Jawaharlal Nehru University, New Delhi. She worked as a Consultant in the Nuclear Security Programme at a Delhi-based think tank, Institute of Peace and Conflict Studies (IPCS).